Τ.Ε.Ι. ΠΑΤΡΑΣ
ΣΧΟΛΗ : ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ : ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ

Π Τ Υ Χ Ι Α Κ Η Ε Ρ Γ Α Σ Ι Α

ΘΕΜΑ:

"ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΕΓΚΛΗΜΑΤΙΚΟΤΗΤΑ"

ΕΙΣΗΓΗΤΡΙΑ : κα ΗΡΑ ΑΝΤΩΝΟΠΟΥΛΟΥ

ΣΠΟΥΔΑΣΤΕΣ :
ΜΑΡΑΓΚΟΤΙΔΗΣ ΙΩΑΝΝΗΣ
ΠΑΝΤΑΖΟΠΟΥΛΟΣ ΚΩΝ/ΝΟΣ

ΣΕΠΤΕΜΒΡΙΟΣ 1995

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 4ο

ΤΟ ΦΑΙΝΟΜΕΝΟ ΤΗΣ ΕΙΣΒΟΛΗΣ

ΚΕΦΑΛΑΙΟ 5ο

ΠΡΟΣΩΠΙΚΟ

ΚΕΦΑΛΑΙΟ 6ο

ΑΠΑΤΗ ΣΤΟ ΧΩΡΟ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

ΚΕΦΑΛΑΙΟ 7ο

ΠΕΡΙΠΤΩΣΕΙΣ ΑΠΑΤΗΣ

ΚΕΦΑΛΑΙΟ 8ο

ΕΤΑΙΡΙΚΟΙ ΕΛΕΓΚΤΕΣ

ΚΕΦΑΛΑΙΟ 9ο

ΤΕΧΝΙΚΕΣ

ΚΕΦΑΛΑΙΟ 10ο

ΠΡΟΣΤΑΣΙΑ - ΑΠΟΖΗΜΙΩΣΗ ΑΠΟ ΑΠΑΤΗ ΣΤΟ ΧΩΡΟ ΤΩΝ Η/Υ

ΠΡΟΛΟΓΟΣ

Οι ηλεκτρονικοί υπολογιστές έφεραν επανάσταση στον τρόπο σκέψης και στον τρόπο δουλειάς, επηρέασαν σε βάθος τη σύγχρονη ζωή.

Πώς θα ήταν δυνατόν να μην επηρεάσουν τις μορφές της εγκληματικότητας, το νόμο αλλά και τα προβλήματα όπως έρχονται αντιμέτωποι με την εγκληματικότητα ;

Θα θέλαμε επ' ευκαιρία της δημιουργίας αυτής της εργασίας να ευχαριστήσουμε την κα 'Ηρα Αντωνοπούλου για την πολύτιμη συνεργασία της στην επιμέλεια αυτής της εργασίας.

ΚΕΦΑΛΑΙΟ 1ο

ΙΣΤΟΡΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Η ΕΝΝΟΙΑ ΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

Η έλευση της Πληροφορικής στον 20ο αιώνα παραλληλίζεται συχνά με τη Βιομηχανική Επανάσταση του 18ου αιώνα. Πράγματι η σπουδαιότερη ίσως επίδραση στην ανθρώπινη ζωή είναι η μετατόπιση του βάρους των ανθρώπινων δραστηριοτήτων στον τριτογενή τομέα παροχής υπηρεσιών και ιδιαίτερα στον κλάδο της επεξεργασίας πληροφορίας.

Η βαθύτατη αυτή διαρθρωτική αλλαγή που επέφερε η Πληροφορική μπορεί να συγκριθεί μόνο με την αλλαγή που προκάλεσε η Βιομηχανική Επανάσταση, μετατοπίζοντας το βάρος της οικονομίας από τον πρωτογενή τομέα στον δευτερογενή τομέα.

Βέβαια δεν θα ήταν ρεαλιστικό να περιμένουμε ότι τέτοιοι ριζικοί μετασχηματισμοί θα εξελιχθούν ισόρροπα και χωρίς τριβές.

Στο χώρο της παροχής υπηρεσιών η Πληροφορική επέτρεψε να ορθολογικοποιηθούν σημαντικά η οργάνωση της εργασίας και η διοίκηση των επιχειρήσεων. Ένα πολύ θετικό σημείο είναι ότι η Πληροφορική προσφέρει μία εντελώς νέα δυνατότητα απασχόλησης στον τομέα της παροχής υπηρεσιών, την τηλε-εργασία ή πιο απλά την εργασία από απόσταση. Είναι η διεκπεραίωση από έναν υπάλληλο μιας επιχείρησης παροχής υπηρεσιών σε ένα χώρο απομακρυσμένο απ' αυτόν της δουλειάς του, αφού μπορεί να αντλεί δεδομένα από την επιχείρηση

που εργάζεται και να στέλνει σε αυτή αποτελέσματα μέσω ενός γρήγορου τηλεπικοινωνιακού δικτύου.

Ο υπολογιστής για πολύ καιρό αποτέλεσε το μόνο έκθεμα της Πληροφορικής, που ήταν προσιτό στο πλατύ κοινό.

Όλοι γνωρίζουν ότι η Πληροφορική είναι ένας χώρος πολυδιάστατος όπου συνυπάρχουν ο σύνθετος κόσμος του προγραμματισμού και των γλωσσών, η ανάπτυξη κάθε τύπου εφαρμογών. Πίσω όμως απ' όλους αυτούς τους ισχυρούς υπολογιστές βρίσκεται ο άνθρωπος ως δημιουργός, αλλά και ως ανταγωνιστής της "τεχνητής νοημοσύνης". Το μεγάλο ζητούμενο όμως είναι η κατανόηση και η αντιμετώπιση κινδύνων που εγείρει η εισαγωγή της στην καθημερινή ζωή, τόσο των ίδιων των ανθρώπων όσο και των κοινωνιών που σχηματίζουν.

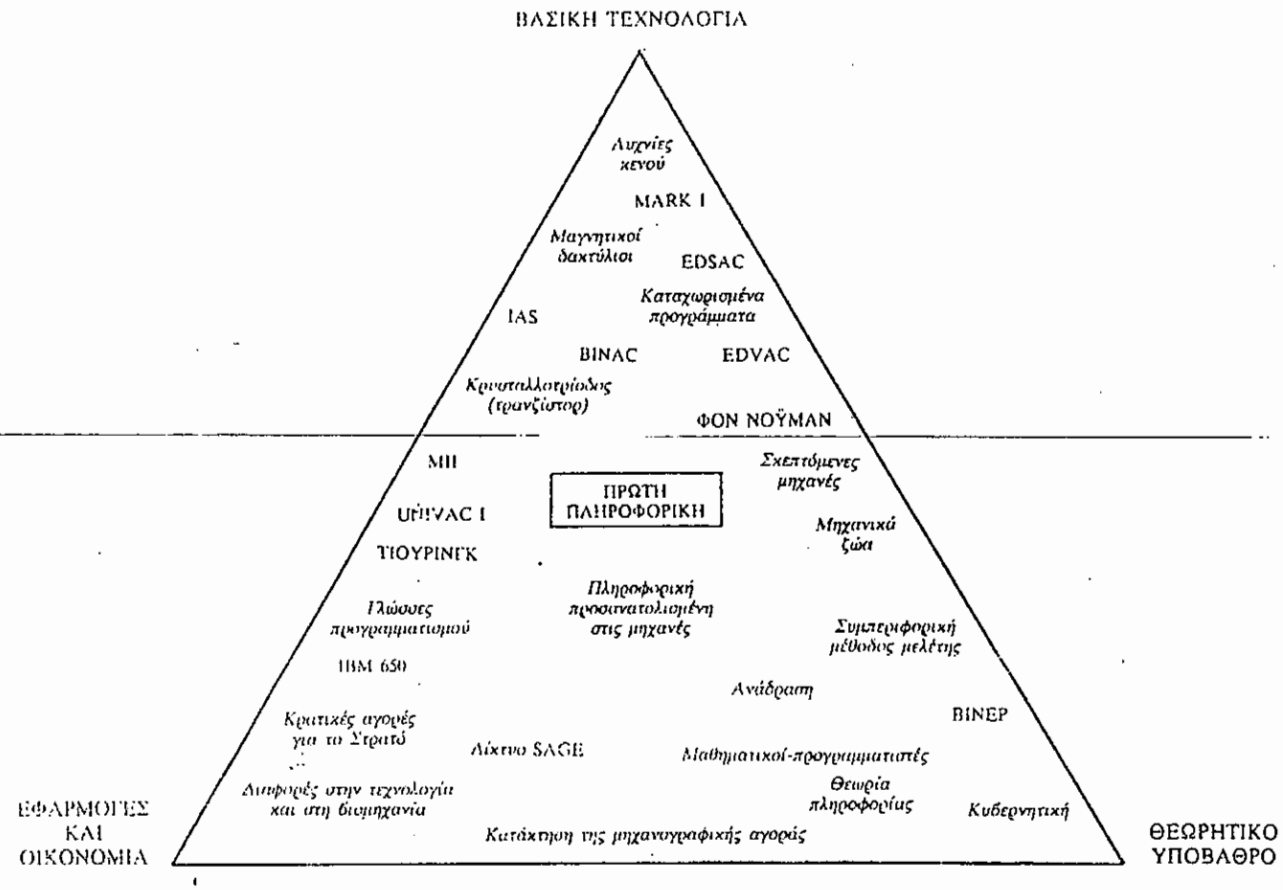
Το να υπάρχει ένα εκτεταμένο δίκτυο επικοινωνίας ενέχει τον κίνδυνο να μη χρησιμοποιηθεί αυτό για σωστή ενημέρωση, αλλά για παραπληροφόρηση και προπαγάνδα. Απαιτείται λοιπόν τα μέλη μιας κοινωνίας να γνωρίζουν που σταματά η δημόσια δράση ενός ατόμου και αρχίζει η ιδιωτική του ζωή.

Το γεγονός αυτό είναι ιδιαίτερα εμφανές στο χώρο των επιχειρήσεων, όπου μέσα από ένα τεράστιο δίκτυο επικοινωνίας και πληροφόρησης ανθεί η παρανομία και η εγκληματικότητα. Πριν μιλήσουμε όμως εκτενέστερα γι' αυτό το γεγονός, θα πρέπει να αναφερθούμε στα μεγάλα στάδια της ανάπτυξης των υπολογιστών που περιγράφονται ως "γενιές". Η "πρώτη γενιά" των υπολογιστών με τις ηλεκτρονικές λυχνίες, η "δεύτερη γενιά" με τις κρυσταλλοτριόδους (τρανζίστορ) μέχρι και για την φημισμένη "πέμπτη γενιά" που ανακοίνωσαν οι Ιάπωνες κατασκευαστές.

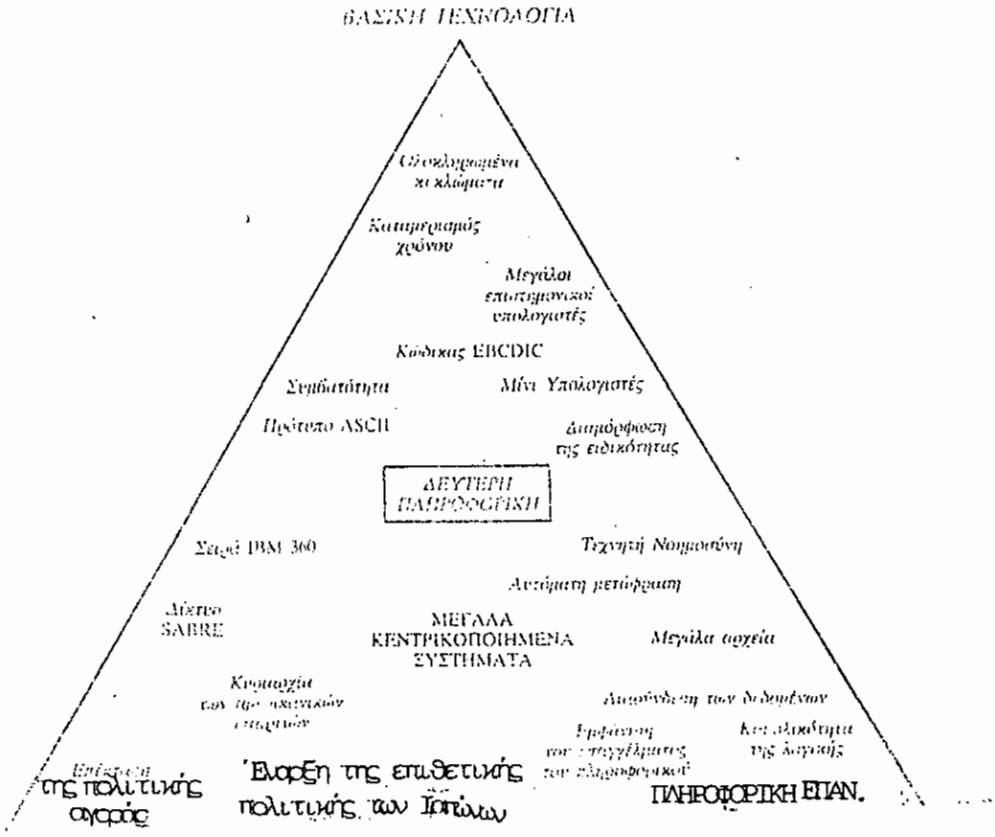
Για να διαπραγματευθεί ωστόσο κανείς την ιστορία της Πληροφορικής που είναι έννοια πολύ ευρύτερη, με πτυχές τόσο

τεχνολογικές όσο και κοινωνικές, οικονομικές και ανθρωπολογικές, χρειάζεται ένα χρονικό πλαίσιο πιο πλατύ και περισσότερο ενοποιητικό. Γι' αυτό θα παραθέσουμε τρία διαγράμματα που αντιστοιχούν σε μία ομαδοποίηση και συνοπτική ταξινόμηση, κάνοντας λόγο για την Πρώτη Πληροφορική που καλύπτει την περίοδο από το 1945 ως τα μέσα περίπου της δεκαετίας του '60, την Δεύτερη Πληροφορική που φτάνει μέχρι το τέλος της δεκαετίας του '70 και την Τρίτη Πληροφορική, αυτή την οποία ζούμε σήμερα.

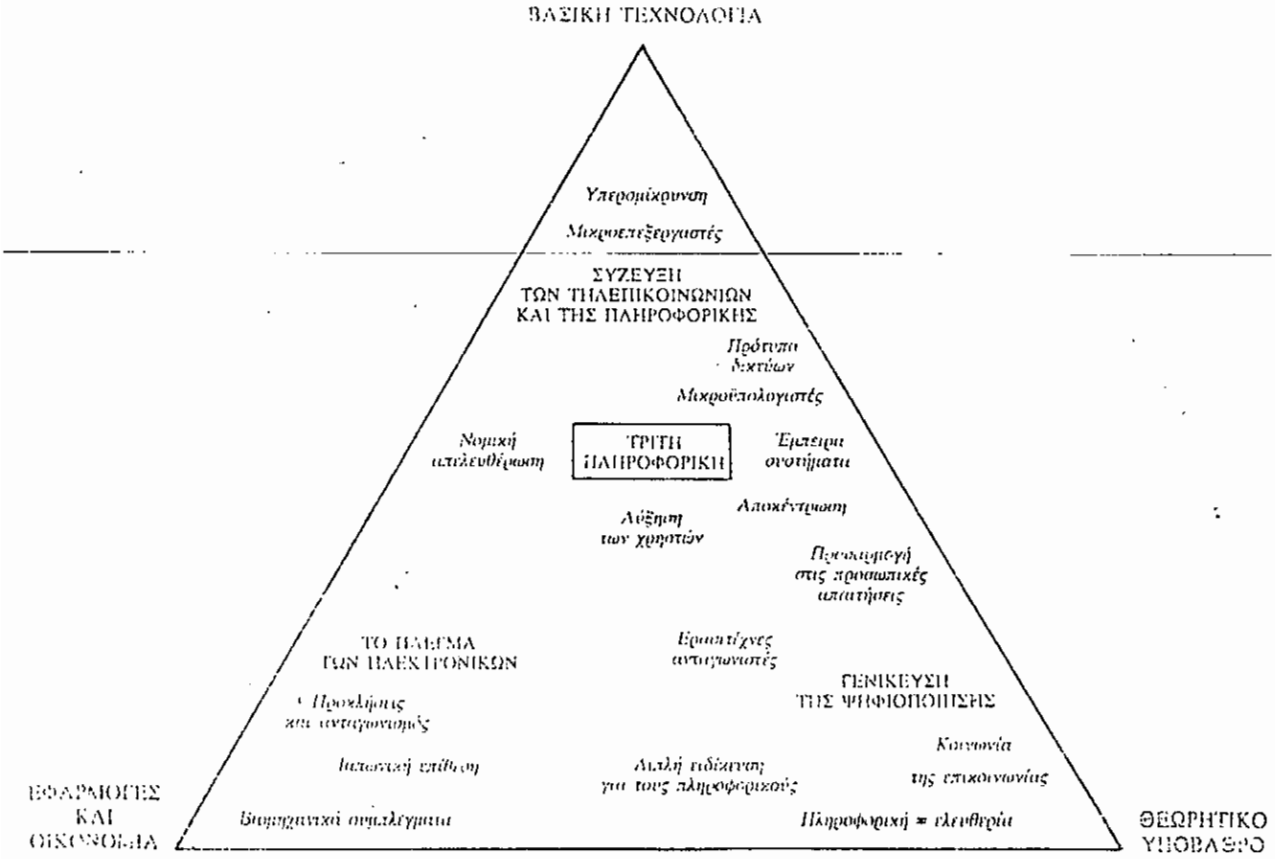
ΔΙΑΓΡΑΜΜΑ ΠΡΩΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ



ΔΙΑΓΡΑΜΜΑ ΔΕΥΤΕΡΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

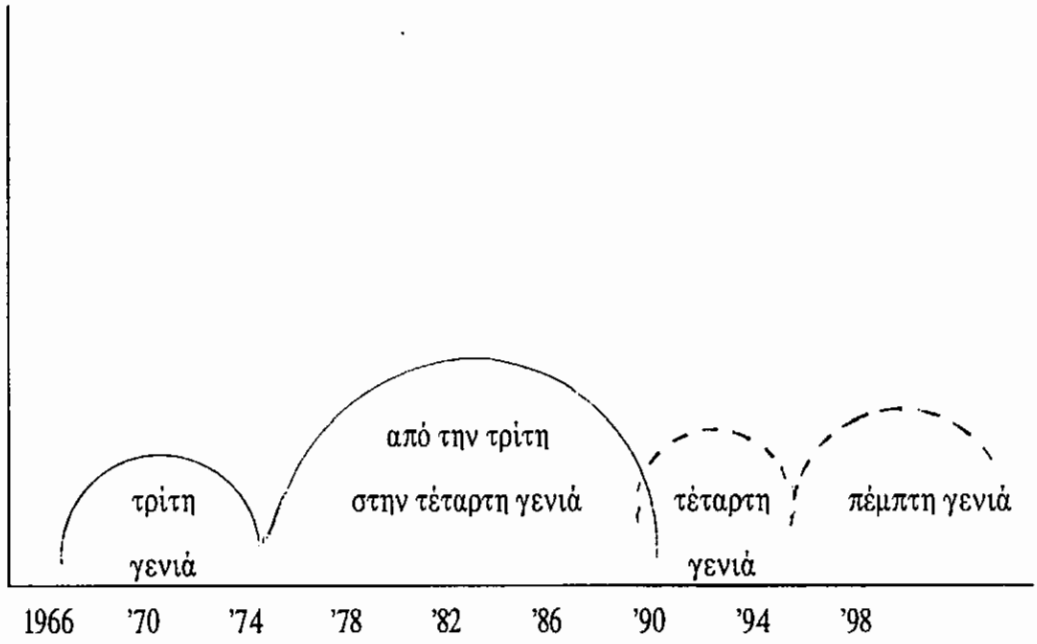


ΔΙΑΓΡΑΜΜΑ ΤΡΙΤΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ



ΔΙΑΓΡΑΜΜΑ (Η/Υ) - ΠΩΛΗΣΕΙΣ)

ΙΣΤΟΡΙΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



Ο όγκος των πωλήσεων υπολογιστικών συστημάτων
σε αντιστοιχία προς τις διαδοχικές γενιές υπολογιστών

ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΑΞΙΟΠΟΙΝΕΣ ΠΡΑΞΕΙΣ

Οι ηλεκτρονικοί υπολογιστές έφεραν επανάσταση στον τρόπο σκέψης και στον τρόπο δουλειάς, επηρέασαν σε βάθος τη σύγχρονη ζωή.

Δεν ήταν δυνατόν να μην επηρεάσουν τις διάφορες μορφές εγκληματικότητας, το Νόμο αλλά και τα προβλήματα όσων έρχονται αντιμέτωποι με την εγκληματικότητα. Όταν μιλάμε για πληροφοριακή

εγκληματικότητα αναφερόμαστε ειδικά στις μορφές αυτές που εμπίπτουν στην κατηγορία των οικονομικών εγκλημάτων.

Τα περισσότερα των εγκλημάτων σήμερα μπορούν να διαπραχθούν με τη βοήθεια ηλεκτρονικών υπολογιστών (Η/Υ). Τα κυριότερα νομικά προβλήματα του φαινομένου αυτού αφορούν τα οικονομικά εγκλήματα και πηγάζουν κυρίως από το γεγονός ότι οι αντίστοιχοι ποινικοί νόμοι προστατεύουν κυρίως ενσώματα και ορατά αντικείμενα κατά προσβολών. Το πληροφοριακό όμως έγκλημα επηρεάζει όχι μόνο τα παραδοσιακά αντικείμενα που εμπεριέχονται σε νέους φορείς (δίσκους - ταινίες κ.λ.π.) αλλά και αφορά νέα αντικείμενα (προγράμματα Η/Υ) και νέες μεθόδους τέλεσης των αξιόποινων πράξεων.

Τα προγράμματα των Η/Υ προστατεύονται αν και υπό προϋποθέσεις ως έργα πνευματικής ιδιοκτησίας, σύμφωνα με το Ν. 2387/20 και τη Διεθνή Σύμβαση της Βέρνης. Ο Ποινικός Κώδικας έχει τροποποιηθεί με μοναδικό σκοπό την προστασία κατά της πληροφοριακής εγκληματικότητας, διευρύνει την έννοια του "εγγράφου" ώστε να θεωρούνται ορισμένες πράξεις ως αξιόποινες (πλαστογραφία, υπεξαγωγή κ.λ.π.), ώστε να αντιμετωπισθούν ειδικές περιπτώσεις πληροφοριακών εγκλημάτων (απόρρητα προγράμματα, δεδομένα και πληροφορίες, παράνομη αντιγραφή, εισβολή). Στην προσπάθεια αυτή η Ελλάδα αλλά και άλλες Ευρωπαϊκές χώρες εκσυγχρονίζουν το νομικό τους πλαίσιο μπροστά στην "Επανάσταση της Πληροφορικής", παίρνοντας παράδειγμα την Γαλλία, την Δ. Γερμανία αλλά και την Αγγλία μετά την περιβόητη υπόθεση R.V. Gold / Schifreen.

ΚΕΦΑΛΑΙΟ 2ο

ΤΟ ΦΑΙΝΟΜΕΝΟ ΤΗΣ ΑΠΑΤΗΣ

Η ΑΠΑΤΗ ΣΤΟ ΧΩΡΟ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Το ενδεχόμενο της απάτης αποτελούσε πάντα μία απειλή για τον επιχειρηματικό χώρο και τον κόσμο των εταιριών γενικότερα.

Για την αντιμετώπιση αυτής της απειλής λαμβάνονται μέτρα προστασίας όπως η θέσπιση νομοθετικού πλαισίου, τα κατάλληλα μέτρα από την πλευρά των επιχειρήσεων, η ασφαλιστική κάλυψη κ.λ.π.

Τα τελευταία χρόνια με την ταχεία ανάπτυξη της τεχνολογίας των πληροφοριών (information technology) αποδείχθηκε ότι είναι ανάγκη να αντιμετωπισθεί με μεγάλη προσοχή το θέμα της απάτης στο περιβάλλον της υψηλής τεχνολογίας.

Στις περιπτώσεις αυτές συνήθως ο δράστης είναι ένας καταρτισμένος επαγγελματίας του χώρου της Πληροφορικής, ικανός να χειρισθεί πολύπλοκα συστήματα βασισμένα στους υπολογιστές για το δικό τους έκνομο συμφέρον.

Η απάτη με υπολογιστές (computer froud) αντιπροσωπεύει σημαντικές ζημιές για τις επιχειρήσεις. Καμμία διοίκηση επιχείρησης που συμμετέχει στη διαμόρφωση του σημερινού ανταγωνιστικού κλίματος δεν μπορεί να αγνοήσει την περίπτωση της απάτης ή μέτρα που πρέπει να ληφθούν για την αντιμετώπισή της.

Η απάτη μπορεί να πάρει πολλές μορφές, ο χαρακτήρας της δε σε κάθε κοινωνία επηρεάζεται από παράγοντες όπως η εμπορική

συμπεριφορά, η κρατούσα ηθική τάξη και ο βαθμός της τεχνολογικής ανάπτυξης.

ΤΟ ΦΑΙΝΟΜΕΝΟ ΤΗΣ ΑΠΑΤΗΣ

Η νομική επιστήμη δεν δίνει ένα λειτουργικό ορισμό της απάτης, αλλά μιλά για απάτη σε βάρος της εταιρίας (company fraud), απάτη επενδύσεων.

Ο Michael Comer υποστήριξε ότι "η συμπεριφορά με την οποία κάποιος προσπαθεί να αποκτήσει πλεονέκτημα έναντι κάποιου άλλου με δόλιο τρόπο είναι απάτη".

Η απάτη με υπολογιστή αποτελεί μορφή απάτης ανεξαρτήτως από τη χρήση ή την κατάχρηση του υπολογιστικού συστήματος. Υπάρχει πάντα κάποια ζημιά και ένα όφελος που το προσπορίζεται χωρίς να έχει τέτοιο δικαίωμα. Η απάτη συνδέεται άμεσα με τη ζημιά και την ανεντιμότητα.

Σκοπός της απάτης είναι η αποστέρηση περιουσιακών στοιχείων από κάποιο τρίτο. Ο δράστης ίσως προκαλέσει σκόπιμη σύγχυση για να παραπλανήσει τον εξαπατούμενο. Εδώ η απάτη εμπεριέχει κάποιο βαθμό συγκάλυψης.

Η συγκάλυψη έχει σαν σκοπό να αποσπάσει την προσοχή από την ίδια την απάτη αν και σε ένα καλά οργανωμένο λογιστικό σύστημα η συγκάλυψη θα αποκαλυφθεί σύντομα. Η συγκάλυψη σε μία απάτη είναι απαραίτητη για τρεις λόγους:

- για την παρεμπόδιση ή την αποφυγή της αποκάλυψης της ζημιάς,
- για την παρεμπόδιση της αποκάλυψης της ταυτότητος του ίδιου του δράστη,
- και (θεωρητικά) για την διευκόλυνση της συνέχισης της απάτης.

(Το γεγονός οφείλεται στο ότι ο υπαίτιος συνεχίζει να διευρύνει την απάτη διά χάριν της απληστίας του και όταν αποκαλυφθεί δεν μπορεί να προσδιορίσει την χρονική στιγμή που άρχισε η απάτη).

Η συγκάλυψη της απάτης είναι σημαντική για το δράστη, γιατί πάντοτε η έρευνα για κάποια απάτη ξεκινά όταν η απάτη έχει αποκαλυφθεί. Χωρίς αποκάλυψη δεν είναι δυνατόν να υπάρξει έρευνα.

Για την συγκάλυψη της απάτης ο δράστης θέτει ως στόχο της συγκάλυψης της ενοχής του, είτε με παραπλανητική παρουσίαση της λογιστικής αξίας ενός περιουσιακού στοιχείου, είτε με την διόρθωση ενός λογαριασμού.

Παραπλανητική παρουσίαση αποτελεί η εσκεμμένη παραποίηση των λογιστικών εγγράφων με σκοπό την εξαπάτηση. Η αρχική συγκάλυψη της ζημιάς είναι το ίδιο σημαντική για το δράστη όσο και η συνεχής συγκάλυψή της.

Ο πρώτος στόχος του δράστη, αφού έχει διαπράξει την απάτη, είναι η συγκάλυψη της ευθύνης. Θα ήταν ακραία απερισκεψία εκ μέρους του να διαπράξει την απάτη και να αφήσει ίχνη που οδηγούν κατευθείαν σε αυτόν. Η μεταβίβαση της κατηγορίας είναι το "έσχατο μέσο" του δράστη, εφόσον η απάτη του αποκαλυφθεί.

Η ίδια η συγκάλυψη μπορεί να αποτελέσει το μέσο με το οποίο διαπράττεται απάτη, κλοπή ή εξαπάτηση. Π.χ. η παράνομη χρήση ενός κλεμμένου συνθηματικού του υπολογιστή - ταυτότητα του χρήστη - δίνει το δικαίωμα στο δράστη να κρύψει την πραγματική του ταυτότητα. Προσποιείται ότι είναι ο εξουσιοδοτημένος χρήστης του υπολογιστικού συστήματος. Τα συνθηματικά δεν αποτελούν αλάνθαστο στοιχείο αναγνώρισης για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στον υπολογιστή. Η τέλεια συγκάλυψη μιας απάτης θα κρύψει τις ζημιές και θα κατευθύνει τις υποψίες μακριά από το δράστη, στην περίπτωση που θα εξακριβωθεί η απάτη. Η τακτική παρουσία του

ενόχου στα μέσα με τη βοήθεια των οποίων έγινε η απάτη, ίσως αποτελεί σοβαρή ένδειξη.

Η απάτη του ίσως απαιτεί συχνή και συνεχή εσφαλμένη παρουσίαση, "φτιάξιμο" και μεταβολές στα διάφορα στοιχεία και στους λογαριασμούς. Ο δράστης πιθανότατα να επιλέξει αντί του να πάρει ολόκληρη την άδειά του να παίρνει τμηματικά από λίγες ημέρες. Ο υπαίτιος ίσως πρέπει να είναι παρών τον περισσότερο καιρό για να μπορεί να συγκαλύπτει την δόλια πράξη του.

ΔΩΡΟΔΟΚΙΑ ΚΑΙ ΔΙΑΦΘΟΡΑ

Η δωροδοκία και η δολιοφθορά είναι από τα παλαιότερα αδικήματα του Κώδικα. Θεωρείται βέβαιο ότι η διαφθορά συνδυάζεται με τη δωροδοκία. Το αδίκημα έγκειται στην προσφορά και στην αποδοχή κάποιου "δώρου" με σκοπό να καρπωθεί κάποιος αμοιβή ή κάποιο πλεονέκτημα. Πάντοτε υπάρχει ο δωροδοκών και ο δωροδοκούμενος.

Η ποινική δίωξη με βάση το Νόμο περί δωροδοκίας σε δημόσιους οργανισμούς οδηγεί στο Κακουργοδικείο. Επιβάλλεται καταδικαστική ποινή δύο χρόνων αναγκαστικής φυλάκισης ή πρόστιμο ή και τα δύο.

Ο ένοχος χάνει τη θέση του και αποκλείεται από την κατάληψη δημόσιας θέσης ισοβίως. Επίσης στερείται των πολιτικών του δικαιωμάτων για 5 χρόνια. Οι απάτες σε βάρος εταιριών αποτελούν ιδιαίτερο αντικείμενο έρευνας της αστυνομίας. Ο εκκαθαριστής μιας εταιρίας μπορεί να καλέσει τον προϊστάμενο της Εισαγγελίας, εάν διαπιστώσει ότι η υπό εκκαθάριση εταιρία έχει εξαπατήσει το κοινό ή έχει υποστεί υπεξαίρεση.

Ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Ο.Ο.Σ.Α.) ορίζει το πληροφοριακό έγκλημα ως κάθε παράνομη, ανήθικη ή χωρίς άδεια συμπεριφορά, που ενέχει την αυτόματη επεξεργασία δεδομένων και / ή την μετάδοση δεδομένων.

Η έκθεση οριοθετεί πέντε κατηγορίες συμπεριφοράς ποινικού ενδιαφέροντος:

1. Εισαγωγή, μεταβολή, καταστροφή δεδομένων, προγραμμάτων με σκοπό την τέλεση εγκλήματος κατά πραγμάτων περιουσιακής φύσεως.
2. Εισαγωγή με σκοπό την τέλεση εγκλήματος κατά της αξιοπιστίας εγγράφων.
3. Εισαγωγή με σκοπό την παρεμπόδιση λειτουργίας πληροφοριακών ή τηλεπικοινωνιακών συστημάτων.
4. Προσβολή των αποκλειστικών δικαιωμάτων του δημιουργού.
5. Χωρίς άδεια εισβολή σε πληροφοριακά συστήματα και αφαίρεση στοιχείων, με σκοπό την παραβίαση μηχανισμών ασφάλειας ή την τέλεση εγκλήματος.

ΣΥΣΤΑΤΙΚΑ ΑΠΑΤΗΣ

Τα τρία συστατικά κάθε απάτης είναι η ανάγκη, η ευκαιρία και η γνώση. Με την πρόσληψη ενός υπαλλήλου δύο από τα τρία αυτά στοιχεία και πιο συγκεκριμένα η ευκαιρία και η γνώση υπάρχουν ήδη, λόγω της φύσης του επαγγέλματος.

Με την Πληροφορική παρέχεται η ευκαιρία, γιατί ο εργαζόμενος οφείλει να χειρίζεται τον υπολογιστή ή το τερματικό ενός υπολογιστή στα πλαίσια των καθημερινών καθηκόντων του. Η γνώση αποκτάται με την κατάλληλη ενημέρωση ή ίσως το άτομο αυτό να έχει προσληφθεί

για τις γνώσεις που έχει ήδη αποκτήσει, όπως γίνεται με τους εξωτερικούς συμβούλους. Οι υπεύθυνοι πολλών οργανισμών δεν κατανοούν τους κινδύνους που συνεπάγεται μια ενδεχόμενη απάτη με υπολογιστή (computer fraud) ή μία ενδεχόμενη κατάχρηση με υπολογιστή (computer abuse). Υποθέτουν ότι η απάτη συμβαίνει στις άλλες επιχειρήσεις και όχι στην δική τους εταιρία.

Παράλληλα οι υπεύθυνοι πολλών οργανισμών δεν θεωρούν την απάτη με υπολογιστή πρόβλημα. Όμως παρουσιάζονται κάποιες ανωμαλίες με το προσωπικό των υπολογιστών. Ειδικότερα μετά τα τέλη της δεκαετίας του 1960 πολλά άτομα του προσωπικού των υπολογιστών προήχθησαν ταχύτατα σε θέσεις προϊσταμένων και διευθυντών, σε ένα κλάδο με νέους ανθρώπους και υψηλές προσδοκίες που παρέμειναν ανεκπλήρωτες, δημιουργώντας δυσαρέσκεια και απογοήτευση.

Όμως με το πέρασμα του χρόνου ο κλάδος της Πληροφορικής πέρασε καθαρά στην περίοδο του επαγγελματισμού, ο δρόμος προς την κορυφή έγινε ιδιαίτερα δύσκολος, με αποτέλεσμα κάποιοι ειδικοί της Πληροφορικής να στραφούν πέρα από τα όρια της τιμιότητος.

Η απογοήτευση προκάλεσε πολλούς κατά τα άλλα ευφυείς ανθρώπους να διαπράξουν άνομες πράξεις σε βάρος των εργοδοτών τους, χρησιμοποιώντας τις συγκεκριμένες ικανότητές τους για την τέλεση πράξεων απάτης και κατάχρησης.

Οι Βρετανικές ασφαλιστικές εταιρίες θεωρούν την απάτη με υπολογιστή πρόβλημα.

Υπάρχουν ασφαλιστήρια συμβόλαια (insurance policies) ειδικά για να καλύπτουν τις απάτες και ορισμένα μάλιστα καλύπτουν τις ζημιές που αυτές συνεπάγονται.

Εκείνο που είναι σίγουρο είναι ότι οι υπολογιστές δημιούργησαν περισσότερες ευκαιρίες για απάτη.

Οι νέες αυτές ευκαιρίες παρουσιάζονται λόγω της εισαγωγής και της χρήσης των υπολογιστών, οι οποίοι έθεσαν σε αχρηστία τις καθιερωμένες διαδικασίες του γραφείου.

Για παράδειγμα σπάνια η εισαγωγή δεδομένων στον υπολογιστή επικυρώνεται από άλλο πρόσωπο.

Σήμερα σε μία επιχείρηση ακόμα και ο τελευταίος χειριστής τερματικού κατέχει μια σημαντική και έμπιστη θέση. Και με τη σχέση εμπιστοσύνης παρουσιάζεται και η ευκαιρία για εξαπάτηση. Βέβαια πρέπει να τονίσουμε ότι η απάτη με υπολογιστή έχει πολλές δυσκολίες, απαιτεί τεχνικές γνώσεις και έτσι δεν είναι εύκολο σε έναν ανειδίκευτο να καταλάβει. Κάποιος που έχει γνώση του λογιστικού συστήματος και του συστήματος του υπολογιστή, παρουσιάζει και τις μεγαλύτερες πιθανότητες για να διαπράξει απάτη.

Βέβαια, προσπαθώντας να διαπράξει κάποιος μια απάτη άμεσα προσβάλλει ένα προστατευόμενο αγαθό (περιουσία - προσωπικότητα - δημόσιο συμφέρον). Έτσι μπορεί να διαπράξει :

- Απάτη μέσω χειρισμού Η/Υ κατά πληροφοριακών συστημάτων (κλοπή, κατάχρηση, απάτη με πιστωτική κάρτα, παραβίαση εχεμύθειας).
- Πληροφοριακή κατασκοπεία.
- Χωρίς άδεια πρόσβαση σε πληροφοριακά συστήματα.
- Κλοπή υπηρεσιών.
- Πληροφοριακή δολιοφθορά.

ΚΕΦΑΛΑΙΟ 3ο

Η ΑΠΑΤΗ ΣΤΟ ΧΩΡΟ ΤΩΝ Η/Υ

Η ΑΠΑΤΗ ΣΤΟ ΧΩΡΟ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ ΚΑΙ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Σήμερα οι εταιρίες και οι άλλοι οργανισμοί είναι πλήρως εξαρτημένοι από τα υπολογιστικά τους συστήματα.

Η αδυσώπητη εξέλιξη προς ένα κόσμο προσανατολισμένο στους υπολογιστές, σημαίνει ότι μία ημέρα όλες οι απάτες θα είναι απάτες με υπολογιστή. Ο πανταχού παρών υπολογιστής εισχωρεί σε γραφεία, σπίτια, εργοστάσια. Χαρακτηριστικό παράδειγμα στην Αμερική όπου μετά τη δύση του ήλιου πολλά πρατήρια καυσίμων δέχονται πληρωμή μόνο με πιστωτικές κάρτες. Δεν δέχονται μετρητά, γιατί ο φόβος μιας πιθανής ληστείας είναι μεγάλος. Αυτό άλλαξε και τον τρόπο του εγκλήματος.

Οι άνθρωποι ληστεύονται για τις πλαστικές πιστωτικές τους κάρτες ή εξαναγκάζονται να αποκαλύψουν τους προσωπικούς αριθμούς ταυτότητος.

Όπως ο υπολογιστής εισβάλλει και διαπερνά την καθημερινή μας ζωή, έτσι εισβάλλει και καθορίζει και την μορφή του αδικήματος.

Ένα άλλο παράδειγμα μας φέρνει στις Η.Π.Α. λίγα χρόνια πριν, όπου οι κρατούμενοι ομοσπονδιακών φυλακών έμαθαν μόνοι τους προγραμματισμό και παραβίασαν αρχεία της Εφορίας, ενώ εξέτιαν ποινές για άλλες καταδίκες.

Εδώ μπορούμε να πούμε όμως ότι η σχέση μεταξύ υπολογιστή και εγκληματία είναι αμφίδρομη : οι υπολογιστές από τη μία θα διευρύνουν τους στόχους των εγκληματικών δραστηριοτήτων και από την άλλη θα ενισχύσουν παράλληλα με το ευρύ φάσμα των δυνατοτήτων τους τον Νόμο.

Στο σημείο αυτό θα ήταν σκόπιμο να διακρίνουμε την απάτη με υπολογιστή απ' την απάτη σχετιζόμενη με υπολογιστή ή υποβοηθούμενη με υπολογιστή.

Η απάτη σχετιζόμενη με υπολογιστή έχει λίγη σχέση με τον ίδιο τον υπολογιστή, πέρα από το γεγονός ότι χρησιμοποιήθηκε ένα πληκτρολόγιο για την εισαγωγή δεδομένων. Η απάτη μπορεί να έχει γίνει με παραποίηση των πρωτοτύπων στοιχείων στα βιβλία.

Επομένως η απάτη η σχετιζόμενη με υπολογιστή είναι μια απάτη όπου ο υπολογιστής εισέρχεται συγκυριακά. Απλώς συμβαίνει να χρησιμοποιείται για την επεξεργασία του λογιστικού συστήματος σε βάρος του οποίου τελείται το συγκεκριμένο αδίκημα.

Η απάτη υποβοηθούμενη με υπολογιστή είναι σίγουρα η λογική επέκταση της απάτης της προηγούμενης κατηγορίας.

Στην περίπτωση αυτή μία συσκευή εισαγωγής δεδομένων χρησιμοποιείται για την τέλεση της απάτης, η οποία μπορεί να συνίσταται στην παραποίηση στοιχείων από τα πρωτότυπα παραστατικά καθώς αυτά εισάγονται ή στην παραποίηση των αριθμών στους λογαριασμούς.

Το είδος αυτό της απάτης δεν χρειάζεται ειδικές γνώσεις υπολογιστών παρά μόνο τη γνώση χειρισμού μιας συσκευής εισαγωγής δεδομένων.

Ερχόμαστε τώρα στην απάτη με υπολογιστή, μια "γνήσια" απάτη που δεν μπορεί να γίνει χωρίς υπολογιστή. Στην κατηγορία αυτή εμπί-

πτουν απάτες στο λειτουργικό σύστημα, απάτες στον προγραμματισμό και ορισμένοι τύποι απάτης στην εισαγωγή δεδομένων.

Έτσι οι πραγματικές απάτες με υπολογιστή απαιτούν ειδικές γνώσεις Πληροφορικής και πολύ μεγάλες ικανότητες.

Από στοιχεία της Επιτροπής Λογιστικών Ερευνών της Βρετανίας εμφανίζεται η παρακάτω κατανομή για τις διάφορες κατηγορίες απάτης με υπολογιστή :

ΚΑΤΗΓΟΡΙΕΣ	ΠΟΣΟΣΤΟ
1. Παραποίηση των δεδομένων εισόδου ή του κύριου αρχείου (Master file)	64%
2. Παραποίηση των δεδομένων εξόδου	3%
3. Μετατροπή του προγράμματος	1%
4. Κατάχρηση των πόρων συστήματος	32%

Οι γνωστές περιπτώσεις απάτης και αδικημάτων με υπολογιστή δεν αποτελούν παρά μόνο την κορυφή του παγόβουνου, αφού μεγάλος είναι ο αριθμός των περιπτώσεων που δεν έχουν ακόμα αποκαλυφθεί.

Οι στατιστικές του Υπουργείου Εσωτερικών περιλαμβάνουν τις απάτες με υπολογιστή κάτω από το γενικό τίτλο "Απάτες και Πλαστογραφήσεις".

Οι υπολογιστές μπορούν να εμπλέκονται σε πολλά εγκλήματα, που είτε συνδέονται με απάτες είτε δεν έχουν σχέση με αυτές.

- Κλοπή.
- Κατάχρηση.
- Δωροδοκία.
- Δολιοφθορά.
- Κατασκοπεία.

- Συνωμοσία.
- Εκβιασμός.
- Απαγωγή.

Το Ομοσπονδιακό Γραφείο Ερευνών των Η.Π.Α. (F.B.I.) ορίζει το έγκλημα με υπολογιστή ως κάθε παράνομη ενέργεια για την οποία απαιτείται η γνώση της τεχνολογίας των υπολογιστών και η οποία είναι βασική για την επιτυχή της εκτέλεση.

Βλέπουμε λοιπόν ότι οι υπολογιστές μπορούν να συμμετέχουν στο έγκλημα κατά τέσσερις διαφορετικούς τρόπους:

- Μπορεί να αποτελούν το στόχο του εγκλήματος (καταστροφή τους ή καταστροφή των αρχείων που τηρούνται σε μαγνητικά ή άλλα μέσα).
- Μπορεί να είναι το θέμα του εγκλήματος (π.χ. ένας υπολογιστής να αποτελεί τον τόπο ενός εγκλήματος).
- Μπορεί να είναι το όργανο του εγκλήματος.
- Μπορεί να είναι το σύμβολο του εγκλήματος. Ένας υπολογιστής μπορεί να χρησιμοποιηθεί για εκφοβισμό ή παραπλάνηση (π.χ. η ψευδής διαφήμιση υπηρεσιών που δεν παρέχονται).

Τα πρώτα χρόνια που εμφανίστηκαν οι υπολογιστές, οι εργαζόμενοι σε αυτούς αποτελούσαν μία ελίτ που μιλούσε μια ειδική γλώσσα και περιβάλλονταν από κάποιο απόκρυφο μυστικισμό. Τώρα πια όμως δεν ισχύει. Οι ειδικοί των υπολογιστών συνεχίζουν να υπάρχουν, όμως οι γνώσεις της Πληροφορικής έχουν διαδοθεί σε ένα ευρύ κύκλο. Ακόμα και οι μαθητές των Δημοτικών Σχολείων γνωρίζουν την ειδική διάλεκτο, ενώ η Πληροφορική επηρεάζει την ομιλία και τη σκέψη μας. Η έλευση των υπολογιστών επηρέασε το χαρακτήρα της κοινωνικής επαφής, αλλά διαμόρφωσε και την ίδια την κοινωνία.

Σήμερα, λαμβάνοντας υπόψη την εκμετάλλευση των μικροϋπολογιστών και του προγραμματισμού, η δυναμική της απάτης με υπολογιστή είναι τεράστια. Οι μικροϋπολογιστές μπορούν να αγοραστούν σήμερα έξω από τα διαθέσιμα κονδύλια της διεύθυνσης, μιας και οι τιμές τους είναι χαμηλές. Υπάρχει ελάχιστος ή και μηδενικός έλεγχος πάνω στην ταχεία εξάπλωση της νέας τεχνολογίας. Οι κατασκευαστές υπολογιστικών συστημάτων μπορούν να κατασκευάσουν συστήματα "επί παραγγελία" για τις ανάγκες του χρήστη.

Πακέτα γενικών προγραμμάτων γραφείου και λογιστικής προσφέρονται "κατευθείαν από το ράφι" και πολλά δεν έχουν καμμία πρόβλεψη προστασίας από ενδεχόμενη απάτη ή κατάχρηση. Ορισμένα υπολογιστικά συστήματα αγοράζονται εν αγνοία της γενικής διεύθυνσης και δεν διαθέτουν δινατότητες κεντρικού ελέγχου.

Στο αναπτυσσόμενο τεχνολογικό περιβάλλον ένας από τους μεγαλύτερους κινδύνους απάτης μπορεί να προέλθει από τους προγραμματιστές υπολογιστών, που κάνουν κακή χρήση του υπολογιστικού συστήματος. Οι προγραμματιστές υπολογιστών μπορεί να δηλώσουν ότι απαιτείται κάποια τροποποίηση του προγράμματος και να την εφαρμόσουν. Αν όμως η τροποποίηση αυτή δεν ελεχθεί από κάποιον υπεύθυνο που έχει τη γνώση, ποιός θα κρίνει αν ήταν αναγκαία και ορθή ως προς τους σκοπούς που στόχευε.

Διαφαίνεται σήμερα ότι με την κατάρρευση του "μυστικισμού" των υπολογιστών και καθώς μεγαλώνουν τα παιδιά της γενιάς της Πληροφορικής στα σχολεία μας, τα προβλήματα απάτης και κατάχρησης με υπολογιστές διογκώνονται. Ιδιαίτερα σημαντικό στοιχείο αποτελεί ο αυξημένος αριθμός ανθρώπων που προγραμματίζουν το δικό τους οικιακό υπολογιστή.

Το φαινόμενο των εισβολέων (hackers) είναι υπαρκτό ιδίως στις Η.Π.Α. Ο εισβολέας είναι το πρόσωπο εκείνο που θα προσπαθήσει να εξαπατήσει το υπολογιστικό σύστημα, όχι από μοχθηρία ή κακή πρόθεση, αλλά από "ακαδημαϊκή πρόκληση". Και βέβαια πρόκειται για ιδιαίτερα επικίνδυνο άτομο.

Πρέπει να πούμε ότι στην περίοδο ανάπτυξης της τεχνολογίας δημιουργήθηκε μια έλλειψη εμπιστοσύνης προς τον υπολογιστή, αφού οι χρήστες δεν απολαμβάνουν τις υπηρεσίες που θα ήθελαν.

Η έλλειψη εμπιστοσύνης οδήγησε και στην έλλειψη επιθυμίας για ανάμιξη από την πλευρά του τελικού χρήστη και άφησε έτσι ανοιχτό το δρόμο στους δόλιους ειδικούς των υπολογιστών. Συνεργία δηλαδή από αμέλεια.

Παράλληλα οι ειδικοί των υπολογιστών κουβαλούσαν μια παραδοσιακή αντιπάθεια και αδιαφορία για την τεκμηρίωση. Κατασκεύαζαν πρόθυμα προγράμματα αλλά και τροποποιήσεις προγραμμάτων, όχι όμως και την αντίστοιχη τεκμηρίωση.

Ο χρήστης δεν καταλαβαίνει τον τρόπο με τον οποίο το σύστημα επεξεργάζεται τα δεδομένα του. Αίρεται λοιπόν η αξιοπιστία του συστήματος. Όλες οι τροποποιήσεις, οι αλλαγές, οι προσαρμογές και οι μεταβολές ενός υπολογιστικού συστήματος, πρέπει να τεκμηριώνονται με πληρότητα και να διατίθενται στο χρήστη έγκαιρα και αποτελεσματικά. Η τεκμηρίωση είναι βασική για την ασφάλεια και τον έλεγχο του συστήματος.

Σε συνδυασμό με το πρόβλημα της ελλειπούς τεκμηρίωσης υπάρχει και το πρόβλημα της έλλειψης ενός συνόλου προτύπων και διαδικασιών που ελέγχουν το υπολογιστικό σύστημα.

Όλα τα μεγάλα συστήματα έχουν συνήθως κάποια πρότυπα και διαδικασίες που υπαγορεύουν τη χρήση τους. Ένα πρότυπο είναι ο

βαθμός τελειότητος που απαιτείται κατά την εκτέλεση μιας συγκεκριμένης εργασίας.

Η διαδικασία αποτελεί το μέσο για την επίτευξη του προτύπου. Η εμφάνιση των μικροϋπολογιστών έκανε πολύ δύσκολη την δημιουργία ενός συστήματος, στο οποίο οι αρμοδιότητες των χρηστών διαχωρίζονται πλήρως, ενώ μη συμβατές λειτουργίες δεν γίνονται μόνο από ένα πρόσωπο. Αγνοώντας τον κίνδυνο αυτό, αφήνουμε την εταιρία απροστάτευτη από ενδεχόμενες ενέργειες εξαπάτησης ή κατάχρησης. Οι αρμοδιότητες πρέπει πάντα να διαχωρίζονται όταν δεν συμβιβάζονται με την ασφάλεια και τον έλεγχο του συστήματος.

Το πρόσωπο που χειρίζεται τον υπολογιστή δεν πρέπει να ταυτίζεται με αυτό που κάνει τις αλλαγές στα πακέτα των προγραμμάτων. Οι προγραμματιστές δεν πρέπει να έχουν πρόσβαση στο ζωντανό υπολογιστικό σύστημα αλλά μόνο στο δοκιμαστικό, εκτός και αν ελέγχονται από τρίτους.

Με άλλα λόγια λοιπόν, οι χειριστές δεν πρέπει να προγραμματίζουν τα πακέτα που δουλεύουν, ενώ οι προγραμματιστές δεν πρέπει να χειρίζονται τον υπολογιστή, τον οποίο είναι υπεύθυνοι να προγραμματίζουν.

'Ενα άλλο ακόμα μεγάλο πρόβλημα στον υπολογιστή αποτελεί η μη ελεγχόμενη πρόσβαση. Οι μικροϋπολογιστές και τα τερματικά γραφείου δεν μπορούν να έχουν τον ίδιο βαθμό φυσικής διασφάλισης με αυτόν ενός μεγάλου συστήματος.

Παρ' όλ' αυτά ο έλεγχος της πρόσβασης είναι πάντα αναγκαίος. Στην ιδανική κατάσταση σε ένα τερματικό υπολογιστή δεν μπορεί να μπει ο οποιοσδήποτε χωρίς να έχει πρόσβαση.

Το πρόβλημα είναι το ίδιο με αυτό μιας κοινής συσκευής αυτόματων συναλλαγών, που δεν είναι παρά ένας υπολογιστής στο δρόμο. Σε αυτήν έχουν πρόσβαση όσοι έχουν την ενδεδειγμένη κάρτα

και ένα προσωπικό κωδικό αριθμό, ώστε να μπορούν να πάρουν χρήματα ή να ζητήσουν διευκολύνσεις.

Η πρόσβαση στους υπολογιστές μπορεί να ελεγχθεί με πολλές μεθόδους πέρα από τις φυσικές. Πολλοί υποστηρίζουν ότι τα τακτικά γραφεία δείχνουν και τακτικό μυαλό. Οι ειδικοί των υπολογιστών είναι εξαιρετικά ανοικοκύρευτοι. Οι προγραμματιστές συνηθίζουν να συσσωρεύουν τις εκτυπώσεις επάνω στα γραφεία τους. Οι λύσεις μεταγλώτισσης βρίσκονται αφύλαχτες σε κάποιο σημείο του γραφείου.

Όλες αυτές οι λίστες περιέχουν πληροφορίες που μπορεί να φανούν χρήσιμες σε κάποιον ανταγωνιστή. Η ελεγχόμενη και ασφαλής καταστροφή των ανεπιθύμητων ή περιττών αντιγράφων των δεδομένων εξόδου δεν πρέπει να υποτιμάται. Τα ακλείδωτα γραφεία μπορεί να έχουν ταινίες, δίσκους ή και κασέτες με πολύτιμα πιθανώς στοιχεία. Η εισαγωγή των υπολογιστών σε ένα γραφείο δεν σημαίνει ότι αχρηστεύει τις κλειδωμένες ντουλάπες.

Σε κάθε λειτουργία του υπολογιστή οι επόπτες πρέπει να εποπτεύουν και όχι να χειρίζονται τις συσκευές. Οι επόπτες αποτελούν το πρώτο επίπεδο διοίκησης και πρέπει να αντιμετωπίζονται κατ' αυτόν τον τρόπο.

Αυτός που ελέγχει τα δεδομένα εισόδου δεν πρέπει να ελέγχει τη λειτουργία και τα δεδομένα εξόδου του ιδίου του υπολογιστικού πακέτου. Οι εργασίες αυτές πρέπει να προγραμματίζονται, να εκτελούνται και να ολοκληρώνονται ως τρεις αυτόνομες και διακριτές λειτουργίες.

Κάποιος που ελέγχει την είσοδο δεδομένων, την επεξεργασία και την διεκπεραίωση και συγχρόνως χειρίζεται τις συσκευές, βρίσκεται στην ιδανική θέση να διαπράξει κάποια απάτη με υπολογιστή ή να χρησιμοποιήσει το υπολογιστικό σύστημα για προσωπικές του υποθέσεις.

ΕΝΔΕΙΞΕΙΣ ΠΙΘΑΝΗΣ ΑΠΑΤΗΣ

Τμήμα χρηστών:

- Μη ισοσκελισμένα λογιστικά βιβλία.
- Λανθασμένο κλείσιμο λογιστικών βιβλίων.
- Καθυστέρηση του συμψηφισμού εκκρεμών τρεχούμενων λογαριασμών.
- Μη ισοσκελισμένη κίνηση λογαριασμού προμηθευτών.
- Υπερβολικές διαγραφές.
- Κακός καταμερισμός καθηκόντων.
- Έλλειψη επίβλεψης.
- Έλλειψη επιτόπιων ελέγχων.

Στην αίθουσα υπολογιστών:

- Μη ελεγχόμενη πρόσβαση.
- Ελλειπής τεκμηρίωση.
- Ακατάστατες λειτουργίες.
- Ανεπαρκής τήρηση εφεδρικών αντιγράφων.
- Έλλειψη ελέγχων.
- Κακός καταμερισμός καθηκόντων.

ΔΙΑΚΟΠΗ ΠΑΡΟΧΗΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ

Η ενδεχόμενη απειλή κατά των υπολογιστικών συστημάτων λόγω απάτης παραμένει πάντα υπαρκτή. Όμως ίσως να είναι πιθανότερες οι απειλές από άλλες αιτίες. Με αυτή την έννοια η απάτη

με υπολογιστή και η διασφάλιση του υπολογιστή αλληλο-επικαλύπτονται.

Οι πιθανές αιτίες διακοπής ενός υπολογιστή εμπίπτουν σε δύο κατηγορίες : στους τυχαίους κινδύνους και στους κινδύνους εκ προθέσεως. Οι τυχαίοι κίνδυνοι περιλαμβάνουν την πυρκαγιά, την πλημμύρα, τον κεραυνό, το ανθρώπινο σφάλμα και την βλάβη κάποιας μονάδας του συστήματος. Οι κίνδυνοι εκ προθέσεως αναφέρονται στην απάτη, στην κατάχρηση, τον εμπρησμό, την κλοπή και την δόλια πρόκληση ζημίας. Και στις δύο περιπτώσεις κινδύνων, την προμελετημένη και την τυχαία, εμπλέκεται συνήθως και ο ανθρώπινος παράγοντας.

Το ανθρώπινο σφάλμα ή η προμελετημένη ενέργεια μπορεί να προέρχεται από εργαζόμενους, από εξουσιοδοτημένους επισκέπτες ή ακόμα και από μη εξουσιοδοτημένους παρείσακτους.

Η διακοπή των υπηρεσιών μπορεί να προκληθεί από κάποια προσωρινή αναστολή μιας λειτουργίας, από την κοινολόγηση πληροφοριών ή από την αλλοίωση, αφαίρεση ή και την καταστροφή των δεδομένων.

Πιο κάτω παραθέτουμε σε ένα πίνακα την τυπική εκατοστιαία κατανομή χαρακτηριστικών επεισοδίων που συνέβησαν σε υπολογιστικές εγκαταστάσεις ανά κατηγορία επεισοδίου και ανά βαθμό σοβαρότητας.

Αξίζει να τονισθεί ο τρόπος σκέψης του διευθυντικού προσωπικού των υπολογιστικών κέντρων. Το ότι οι ζημιές λόγω δόλιας καταστρεπτικής ενέργειας, κλοπής και απάτης δεν φαίνεται να είναι ιδιαίτερα σημαντικές, ίσως σημαίνει ότι τα επεισόδια παραμένουν ανεξερεύνητα ή δεν αποκαλύπτονται. Αυτό είναι ένα πρόβλημα γενικότερης προοπτικής για την διεύθυνση της επιχείρησης.

ΠΙΝΑΚΑΣ ΕΚΑΤΟΣΤΙΑΙΑΣ ΚΑΤΑΝΟΜΗΣ ΕΠΕΙΣΟΔΙΩΝ ΣΕ ΧΩΡΟ ΥΠΟΛΟΓΙΣΤΩΝ

ΑΙΤΙΑ ΕΠΕΙΣΟΔΙΟΥ	ΜΗ ΣΟΒΑΡΟ ΕΠΕΙΣΟΔΙΟ	ΣΧΕΤΙΚΑ ΣΟΒΑΡΟ	ΣΟΒΑΡΟΤΑΤΟ
- Βλάβη υλικού	10%	80%	10%
- Ανθρώπινο σφάλμα	8%	82%	10%
- Σφάλμα λογισμικού	10%	86%	4%
- Σφάλμα επικοινωνιών	40%	52%	8%
- Πτώση τάσης	8%	90%	2%
- Πυρκαγιά - πλημμύρα	90%	9%	1%
- Δόλια πρόκληση ζημιάς	99%	1%	-
- Κλοπή και απάτη	99%	1%	-

Το δίλημμα βρίσκεται στο σημείο αυτό, γιατί η πλειονότητα των διευθυντών των επιχειρήσεων, αν και γνωρίζουν πως το προσωπικό τους δεν είναι απόλυτα έντιμο, δεν δείχνουν να ενδιαφέρονται γιατί πιστεύουν πως τα υπολογιστικά συστήματα είναι απόλυτα ασφαλή. Από την άλλη μεριά οι ειδικοί των υπολογιστών στον ίδιο τον οργανισμό γνωρίζουν πως κάθε υπολογιστικό σύστημα είναι τρωτό, αλλά δεν αντιλαμβάνονται πως υπάρχουν άνθρωποι ανέντιμοι μιας και δεν έχουν εμπειρία σε τέτοια προβλήματα.

Οι απειλές εναντίον ενός υπολογιστικού συστήματος πρέπει να αντιμετωπίζονται ρεαλιστικά. Η άγνοια μπορεί να αποδειχθεί ευδαιμονία αλλά είναι ίσως και απερισκεψία σε αυτό το ανταγωνιστικό εμπορικό κλίμα.

Η έλλειψη φροντίδας ενθαρρύνει την απάτη. Πάντα μπορούν να ληφθούν κάποια πρακτικά μέτρα, μερικά από τα οποία δεν είναι "απόκοσμα" που θα μειώσουν τις πιθανότητες. Π.χ. πρέπει να γίνεται με ασφαλή τρόπο η διάθεση χαρτιών, άχρηστων χαρτιών, όπως θα δούμε παρακάτω.

ΑΧΡΗΣΤΑ ΧΑΡΤΙΑ - ΔΙΑΘΕΣΗ

Η εισαγωγή της νέας τεχνολογίας συχνά αύξησε την ποσότητα του παραγόμενου χαρτιού στα γραφεία, παρόλες τις αντίθετες προβλέψεις. Επί αιώνες τα χειρόγραφα ή τα τυπωμένα χαρτιά αποτελούν τα αποδεκτά μέσα της επίσημης επικοινωνίας.

Οι τηλεφωνικές συσκευές ή οι συμφωνίες γίνονταν σε συναντήσεις επιτροπών και επικυρώνονταν με γραπτά κείμενα πριν καταστούν δεσμευτικές. Η υπογραφή σε ένα επίσημο έγγραφο αποτελεί δέσμευση για μία σειρά ενεργειών. Είναι πολύ δύσκολο να σταματήσει κάποιος αυτή την παράδοση. Με ένα λεκτικό επεξεργαστή είναι εύκολο να τυπώσεις το προσχέδιο ενός επίσημου εγγράφου, να το αλλάξεις και να το ξανατυπώσεις με τις διορθώσεις στην κατάλληλη θέση.

Το αρχικό προσχέδιο παύει να είναι χρήσιμο και άρα είναι πια ανεπιθύμητο.

Πρέπει λοιπόν να υπάρχουν διαδικασίες στα γραφεία για τη διάθεση των άχρηστων ή των διπλών αντιγράφων και πιο συγκεκριμένα των εγγράφων εκείνων που περιέχουν εμπιστευτικές ή ευαίσθητες πληροφορίες. Πρόσθετη φροντίδα πρέπει να λαμβάνεται για τα έγγραφα εκείνα που περιέχουν προσωπικές πληροφορίες ή προσωπικά στοιχεία των εργαζομένων και των πελατών. Η διάθεση

των άχρηστων εγγράφων αποτελεί μία σημαντική ενέργεια, μπορεί να γίνε με διάφορους τρόπους και να πάρει μία από τις πιο κάτω μορφές :

Η πιο συνηθισμένη μορφή διάθεσης των άχρηστων εγγράφων είναι η συλλογή τους από εξειδικευμένες εταιρίες.

Μία τέτοια εταιρία μπορεί να αφήνει ένα κάδο μέσα στα γραφεία της επιχείρησης για να τον γεμίζουν με άχρηστα χαρτιά και η εταιρία θα τον αδειάζει σε τακτά χρονικά διαστήματα.

Η αποκομιδή μπορεί να συμφωνηθεί σε ημερήσια, εβδομαδιαία ή και σε μηνιαία βάση, ανάλογα με τον όγκο των χαρτιών.

Υπάρχουν εξειδικευμένες εταιρίες που εμπορεύονται ή και επεξεργάζονται τα άχρηστα χαρτιά.

Μία άλλη μορφή έχει να κάνει με τους εμπόρους χαρτιού, οι οποίοι μπορεί να πληρώσουν πολλά για να πάρουν το χαρτί, ειδικότερα εάν αυτό είναι συγκεκριμένης και αποδεκτής ποιότητας και φυσικά σε μεγάλη ποσότητα. Βέβαια πάνω απ' όλα μετράει η ασφαλής διάθεση του χαρτιού, γι' αυτό οι έμποροι πρέπει να ελέγχονται για την ακεραιότητα και την αξιοπιστία τους, όταν πρόκειται να τους διαθέσουμε εμπιστευτικά έγγραφα.

Εύκολα αυτοί θα μπορούσαν να μας δώσουν ονόματα άλλων πελατών με τους οποίους συνεργάζονται και τους εξυπηρετούν.

Το καλύτερο όμως που θα μπορούσαμε να κάνουμε για να είμαστε σίγουρα ασφαλείς θα ήταν να καταστρέψουμε το χαρτί πριν το δώσουμε σε οποιονδήποτε έμπορο, αφού αυτόν δεν τον απασχολεί αν θα είναι ή όχι το χαρτί τεμαχισμένο. Οι έμποροι άλλωστε το χαρτί αυτό το προορίζουν για πολτοποίηση.

Υπάρχουν διάφοροι τύπου "καταστροφέων εγγράφων". Ποικίλουν από μικρά επιτραπέζια μοντέλα γραφείου πολύ εύχρηστα, μέχρι μηχανές μεγάλες για να καταστρέφουν ποσότητες χαρτιού.

Η καταστροφή των εγγράφων μπορεί να αποτελέσει αυτοχρηματοδοτούμενη λειτουργία, αν και είναι πιθανό να υπάρξουν διάφορα προβλήματα όπως οι μειωμένες δυνατότητες καταστροφής, το απαιτούμενο προσωπικό και οι δυσκολίες για την αποθήκευση του τεμαχισμένου χαρτιού.

Οι "καταστροφείς εγγράφων" απαιτούν τακτική συντήρηση έστω και σε πολύ αραιά διαστήματα. Η καταστροφή των χαρτιών θα αποτελέσει παραδεκτή λύση μόνο αφού υπολογιστεί το κόστος της λειτουργίας. Τα τεμαχισμένα χαρτιά μπορεί να καταλάβουν χώρο δέκα με δεκαπέντε φορές μεγαλύτερο απ' ότι τα πρωτότυπα έγγραφα.

Μπορεί λοιπόν κάποια εταιρία να αγοράσει μηχανές δεματιάσματος ή να δημιουργήσει ειδικούς χώρους και κλίβανους για να βάλει εκεί τα χαρτιά που προορίζονται για καύση.

Αναφέραμε λοιπόν μερικά από τα "εφικτά μέτρα" για την προφύλαξη από την απάτη, τα οποία δεν είναι κατ' ανάγκη υψηλού τεχνικού επιπέδου, αλλά όταν λαμβάνονται καθιστούν την τέλεση της απάτης ακόμα πιο δύσκολη και αδύνατη.

ΚΕΦΑΛΑΙΟ 4ο

ΤΟ ΦΑΙΝΟΜΕΝΟ ΤΗΣ ΕΙΣΒΟΛΗΣ

Ο ΕΙΣΒΟΛΕΑΣ ΣΤΟ ΧΩΡΟ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Η ανάπτυξη των υπηρεσιών που βασίζονται στους υπολογιστές συνοδεύθηκε από την εμφάνιση ενός πλήθους αδικημάτων που συνδέονται με αυτούς.

Συχνά τα αδικήματα που διαπράττονται είναι τα παραδοσιακά και ο υπολογιστής είναι απλώς ένα μέσο διευκόλυνσης, εντελώς συμπτωματικό.

Τα σημερινά ηλεκτρονικά συστήματα έχουν προσδώσει στην απάτη μία νέα διάσταση. Ορισμένες μορφές παρανόμων δραστηριοτήτων που συνδέονται με υπολογιστές παίρνουν μεγάλη δημοσιότητα, τόσο στα τεχνικά έντυπα όσο και στα έντυπα ποικίλης ύλης.

Υπάρχουν βέβαια και περιπτώσεις που σπάνια βλέπουν το φως της δημοσιότητας. Είναι προφανές ότι ο όρος "εισβολέας" σημαίνει διαφορετικά πράγματα για διαφορετικούς ανθρώπους. Μερικές φορές δεν υποδηλώνει παρά τον ασυγκράτητο προγραμματιστή που είναι έτοιμος να αναλώσει ακόμα και το χρόνο του ύπνου του για να δουλέψει με τη μηχανή, να καλύψει κάποιο κενό ή κάποια "ατέλεια". Αυτές οι δραστηριότητες δεν είναι απαραίτητα απαγορευμένες ή παράνομες.

Κατά μία άλλη έννοια όμως η εισβολή υποδηλώνει μία αξιόποινη πράξη, την επιδέξεια χρησιμοποίηση του υπολογιστή για την διάπραξη πράξεων διαφόρων ειδών.

Το φαινόμενο της εισβολής έχει πάντα ψυχολογικό ενδιαφέρον, αλλά δεν εμπίπτει πάντα στην αρμοδιότητα του νόμου.

Ο ασυγκράτητος προγραμματιστής υπάρχει εδώ και σαράντα χρόνια σε όλη την ιστορία των ηλεκτρονικών υπολογιστών.

Τα τελευταία δέκα χρόνια όμως το φαινόμενο προκάλεσε το αυξημένο ενδιαφέρον των ψυχολόγων, των νομοθετών και άλλων επιστημόνων. Το 1976 ο Joseph Weizenbaum καθηγητής στο MIT, αλλά περισσότερο γνωστός ως ο δημιουργός του προγράμματος "ΕΛΙΖΑ" (πρόγραμμα που έγραψε για να δείξει πόσο εύκολο είναι σε έναν υπολογιστή να δώσει την εντύπωση "σκεπτόμενης μηχανής"). Το πρόγραμμα εξομοίωσε την συνομιλία ανάμεσα σε ένα Ψυχοθεραπευτή και τον ασθενή του. Και φέρει το όνομα της Elisa Dolittle (από το έργο "Πυγμαλίων"). Τράβηξε την προσοχή μας σε μία "διανοητική ανωμαλία" που τώρα εμφανίζεται μετασχηματισμένη λόγω του υπολογιστή. Περιέγραψε προγραμματιστές υπολογιστικών κέντρων που γνώριζε προσωπικά, σημειώνοντας ότι ήταν "έξυπνοι νέοι, με ατημέλητη εμφάνιση και συνήθως με κόκκινα κομμένα μάτια".

Συνέχεια μπροστά σε ένα πληκτρολόγιο με την προσοχή τους καρφωμένη, που φαίνονταν αδιάφοροι για την εμφάνιση και την αφηρημάδα τους "υπάρχουν μόνο μέσω των υπολογιστών και γι' αυτούς".

Ο Weizenbaum αποκαλεί την κατάσταση Ψυχοπαθολογική. Οι άνθρωποι σιγά - σιγά εθίζονται, αρχίζουν κατά κάποιο τρόπο να συμπεριφέρονται σαν μανιακοί, αρνούνται να φάνε, αρνούνται και την παρέα των κοριτσιών τους.

Υπάρχει μία έξις, ένας εξαναγκασμός που κάνει τους εισβολείς να θεωρούν κάθε υπολογιστικό σύστημα ως πρόκληση, ως σύστημα που πρέπει να ελεγχθεί, να εξερευνηθεί.

Ήδη έχουν εμφανισθεί εισβολείς που αγωνίζονται να μπουν σε "κλειστά" υπολογιστικά συστήματα όχι για να αποκομίσουν χρηματικά οφέλη, αλλά απλώς ως "πνευματική άσκηση", για να βελτιώσουν τις προγραμματικές τους ικανότητες.

Οι διευθυντές και όλα τα λοιπά στελέχη που αγωνίζονται για να προστατεύσουν τις εμπιστευτικές πληροφορίες, τις χρηματικές καταθέσεις αλλά και τα λοιπά πολύτιμα αγαθά της εταιρίας τους, είναι φυσικά εντελώς αντίθετοι με τις πρωτοβουλίες των εισβολέων.

Η αντικοινωνική φύση του φαινομένου της εισβολής συζητείται όλο και περισσότερο. Παλιότερα σύνηθεις εισβολείς οι άνθρωποι που εγκατέλειπαν το σχολείο ή άλλαζαν επάγγελμα.

Κάποιοι απ' αυτούς μπήκαν στο Τεχνολογικό Ινστιτούτο της Μασαχουσέτης και άρχισαν το πρόγραμμα MAC (Multiple Access Computers = Υπολογιστές Πολλαπλής Προσπέλασης) που στόχευε στην ανάπτυξη της ιδέας του διαμερισμικού χρόνου.

Παρακινούμενοι από το σκοπό να ελέγξουν τους υπολογιστές πολλών χρηστών μέχρι και τα όριά τους, απέκτησαν γνώσεις που αποτελούσαν τη βάση των προσπαθειών των μελλοντικών εισβολέων.

Το φαινόμενο της εισβολής τα τελευταία χρόνια έχει τύχει ευρείας δημοσιότητας με διάφορους τρόπους.

Με την κινηματογραφική ταινία "War Games" γίνανε γνωστές στο ευρύ κοινό δραστηριότητες που ήταν ήδη γνωστές στους θαυμαστές των υπολογιστών.

Στην ταινία αυτή ένας μαθητής του Γυμνασίου χρησιμοποιεί το μικροϋπολογιστή του και ένα διαμορφωτή / αποδιαμορφωτή για να μπει στα μηχανογραφημένα αρχεία του σχολείου και να αλλάξει τους

βαθμούς των εξετάσεών του. Αργότερα, και εδώ το πρόβλημα γίνεται πιο ανησυχητικό, βρίσκει το "κλειδί" ενός στρατιωτικού αμυντικού συστήματος και τρέχει μια προσομοίωση (Simulation) ενός πολεμικού παιχνιδιού, που εκλαμβάνεται από το σύστημα ως πραγματική διεθνής κρίση. Πολλοί ειδικοί των υπολογιστών επιδοκίμασαν την ταινία, θεωρώντας την ως ένα τελείως ρεαλιστικό σενάριο.

Είναι ενδιαφέρον ότι οι σεναριογράφοι Walter Parkes και Larry Lasker ερεύνησαν τις εγκαταστάσεις των στρατηγικών πυρηνικών όπλων των Η.Π.Α. επί δύο χρόνια πριν αρχίσουν το "War Games". Ο Parkers συγκεκριμένα είπε: "Δεν ξέραμε όταν ξεκινούσαμε ότι η ταινία θα είχε αντιπυρηνικό θέμα. Θέλεις να πιστεύεις ότι η πυρηνική άμυνα βρίσκεται σε καλά χέρια, όμως όσο πιο πολύ ψάχναμε τόσο ανακαλύπταμε ότι τίποτα δεν ελέγχεται".

Ένας αριθμός πραγματικών γεγονότων έρχεται να υπογραμμίσει την αληθοφάνεια του φανταστικού σεναρίου του "War Games".

Το 1984 δύο νεαροί εισβολείς κατάφεραν να "μπουν" στο μυστικό δίκτυο υπολογιστών ARRA, που χρησιμοποιείται για την ηλεκτρονική ανταλλαγή δεδομένων της "Υπηρεσίας Προηγμένων Ερευνητικών Προγραμμάτων του Πενταγώνου" (Advanced Research Projects Agency). Το γεγονός αυτό είχε ως αποτέλεσμα μία ηλεκτρονική καταδίωξη σε όλη την αμερικανική ήπειρο που κατέληξε στην Υπηρεσία Τηλεπικοινωνιών της Νορβηγίας, αφού πέρασε από το NORAD, το επιτελείο αντιαεροπορικής άμυνας της Βόρειας Αμερικής, σε ένα υπόγειο οχυρό στην Ομάχα της Νεμπράσκα. Αυτή η (αληθινή) ιστορία είναι σχεδόν όμοια με την πλοκή του "War Games".

Τελικά οι δύο νεαροί από το Λος Άντζελες, ο Kevin Poulsen και ο Ron Austin, συνελήφθησαν στα σπίτια τους από έξι οπλισμένους αξιωματικούς. Είχαν καταφέρει να "σπάσουν" το τεράστιο απόρρητο

δίκτυο χρησιμοποιώντας δύο μικροϋπολογιστές (Vic-20 και TRS-80) που δεν κόστιζαν πάνω από 50.000 δρχ.

Το φαινόμενο της εισβολής πήρε ιδιαίτερη δημοσιότητα μέσα από τις συνεχείς περιπτώσεις απάτης που πραγματοποιούνται τα τελευταία χρόνια.

Είναι γεγονός ότι σήμερα η εισβολή αποτελεί ένα πολυσύνθετο φαινόμενο. Μπορεί να προκαλείται από ψυχολογική παρόρμηση ή να είναι μέσο ικανοποίησης μιας πνευματικής έπαρσης.

Μπορεί επίσης να αποτελεί μια προμελετημένη απόπειρα εξαπάτησης ή ένα μέσο συσσώρευσης πλούτου ή ισχύος.

Γι' αυτό συγκεντρώνει το αυξημένο ενδιαφέρον διευθυντών και άλλων στελεχών επιφορτισμένων με τη διαφύλαξη της ασφάλειας των συστημάτων που βασίζονται στους υπολογιστές.

ΤΕΧΝΙΚΕΣ ΕΙΣΒΟΛΕΩΝ

Για να μπεις σε ένα σύστημα, πέρα από το καθιερωμένο δίκτυο ή πρέπει να έχεις σύνδεση μέσω επιλεγμένης γραμμής ή να είσαι συνδεδεμένος με το δίκτυο PSS της British Telecom.

- *Συνδέσεις μέσω επιλεγόμενης γραμμής :* Ορισμένα συστήματα διαθέτουν τη δυνατότητα σύνδεσης μέσω επιλεγόμενης γραμμής (dial - in line) που προσφέρεται για την ευκαιριακή σύνδεση από απομακρυσμένα σημεία. Επίσης συχνά κάποιοι εργαζόμενοι επιθυμούν να συνδεθούν, μέσω επιλεγόμενης γραμμής, με το κεντρικό σύστημα της εταιρίας τους, από διαφορετικά σημεία, εκτός του καθιερωμένου δικτύου της. Π.χ. πωλητές που επιθυμούν να συνδεθούν με το σύστημα από τα γραφεία ενός πελάτη. Ακόμα και οι εγκαταστάσεις που δεν έχουν τη δυνατότητα σύνδεσης μέσω

επιλεγόμενης γραμμής, μπορεί να έχουν επιλεγόμενες γραμμές ως εφεδρικές των μισθωμένων μόνιμων γραμμών τους.

Σε περίπτωση που η μισθωμένη γραμμή τεθεί εκτός λειτουργίας, τότε η επιλεγόμενη γραμμή μπορεί να χρησιμοποιηθεί προσωρινά ως εφεδρική.

Υπάρχουν και διάφοροι άλλοι λόγοι που κάνουν αναγκαία την ύπαρξη επιλεγόμενης τηλεφωνικής γραμμής. Συχνά στα μεγάλα συστήματα, το τεχνικό προσωπικό της κατασκευάστριας εταιρίας μπορεί να καλεί μέσω των επιλεγόμενων τηλεφωνικών συνδέσεων και να εξετάζει τα διαγνωστικά και στατιστικά στοιχεία που αυτόματα συγκεντρώνει η μηχανή.

Μπορεί ακόμα και να προχωράει σε αλλαγές στο λογισμικό του συστήματος. Η συντήρηση του συστήματος από απόσταση αποτελεί κίνδυνο για την ασφάλεια. Ο ελεγκτής ή ο προϊστάμενος ασφαλείας πρέπει να ενημερώνεται για το γεγονός και να εξετάζει τις τυχόν επιπτώσεις. Π.χ. πόσο καθησυχαστικές είναι οι διαβεβαιώσεις της κατασκευάστριας εταιρίας για την εντιμότητα του προσωπικού της ;

- Μπορούν οι δίσκοι με τα εμπιστευτικά δεδομένα να αποσυνδεθούν από το σύστημα, κατά την διάρκεια της συντήρησης από απόσταση ;
- Μετά την ολοκλήρωση της συντήρησης, πρέπει το λειτουργικό σύστημα να ξαναφορτωθεί από το εφεδρικό, για την περίπτωση που έχουν εισαχθεί μη εγκεκριμένες αλλαγές ;
- Πόσο αποτελεσματικοί είναι οι περιορισμοί που βάζει το λογισμικό, όσον αφορά το σκοπό και τον τύπο της πρόσβασης που πραγματοποιεί στο σύστημα το τεχνικό προσωπικό του κατασκευαστή ;

Είτε χρησιμοποιείται η επιλεγόμενη τηλεφωνική σύνδεση ως εφεδρική, είτε χρησιμοποιείται για συντήρηση από απόσταση, είναι σημαντικό οι γραμμές που έχουν προσπέλαση στον υπολογιστή να

μην μένουν σε μόνιμη βάση ανοιχτές. Είναι προτιμότερο να υπάρχει χειροκίνητη σύνδεση, όταν απαιτείται η προσπέλαση στον κεντρικό υπολογιστή. Ο ενδιαφερόμενος συνήθως υποχρεούται να μιλήσει με το τμήμα ελέγχου του δικτύου και να δώσει το συνθηματικό του.

Τότε το τμήμα ελέγχου του δικτύου ξανατηλεφωνεί στον ενδιαφερόμενο ή στο απομακρυσμένο σημείο, σε ένα προκαθορισμένο αριθμό και τότε μόνο επιτρέπεται η σύνδεση στον υπολογιστή. Στη συνέχεια ο ενδιαφερόμενος πρέπει να προχωρήσει στις ενέργειες ζητώντας να υπογράψει στον υπολογιστή.

Συχνά όμως για επιχειρηματικούς λόγους, είναι ανάγκη και επιτρέπεται να συνδεθούν στον υπολογιστή τόσο πολλοί μέσω της επιλεγόμενης τηλεφωνικής γραμμής, έτσι που η σύνδεση δεν είναι δυνατόν να στηρίζεται σε χειροκίνητους διακόπτες.

Οι συσκευές που έχουν την δυνατότητα να ξανακαλέσουν τον "αιτούντα σύνδεσης" κυκλοφορούν όλο και περισσότερο, με σκοπό να βοηθήσουν τον έλεγχο των συνδέσεων στα συστήματα αυτού του τύπου.

Η συσκευή αυτή τοποθετείται στο χώρο όπου βρίσκεται ο υπολογιστής, δέχεται μηνύματα εισόδου, αντιπαραβάλλει συχνά τα συνθηματικά με συνθηματικά που περιέχονται σε καταλόγους στην μνήμη της και ξανατηλεφωνεί σε προκαθορισμένο νούμερο, το οποίο αντιστοιχεί και στον "αιτούντα" και βρίσκεται αποθηκευμένο σε έναν πίνακα στη μνήμη της συσκευής, ώστε να επιβεβαιώσει ότι το τηλεφώνημα έγινε από εξουσιοδοτημένο αριθμό.

Προφανώς οι συσκευές αυτές μπορούν να χρησιμοποιηθούν μόνο όταν ο χρήστης καλεί από ένα προκαθορισμένο νούμερο, το οποίο υπάρχει στο πρόγραμμα του συστήματος.

Εάν δεν είναι τέτοια η περίπτωση τότε ο έλεγχος των συνθηματικών γίνεται μέσω του λογισμικού.

- *Δίκτυο PSS :* Το δίκτυο PSS (Packet Switch - Stream). Το Βρετανικό δημόσιο δίκτυο μετάδοσης και μεταγωγής δεδομένων αποτελεί μια εξειδικευμένη υπηρεσία μετάδοσης δεδομένων.

  Για την χρησιμοποιήση του δικτύου PSS απαιτείται ένας αριθμός ταυτότητας χρήστη του δικτύου τον οποίο χρησιμοποιεί το PSS για τη χρήση των εξόδων χρήσης του δικτύου.

  Είναι επίσης απαραίτητη η διεύθυνση χρήστη του δικτύου του σημείου στο οποίο ζητείται η προσπέλαση. Οι διευθύνσεις των χρηστών του δικτύου δημοσιεύονται στον κατάλογο του PSS.

  'Ενας επίδοξος εισβολέας μπορεί κάλλιστα να τηλεφωνήσει σε έναν τοπικό σταθμό συναρμολογητή / αποσυναρμολογητή πακέτων μηνυμάτων για το κοινό, σε σκοπό την πρόσβαση στο σύστημα PSS .

  Στην συνέχεια δίνει το δικό του ή έναν κλεμμένο αριθμό ταυτότητας χρήστη του δικτύου (NUS) και ακολούθως δίνει τη διεύθυνση χρήστη του δικτύου (NUA) του συστήματος στο οποίο θέλει να μπει. Κατόπιν ο εισβολέας απλώς χρειάζεται να ζητήσει σύνδεση με τον υπολογιστή, με το συνήθη τρόπο, δίνοντας δηλαδή τον αριθμό ταυτότητας ενός χρήστη, του συνθήματος και ένα συνθηματικό. 'Ενας συνεχώς αυξανόμενος αριθμός υπολογιστών συνδέεται στο σύστημα PSS και άρα καθίσταται υποψήφιο θύμα πιθανής εισβολής.

ΤΕΧΝΙΚΕΣ ΑΠΑΤΗΣ

Η συνεχώς εξαπλούμενη απάτη με υπολογιστές δημιούργησε και την δική της "αργκό". Παραθέτουμε πιο κάτω μια λίστα με τα πιο ενδεικτικά παραδείγματα :

- *Η λογική βόμβα (Login bomb):* Η λογική βόμβα είναι παρόμοια με την ωρολογιακή βόμβα, με τη μόνη διαφορά ότι ο χρήστης για να

ενεργοποιήσει το αδίκημά του, χρησιμοποιεί το συνδυασμό κάποιων γεγονότων αντί του ρολογιού του υπολογιστή.

- *Η έμμεση διείσδυση :* Η τεχνική αυτή συνίσταται στην παγίδευση της γραμμής επικοινωνίας ενός νόμιμου χρήστη του δικτύου και στη χρήση των συνθηματικών του για την πρόσβαση στον υπολογιστή του.
- *Το σαλάμι :* Η τεχνική αυτή είναι από τις περισσότερο κοινές για την εξαπάτηση ενός συστήματος. Ο προγραμματιστής ενός οικονομικού οργανισμού (εταιρίας, τράπεζας κ.λ.π.) τροποποιεί ένα πρόγραμμα, ώστε να στρογγυλοποιεί τις συναλλαγές προς τα κάτω, μεταφέροντας τις διαφορές στο λογαριασμό του.
- *Η ωρολογιακή βόμβα :* Η τεχνική αυτή είναι χρήσιμη, όταν ο ένοχος δεν θέλει να είναι παρών ενώ διαπράττεται το αδίκημα. Το ρολόϊ του συστήματος χρησιμοποιείται για να ενεργοποιήσει το πρόγρμμα το οποίο διαπράττει την απάτη, ενώ ο ένοχος είναι απών.
- *Παραποίηση δεδομένων :* Με τη μέθοδο αυτή κάποια δεδομένα μεταβάλλονται αποφέροντας οφέλη στο δράστη.
- *Ο Δούρειος Ίππος :* Η παρεμβολή ενός τμήματος κώδικα σε ένα πρόγραμμα, με τόπο που να μην είναι προφανής.
- *Καταστροφή προγράμματος (Zapping) :* Η τεχνική αυτή συνίσταται στην καταστροφή κάποιου προγράμματος

ΠΩΣ ΑΝΑΚΑΛΥΠΤΟΝΤΑΙ ΟΙ ΑΡΙΘΜΟΙ ΚΛΗΣΗΣ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ

Ο εισβολέας πριν προσπαθήσει να μπει στο σύστημα πρέπει να έχει έναν τηλεφωνικό αριθμό για την επιλογή του συστήματος. Αυτό είναι ευκολότερο απ' όσο αρχικά φαίνεται.

Μπορεί π.χ. να τηλεφωνήσει στο τμήμα υπολογιστών της εταιρίας (ο αριθμός υπάρχει στον τηλεφωνικό κατάλογο), προσποιούμενος ότι είναι ένας "χρήστης σε σύγχυση" και να ζητήσει τον αριθμό για την επιλογή του συστήματος. Μάλιστα ορισμένες εταιρίες κυκλοφορούν τους αριθμούς επιλογής σε ευρύ κύκλο μέσα στην εταιρία, διακινδυνεύοντας έτσι από τους πιθανούς εισβολείς, τους υπαλλήλους, τους πρώην υπαλλήλους ή τους συνεργάτες τους. Ένας άλλος τρόπος επιτυχούς προσπέλασης είναι η χρήση μιας συσκευής που ονομάζεται αυτόματος επιλογέας.

Στην ουσία ο εισβολέας προγραμματίζει το μικροϋπολογιστή του να ζητάει απ' τον αυτόματο επιλογέα να καλεί μια σειρά από τηλεφωνικούς αριθμούς. Εάν θέλει να μπει σε συγκεκριμένο υπολογιστή μπορεί να περιορίσει την έρευνά του σε ένα σύνολο αριθμών που χρησιμοποιείται στο τηλεφωνικό κέντρο της περιοχής στην οποία βρίσκεται ο υπολογιστής, με την προϋπόθεση βέβαια ότι ο υπολογιστής είναι συνδεδεμένος με το τοπικό τηλεφωνικό κέντρο. Όταν μία γραμμή δεδομένων είναι κατειλημμένη, τότε το σύστημα καταγράφει τον αριθμό της και δοκιμάζει τον επόμενο.

Όταν βρεθεί ο τηλεφωνικός αριθμός από έναν εισβολέα αμέσως διαδίδεται σε όλη την "κοινότητα εισβολέων". Οι εισβολείς συχνά είναι μέλη επίσημων συλλόγων και λεσχών και ανταλλάσουν τηλεφωνικούς αριθμούς και συνθηματικά. Ένας τρόπος για την μεταξύ τους επικοινωνία είναι μέσω των ηλεκτρονικών πινάκων ανακοινώσεων. Ο πίνακας αυτός είναι η ηλεκτρονική έκδοση ενός ειδησεογραφικού δελτίου μιας λέσχης. Ουσιαστικά πρόκειται για ένα μικροϋπολογιστή που συνδέεται με το τηλέφωνο, μέσω ενός διαμορφωτή / αποδιαμορφωτή (modem) αυτόματης απόκρισης.

Οι "αναγνώστες" έχουν προσπέλαση στον πίνακα ανακοινώσεων, μέσω των μικροϋπολογιστών τους και μπορούν να διαβάσουν κάθε πληροφορία που περιέχει ή να αφήσουν κάποια μηνύματα κ.λ.π.

Το κόστος της δημιουργίας ενός ηλεκτρονικού πίνακα ανακοινώσεων είναι ουσιαστικά το κόστος αγοράς ενός μικροϋπολογιστή και ενός διαμορφωτή / αποδιαμορφωτή αυτόματης απόκρισης και βέβαια το κόστος ενοικίασης μιας τηλεφωνικής γραμμής. Καθένας που καλεί τον πίνακα ανακοινώσεων υποβάλλεται στη δαπάνη της τηλεφωνικής κλήσης.

Μόλις οι εισβολείς ανακαλύψουν απόρρητες πληροφορίες μιας εγκατάστασης όπως π.χ. τηλεφωνικούς αριθμούς, ταυτότητες χρηστών, συνθηματικά κ.λ.π., μπορούν να τις αφήσουν στον πίνακα ανακοινώσεων στη διάθεση των υπολοίπων της ομάδας και φυσικά σε βάρος της συγκεκριμένης εγκατάστασης.

ΠΩΣ ΑΝΑΚΑΛΥΠΤΟΝΤΑΙ ΟΙ ΤΑΥΤΟΤΗΤΕΣ ΚΑΙ ΤΑ ΣΥΝΘΗΜΑΤΙΚΑ ΤΩΝ ΧΡΗΣΤΩΝ

Εάν υποθέσουμε ότι ένας εισβολέας καταφέρει να δει στο τερματικό του απάντηση (συνήθως το σήμα της εταιρίας) από τον υπολογιστή στον οποίο προσπαθεί να μπει, πρέπει να πληκτρολογήσει μια αποδεκτή ταυτότητα χρήστη και ένα συνθηματικό. Συχνά δεν είναι ιδιαίτερα δύσκολο να βρεις ένα αριθμό ταυτότητας χρήστη, αφού οι πληροφορίες σαν κι αυτή δεν θεωρούνται γενικά εμπιστευτικές. Αυτό μπορεί να γίνει:

- δοκιμάζοντας τυπικές ταυτότητες χρηστών που μπορεί να υπάρχουν στο σύστημα και δημοσιεύονται στα βιβλία του κατασκευαστή που το περιγράφουν,

- ψάχνοντας στα άχρηστα χαρτιά της εγκατάστασης. Οι αριθμοί ταυτότητας των χρηστών συνήθως τυπώνονται στις λίστες των υπολογιστών,
- με τη μέθοδο των συνεχών δοκιμών. Το σύστημα συχνά δέχεται απεριόριστο αριθμό προσπαθειών, μέχρι να βρεθεί η σωστή ταυτότητα χρήστη, χωρίς να δίνει προειδοποίηση ή να απομονώνει το τερματικό.

Αφού ο εισβολέας καταφέρει να υπογράψει στο σύστημα με την ορθή ταυτότητα χρήστη, χρειάζεται κατόπιν το σωστό συνθηματικό για να μπει σε αυτό. Οι χρήστες πρέπει να μάθουν να χρησιμοποιούν το συνθηματικό τους ως στοιχείο άκρως εμπιστευτικό.

Ως εκ τούτου τα συνθηματικά δεν πρέπει να βρίσκονται εύκολα όπως οι ταυτότητες χρηστών. Όμως άπαξ και ο εισβολέας μάθει με οποιονδήποτε τρόπο ένα συνθηματικό, μπορεί να το ανακοινώσει μέσω του ηλεκτρονικού πίνακα ανακοινώσεων και έτσι να μεταδοθεί αμέσως στους άλλους εισβολείς.

Η πιθανότητα να βρεθεί κάποιο συγκεκριμένο συνθηματικό στον πίνακα ανακοινώσεων είναι μικρή. Όμως αν κάποια μονάδα έχει την ατυχία να βρεθεί η πληροφορία της αυτή δημοσιευμένη, τότε είναι σίγουρο ότι θα υποστεί πλήθος εισβολών.

Εάν δεν υπάρχει στον πίνακα ανακοινώσεων, ο εισβολέας μπορεί να ξαναπροσπαθήσει τηλεφωνώντας στο τμήμα υπολογιστών της εταιρίας, προσποιούμενος ότι είναι ένας χρήστης που ξέχασε το συνθηματικό του. Σε ένα καλο-οργανωμένο σύστημα πρέπει να υπάρχουν οι κατάλληλες διαδικασίες για την αντιμετώπιση αυτών των κλήσεων, όμως σε αρκετές περιπτώσεις θα δοθεί το συνθηματικό στο "χρήστη."

Μια άλλη πιο ανησυχητική μέθοδος εισόδου στο σύστημα είναι με τη χρήση των τυποποιημένων ταυτοτήτων και συνθηματικών.

Τα περισσότερα συστήματα έχουν τυποποιημένες ταυτότητες όπως την ταυτότητα του διευθυντή της εγκατάστασης (SYSMAN, ADMSN ή SPECIAL), του προϊσταμένου χειρισμού (OPS, OPERATIONS κ.λ.π.), καθώς και των μηχανικών, των προγραμματιστών του συστήματος κ.λ.π. Κατά την εγκατάσταση του συστήματος εισάγονται συνήθως αυτές οι τυποποιημένες ταυτότητες μαζί με το αρχικό συνθηματικό (PASSWORD ή μία σειρά από Χ). Όλες αυτές οι πληροφορίες πολλές φορές αναφέρονται στα έντυπα του κατασκευαστή, τα οποία παρέχονται μαζί με το σύστημα ή πωλούνται ανεξάρτητα σε κάθε ενδιαφερόμενο.

Όποιος γνωρίζει τις τυποποιημένες ταυτότητες χρήστη έχει ένα στήριγμα μέσα στο σύστημα. Ακόμα χειρότερα, εάν το τυποποιημένο συνθηματικό δεν αλλάξει, ο δράστης μπορεί να υποβάλλει το συνθηματικό που είναι καταγραμμένο στα εγχειρίδια και να μπει στο σύστημα με το μεγάλο βαθμό εξουσιοδότησης ενός από τους βασικούς χρήστες του συστήματος και όχι ως ένας κοινός χρήστης.

Τέτοιες ταυτότητες χρήστη συνήθως εξασφαλίζουν τον ανώτερο βαθμό εξουσιοδότησης σε σχέση με τους κοινούς χρήστες.

Για παράδειγμα η ταυτότητα χρήστη του διευθυντή της εγκατάστασης συνήθως είναι ιεραρχικά ανώτερη, όσον αφορά την προσπέλαση στο σύστημα και με αυτή μπορεί να αποφύγει ελέγχους συνθηματικών σε πολλά συστήματα και να διαγράψει ή να ενημερώσει αρχεία και άλλες παραμέτρους του συστήματος.

Εάν ο εισβολέας δεν είναι τόσο τυχερός ώστε να βρει ένα σύστημα με τυποποιημένα συνθηματικά, στην επόμενη προσπάθειά του θα δοκιμάσει τα πιο συνηθισμένα, όπως κοινά ονόματα κ.λ.π.

Ένας ειδικός στα συστήματα ασφαλείας των υπολογιστών έχει πει ότι, αν ζητηθεί από τους χρήστες να αλλάζουν το συνθηματικό τους κάθε μήνα, τότε το πιο συνηθισμένο που βρίσκουν οι προγραμματιστές είναι το όνομα της "κοπέλας του μήνα" από το PLAY BOY.

Υπάρχει πάντα και ο κίνδυνος από τις απόπειρες πρόσβασης στο σύστημα με τη μέθοδο των συνεχών δοκιμών. Μια ακραία εκδοχή αυτής της μεθόδου είναι να γραφτεί ένα πρόγραμμα το οποίο παράγει όλους τους δυνατούς συνδυασμούς αλφαριθμητικών χαρακτήρων, μέχρις ότου υποβληθεί στο σύστημα ο γνωστός συνδυασμός. Για την αντιμετώπιση αυτής της μεθόδου μπορούν να εφαρμοστούν αρκετοί τύποι ελέγχου. Πρώτος τρόπος το συνθηματικό να είναι αρκετά μεγάλο. Τότε ο χρόνος που θα απαιτηθεί για να επιχειρηθούν όλοι αυτοί οι δυνατοί συνδυασμοί, είναι τεράστιος. 'Ενα συνθηματικό με 8 αλφαριθμητικούς χαρακτήρες για παράδειγμα δίνει 36 (26 γράμματα και 10 αριθμοί) εις την όγδοη δυνατά συνθηματικά. Αυτό σημαίνει περίπου 2.820.000.000.000. Ακόμα και με τις ταχύτητες των σύγχρονων υπολογιστών θα απαιτηθούν πολλές ημέρες για να επιχειρηθούν όλα αυτά τα πιθανά συνθηματικά.

Αν όμως το μήκος του συνθηματικού είναι 4 μόνο αλφαριθμητικοί χαρακτήρες, τότε υπάρχουν μόνο 10.000 συνδυασμοί, δηλαδή πολύ εύκολη δουλειά για οποιονδήποτε υπολογιστή.

Μια δεύτερη σημαντική μέθοδος για την αποτροπή των συνεχών δοκιμών, είναι να αποσυνδέεται το τερματικό μετά από ένα ορισμένο αριθμό ανεπιτυχών προσπαθειών προσπέλασης.

Στην περίπτωση αυτή είναι σημαντική η ύπαρξη πρόβλεψης, ώστε να εμποδίζεται ο χρήστης να ξαναπροσπαθήσει.

Μια μέθοδος είναι να αποσυνδέεται το τερματικό για κάποιο χρονικό διάστημα, στη διάρκεια του οποίου θα διεξαχθεί η έρευνα για τον εντοπισμό του χρήστη.

'Αλλη μέθοδος είναι η ακύρωση του αριθμού ταυτότητας του χρήστη που χρησιμοποιήθηκε.

ΚΕΦΑΛΑΙΟ 5ο

ΠΡΟΣΩΠΙΚΟ

ΘΕΜΑΤΑ ΠΡΟΣΩΠΙΚΟΥ (ΣΥΝΔΙΚΑΤΑ - ΠΡΟΣΩΠΙΚΟ Η/Υ)

Το θέμα του προσωπικού που εργάζεται στο χώρο των υπολογιστών σχετίζεται άμεσα με το πρόβλημα της απάτης. Εφόσον δεν λαμβάνεται πρόνοια κατά την επιλογή και τη διοίκηση του προσωπικού, η πιθανότητα μιας ενδεχόμενης απάτης είναι αυξημένη.

Κάποιοι υπάλληλοι πιθανόν να ρέπουν προς την ανεντιμότητα, κι αυτό μπορεί να συμβαίνει σε μια άριστα διοικούμενη εταιρία. Άλλοι πάλι μπορεί να εξελιχθούν σε απείθαρχους και απρόθυμους υπαλλήλους λόγω της ανεπαρκούς διοίκησης, με συνέπεια να χάσουν τους ηθικούς ενδοιασμούς τους σε ότι αφορά τους πόρους και την επιτυχία της εταιρίας. Τα ενδεχόμενα αυτά πρέπει να εκτιμούνται μέσα στο γενικό πλαίσιο της διοίκησης προσωπικού. Για παράδειγμα, η διοίκηση του προσωπικού και οι διαπραγματεύσεις για θέματα μισθών ή συνθηκών εργασίας, η διευθέτηση των παραπόνων, η ύπαρξη κατάλληλων δυνατοτήτων εξέλιξης μέσα στην εταιρία κ.λ.π. σχετίζονται άμεσα με την διαμόρφωση της ατμόσφαιρας, του χώρου δουλειάς, όπου η ακεραιότητα του προσωπικού ενθαρρύνεται ή αποθαρρύνεται.

Ένα στοιχείο απογοήτευσης έχει κάνει την εμφάνισή του στο χώρο της Πληροφορικής. Το προσωπικό των ηλεκτρονικών υπολογιστών ευαισθητοποιείται όλο και περισσότερο στο θέμα της απεργιακής κινητοποίησης ως όπλου στις διαπραγματεύσεις με τη

διοίκηση. Συγχρόνως οι δυνατότητες διοικητικής εξέλιξης μέσα στην εταιρία μειώνονται όλο και περισσότερο για το προσωπικό των ηλεκτρονικών υπολογιστών. Είναι σημαντικό ότι το προσωπικό των ηλεκτρονικών υπολογιστών συχνά θεωρείται ως "πρώτη επιλογή" για κάθε μορφή κλαδικής απεργιακής κινητοποίησης. Τα συνδικάτα βρήκαν σε αυτή την επιλογή ένα πανίσχυρο διαπραγματευτικό όπλο. Για να αντιμετωπίσει αυτά τα προβλήματα ο εργοδότης πρέπει να υπολογίσει:

1. Κατά πόσο το προσωπικό του ηλεκτρονικού υπολογιστή αποτελεί ένα ξεχωριστό και κλειστό σύνολο σε σχέση με τους υπόλοιπους εργαζόμενους της εταιρίας.
2. Κατά πόσο το προσωπικό του ηλεκτρονικού υπολογιστή θεωρεί την εργασία του ικανοποιητική ή το κατά πόσο θα έπρεπε να διερευνηθούν όλες οι πιθανές δυνατότητες για την ικανοποίηση των παραπόνων πέρα της συλλογικής δράσης. Τα προβλήματα που αντιμετωπίζουν οι χειριστές των υπολογιστών διαφέρουν αρκετά από τα προβλήματα που αντιμετωπίζουν οι συνάδελφοί τους προγραμματιστές. Οι χειριστές συνήθως θεωρούνται οπαδοί των συνδικάτων, ενώ οι προγραμματιστές θεωρούνται εκκολαπτόμενοι διευθυντές.

ΕΠΙΛΟΓΗ ΠΡΟΣΩΠΙΚΟΥ

Η σωστή επιλογή προσωπικού είναι μια σπουδαιότατη προστατευτική δικλείδα, ώστε να αποφευχθεί η πρόσληψη ανέντιμου προσωπικού.

Σκοπός της εξονυχιστικής εξέτασης των υποψηφίων είναι η επιλογή έντιμων, ικανών και κατάλληλων εργαζόμενων για τις συγκεκριμένες θέσεις.

Πολλές εταιρίες δεν ελέγχουν το παρελθόν των υποψηφίων όταν ζητούν προσωπικό για πρόσληψη. Παράλληλα οι εταιρίες που επιχειρούν τέτοιους ελέγχους ζητώντας συστατικές επιστολές το κάνουν μόνο μετά την πρόσληψη. Έτσι ο έλεγχος του παρελθόντος δεν αντιμετωπίζεται με σοβαρότητα από τις εταιρίες. Εντούτοις είναι καθήκον της διοίκησης να φροντίζει, ώστε το προσωπικό που προσλαμβάνεται να είναι αξιόπιστο και ειλικρινές. Ένας ανέντιμος εργαζόμενος που προσλαμβάνεται από μια εταιρία μπορεί να εξαναγκάσει το αξιόπιστο προσωπικό σε παραίτηση. Η διοίκηση οφείλει να γνωρίζει και να διασταυρώνει το παρελθόν των υποψηφίων, αν και πολλές εταιρίες υφίστανται τις δραστηριότητες ανθρώπων που διαπράττουν αδίκημα για πρώτη φορά.

Τα πιο συνηθισμένα ψευδή στοιχεία στις αιτήσεις και στα βιογραφικά σημειώματα προέρχονται από πλαστογράφηση πτυχίων και παραποίηση των βεβαιώσεων προϋπηρεσίας. Αλλά ακόμα και στην περίπτωση που τα στοιχεία δεν έχουν παραποιηθεί, η αξία των συστατικών επιστολών και των βεβαιώσων προϋπηρεσίας είναι συζητήσιμη. Κάποιες εταιρίες υιοθετούν μια πολιτική, σύμφωνα με την οποία επιτρέπουν στους ανέντιμους υπαλλήλους να παραιτηθούν αντί να τους διώξουν, ενώ κάποιες άλλες προχωρούν ακόμα περισσότερο μέχρι το σημείο να τους εφοδιάζουν με συστατικές επιστολές, στις οποίες δεν αναφέρεται τίποτα για την ανεντιμότητά τους.

Υπάρχουν πολλοί λόγοι για τους οποίους ένας εργοδότης θα πρέπει να καθιερώσει μία αποτελεσματική πολιτική για την εξονυχιστική εξέταση των υποψηφίων:

- Για την προστασία του υπάρχοντος προσωπικού.

- Για την επιλογή του καλύτερου υποψηφίου.
- Για την προστασία των περιουσιακών στοιχείων και των δεδομένων της εταιρίας.
- Για την διαφύλαξη της υπάρχουσας καλής θέλησης του προσωπικού.
- Για την διαφύλαξη της εργασιακής ειρήνης.

Η διοίκηση πρέπει να υιοθετήσει μια πολιτική προς τους εργαζόμενους, που θα αφορά τόσο τους εποχιακούς όσο και τους επί συμβάσει υπαλλήλους. Είναι συζητήσιμο το κατά πόσο ο έλεγχος του παρελθόντος θα πρέπει να γίνεται και για τους υποψηφίους για προαγωγή μέσα στην εταιρία. Πρέπει επίσης να είναι σαφές το ποιός είναι υπεύθυνος για την εφαρμογή της πολιτικής προσλήψεων και το πως θα εφαρμόζεται αυτή.

Οι αιτήσεις πρόσληψης πρέπει να συμπληρώνονται από όλους τους υποψηφίους. Η μορφή και παραγωγή των εντύπων αιτήσεων είναι ένα θέμα που πρέπει να απασχολεί τη διοίκηση. Όλες οι ερωτήσεις στο έντυπο των αιτήσεων πρέπει να είναι υποχρεωτικές και σχετικές. Να είναι τέτοιες που να μπορούν να αποκαλύψουν το συγκεκριμένο υποψήφιο, τις ικανότητές του, τα προσόντα και την εμπειρία του. Μέσα από τις ερωτήσεις να μπορέσει η διοίκηση να εκτιμήσει τα προσόντα, την καταλληλότητα και τη θέση, την εμπειρία, την ειλικρίνεια και την αξιοπιστία του/της υποψηφίου. Οι ερωτήσεις πρέπει να είναι λογικές και σαφείς.

Η διοίκηση θα πρέπει να δηλώσει σαφώς σε περίπτωση που ερωτηθεί, με ποιό τρόπο θα χρησιμοποιήσει και με ποιό τρόπο θα ελέγξει την ειλικρίνεια των πληροφοριών που συμπληρώνονται στις έντυπες αιτήσεις. Ένας υποψήφιος που δεν έχει τίποτα να κρύψει, δεν θα έχει πρόβλημα να απαντήσει σε τέτοιες ερωτήσεις.

ΜΕΘΟΔΟΙ ΕΠΙΛΟΓΗΣ ΠΡΟΣΩΠΙΚΟΥ

Η διοίκηση μπορεί να χρησιμοποιήσει διάφορες μεθόδους για να ελέγξει όσα ισχυρίζεται ο υποψήφιος:

- *Γραπτές συστάσεις:*

  Είναι δυνατόν να αποκτηθούν από προηγούμενους εργοδότες ή εκπαιδευτικά ιδρύματα, στα οποία φοίτησε ο υποψήφιος. Οι γραπτές συστάσεις είναι μια κοινωνικά αποδεκτή μέθοδος για τη συλλογή πληροφοριών για κάποιο άτομο, αλλά συχνά παρέχει ανεπαρκείς πληροφορίες για μία σε βάθος μελέτη και εκτίμηση των ικανοτήτων του συγκεκριμένου ατόμου.

- *Τηλεφωνικές συστάσεις:*

  Είναι μια γρήγορη και αποτελεσματική μέθοδος για να σχηματιστεί γνώμη για κάποιο συγκεκριμένο άτομο. Τηλεφωνώντας στον προηγούμενο εργοδότη του υποψηφίου και μιλώντας προσωπικά στον ίδιο, μπορείτε συχνά να φωτίσετε στοιχεία του υποψηφίου τα οποία δεν είναι προφανή από μία γραπτή συστατική επιστολή.

- *Συνεντεύξεις από την διεύθυνση προσωπικού:*

  Γίνεται από τους υπεύθυνους τού τμήματος ή της διεύθυνσης προσωπικού. Η μέθοδος αυτή δεν προσφέρεται για τον εντοπισμό των αποφασισμένων κακοποιών. Μπορεί ως συμπληρωματική μέθοδος να συνεισφέρει στον εξονυχιστικό έλεγχο των υποψηφίων αλλά δεν πρέπει να χρησιμοποιείται ως αποκλειστική μέθοδος.

- *Ψυχολογικά τεστ:*

  Τα ψυχολογικά τεστ έχουν γίνει πολύ δημοφιλή τα τελευταία χρόνια, αλλά η αξιοπιστία τους είναι συζητήσιμη και αμφισβητήσιμη. Υποτίθεται ότι προσδιορίζουν τα χαρακτηριστικά

της προσωπικότητας ενός συγκεκριμένου ατόμου, αλλά δεν αποτελούν ένα αλάνθαστο μέσο για τον έλεγχο της εντιμότητάς του.

- *Γραφολογική εξέταση:*

  Η Γραφολογία έχει γίνει αρκετά αποδεκτή τα τελευταία χρόνια. Η επιστράτευση ενός ειδικού γραφολόγου, για να αναγνωρίσει τα χαρακτηριστικά του υποψηφίου, μπορεί να δώσει χρήσιμες πληροφορίες, αλλά όπως και με τα λοιπά "τεστ" και τις αναλύσεις, τα αποτελέσματα πρέπει να εκτιμηθούν με προσοχή.

- *Έλεγχος με ανιχνευτή ψεύδους:*

  Η χρησιμότητα του ανιχνευτή ψεύδους είναι αμφισβητήσιμη. Το σύστημα αυτό μπορεί να είναι γρήγορο και ακριβές, αλλά όχι και αλάνθαστο, ενώ σε πολλές περιπτώσεις είναι και κοινωνικά απαράδεκτο. Είναι προφανές ότι οι συσκευές αυτές πρέπει να χρησιμοποιούνται, εάν χρησιμοποιούνται, μόνο από εκπαιδευμένους έμπειρους χειριστές.

  Η χρήση του μπορεί να βοηθήσει τον εργοδότη να αποφύγει την πρόσληψη ενός υπαλλήλου με κρυφή ανέντιμη προϊστορία ή ενός υποψηφίου ο οποίος έχει σκόπιμα αναφέρει ψευδή στοιχεία στην αίτησή του. Επίσης μπορούν να εντοπισθούν μια σειρά άλλων προβλημάτων όπως ο αλκοολισμός, οι οικονομικές δυσκολίες, η ασθένεια ή μια πιθανή διανοητική αστάθεια, αλλά όπως είπαμε και προηγουμένως η χρησιμότητά του είναι αμφισβητήσιμη.

ΠΩΣ ΚΛΕΒΟΥΝ ΟΙ ΕΡΓΑΖΟΜΕΝΟΙ

Ο εσωτερικός κλέφτης σε έναν οργανισμό μπορεί να είναι ο οποιοσδήποτε, από το γενικό διευθυντή ως το θυρωρό, από το στέλεχος της Πληροφορικής μέχρι το χειριστή του υπολογιστή. Συχνά τα θύματα

μιας εσωτερικής κλοπής είναι ανυποψίαστα για το αδίκημα που διαπράχθηκε. Οι συνάδελφοι του ενόχου μπορεί να μην είναι πρόθυμοι να δώσουν στοιχεία για το συνάδελφό τους. Επαφίεται στον εργοδότη η ανάληψη πρωτοβουλιών. Πρέπει η διεύθυνση να είναι σε θέση να ανιχνεύσει το αδίκημα, να αναγνωρίσει τον κλέφτη και να επιβάλει μια πολιτική ποινικής δίωξης. Οι συνηθισμένες κατηγορίες απάτης είναι οι ακόλουθες :

- η λήψη μισθών και αποζημιώσεων από εργαζομένους που δεν τους δικαιούνται,
- η υπερχρέωση και απολαβή της διαφοράς,
- η μεταβολή των στοιχείων της απογραφής,
- η χρήση του εξοπλισμού για προσωπικό όφελος,
- η εμφάνιση ψευδών φύλλων παρουσίας,
- η δωροληψία για προνομιακή μεταχείριση,
- η εμφάνιση ανύπαρκτου προσωπικού στις καταστάσεις πληρωμών,
- η ψευδής εγγραφή δαπανών,
- η πώληση εμπιστευτικών πληροφοριών σε ανταγωνιστές,
- η παρουσίαση εικονικών προμηθευτών,
- η κλοπή πληρωμών

ΚΕΦΑΛΑΙΟ 6ο

Η ΑΠΑΤΗ ΣΤΟ ΧΩΡΟ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

Η ΑΝΑΓΝΩΡΙΣΗ ΤΗΣ ΖΗΜΙΑΣ

Υπάρχουν πάντα ενδείξεις κατά την τέλεση μιας απάτης. Εναπόκειται στον εργοδότη να προσέχει ώστε να καταλαβαίνει τα αποκαλυπτικά σημάδια. Τέτοια είναι:

- επίσημα στοιχεία παραποιημένα, ελλειπή ή κατεστραμμένα,
- χρήση ανεπίσημων ή πλαστών υπογραφών,
- κατάχρηση αλκοόλ ή ναρκωτικών από το προσωπικό,
- χαρτοπαιξία από το προσωπικό,
- επανεγγραφή των αρχείων,
- η απροθυμία των εργαζομένων να αλλάξουν θέση ή να προαχθούν,
- η εμφάνιση ταραχής σε μέλη του προσωπικού από ερωτήσεις ρουτίνας,
- η διαβίωση μελών του προσωπικού πέρα από τις οικονομικές δυνατότητές τους,
- τα υπερβολικά παράπονα από προμηθευτές ή πελάτες,
- οι ελλείψεις στα αποθέματα ή το ταμείο.

Η πλειονότητα των ανθρώπων που κλέβουν το κάνει για προσωπικά οφέλη παρά από άλλα κίνητρα, τα οποία όμως μπορεί να συνυπάρχουν. Οι εργοδότες πρέπει να προσέχουν αυτές τις περιπτώσεις:

- εκδίκηση για ένα (πραγματικό ή φανταστικό) λάθος,
- πίεση από συναδέλφους,
- η επιθυμία να "νικήσει" το σύστημα,

- οι κακές σχέσεις προσωπικού - διεύθυνσης,
- η κλοπή ως "τρόπος ζωής" της εταιρίας.

Ο ΧΕΙΡΙΣΜΟΣ ΤΟΥ ΘΕΜΑΤΟΣ ΑΠΑΤΗ

Εφόσον έχει αναγνωρισθεί ο υπαίτιος, οι κινήσεις του εργοδότη πρέπει να είναι προσεκτικές και πολύ καλά καθορισμένες. Η γρήγορη δράση μπορεί να δημιουργήσει χειρότερα προβλήματα από αυτά που προσπαθεί να επανορθώσει. Η παντελής όμως απουσία δράσης μπορεί να οδηγήσει τον οργανισμό σε πτώχευση.

Πριν κατηγορηθεί ο εργαζόμενος σαν κλέφτης ή απατεώνας, είναι σημαντικό να προηγηθούν οι παρακάτω ενέργειες:

- Η επιβεβαίωση της τέλεσης του εγκλήματος.
- Ο καθορισμός του είδους του αδικήματος.
- Ο εντοπισμός των πιθανών ενόχων.
- Ο εντοπισμός όλων των πιθανών στοιχείων.
- Ο εντοπισμός όλων των πιθανών μαρτύρων.
- Ο προσδιορισμός των γνώσεων που απαιτούνται για την επιτυχή διεκπεραίωση της υπόθεσης.

Αφού επιβεβαιωθεί η τέλεση του αδικήματος, έρχεται η κατάλληλη στιγμή για την εξέταση μαρτύρων και υπόπτων. Αυτός που κάνει τις έρευνες / ανακρίσεις πρέπει:

- να είναι επαγγελματίας και ευγενικός,
- να μην προσβάλλει,
- να μην καταδικάζει,
- να μην απειλεί,
- να δίνει τη δυνατότητα στον ύποπτο να εξηγεί τις ενέργειές του,
- να μην προχωρεί σε σωματική έρευνα χωρίς τη γραπτή συγκατάθεση του ανακρινούμενου,

- να συνοδεύεται πάντα από έναν παρατηρητή κατά τη διάρκεια των ερευνών / ανακρίσεων,
- να έλθει σε επαφή με την αστυνομία.

Η αστυνομία πολλές φορές δεν θέλει να εμπλακεί σε διαμάχες εργοδοσίας - εργαζομένων κι έτσι ο εργοδότης πρέπει να είναι έτοιμος:

- να παρουσιάσει τα στοιχεία που αποκαλύφθηκαν,
- να δώσει τα ονόματα αυτών που φέρονται ως αναμεμιγμένοι στην υπόθεση,
- να αιτιολογήσει τα συμπεράσματά του,
- να δώσει τα ονόματα όλων των πιθανών μαρτύρων,
- να συγκεκριμενοποιήσει το ύψος των ζημιών,
- να αποφύγει μη επιβεβαιωμένες καταγγελίες.

Η αστυνομία ίσως είναι διστακτική να ασκήσει ποινική δίωξη σε δύσκολες υποθέσεις και η διεύθυνση πρέπει να την βοηθήσει όσο το δυνατόν περισσότερο. Μέχρι αποδείξεως της ενοχής του ενώπιον δικηγόρου, ο (προφανώς) ανέντιμος εργαζόμενος έχει τα ίδια δικαιώματα με τους συναδέλφους του.

"ΕΡΕΥΝΕΣ ΣΕ ΠΕΡΙΠΤΩΣΗ ΑΠΑΤΗΣ"

Όταν διαπιστωθεί κάποια απάτη, είναι αναγκαία η εξέταση (ανάκριση) των μαρτύρων και των υπόπτων. Αυτό πρέπει να γίνει με τρόπο επαγγελματικό. Σκοπός είναι η αποκάλυψη της αλήθειας και πρέπει να λαμβάνονται υπόψη τα δικαιώματα (ηθικά και νομικά) των εξεταζομένων.

Εξέταση ή ανάκριση σημαίνει ανθρώπινες σχέσεις. Είναι πασίγνωστο το πόσο ασαφείς είναι οι διαπροσωπικές σχέσεις, αλλά και τα χαρακτηριστικά των ανθρώπων. Ποτέ δεν πρέπει να θεωρείται η

ανθρώπινη συμπεριφορά δεδομένη και σταθερή. Αυτός είναι και ο λόγος για τον οποίο η λογική των κοινών / τυπικών ερωτήσεων δεν "δουλεύει" πάντα με τις συνεντεύξεις.

Σε μια εξέταση η πρώτη επαφή ανάμεσα στον εξεταζόμενο και τον "εξεταστή" είναι πολύ σπουδαία. Η εμπειρία της αστυνομίας δείχνει ότι κατά την εξέταση ενός ατόμου, μια φιλική συμπεριφορά θα κάνει τον εξεταζόμενο να μη νοιώθει άνετα σε λιγότερο από μία ώρα. Θα νοιώθει ότι όλος ο κόσμος είναι εναντίον του. Τελικά ο εξεταζόμενος θα ανυπομονεί να τελειώσει η εξέταση. Κάτω από αυτές τις συνθήκες η ενοχή ή η αθωότητα είναι αδιάφορες.

Σε μια εξέταση ο εξεταζόμενος τείνει να συμφωνήσει με ο,τιδήποτε λέει ο εξετάζων. Ο λόγος είναι ότι ο εξεταζόμενος, ο οποίος πιθανότατα δεν νοιώθει άνετα, αποζητά άνεση και ασφάλεια. Η πλειονότητα των εξεταζομένων θα είναι απροετοίμαστοι να ρωτήσουν τους εξεταστές τους. Ο εξετάζων ελέγχει τη συζήτηση.

Κάποιοι προτείνουν ότι οι ανακρίσεις για απάτη πρέπει να λαμβάνουν χώρα έξω από το χώρο εργασίας του ανακρινόμενου, με σκοπό να δημιουργείται στον ανακρινόμενο αίσθημα ανασφάλειας. Ο ανακριτής μπορεί να θέλει να κάνει τον ανακρινόμενο να νοιώσει ότι βρίσκεται σε κίνδυνο, αν και πάλι υπάρχουν ηθικές εμπλοκές στη μέθοδο αυτή, οι οποίες δεν πρέπει να αγνοούνται.

Στη διάρκεια της εξέτασης ο ανακριτής θα πρέπει να μιλάει μόνο το 1/3 του χρόνου. Χρειάζεται μόνο να σκεφτεί και να εκτιμήσει τις απαντήσεις που παίρνει. Ερωτήσεις που μπορούν να απαντηθούν με ένα ΝΑΙ ή ένα ΟΧΙ θα πρέπει να αποφεύγονται. Το είδος αυτό των ερωτήσεων δεν προκαλεί τον εξεταζόμενο να μιλήσει για πολύ, και άρα δεν υπάρχει πιθανότητα να αποκαλύψει κάποιες πληροφορίες που δεν υποψιάζεστε. Αντί της ερώτησης "είχες καλό ταξίδι;" ίσως προτιμότερη θα ήταν η ερώτηση "πώς ήταν το ταξίδι;".

Η εξέταση έχει το τελετουργικό της. Υπάρχουν οι προσδοκίες, οι αβρότητες στη συμπεριφορά. Είναι μια διαδικασία με φάσεις.

Δεν υπάρχει λόγος να αρχίσει ο εξεταστής να απειλεί. Είναι αναπόφευκτο ο εξεταζόμενος να βρίσκεται σε ένταση. Συγχρόνως όμως ο εξεταστής θα πρέπει να είναι σίγουρος ότι ελέγχει την κατάσταση. Κάποιοι άνθρωποι είναι ικανοί να ελέγχουν την κατάσταση ακόμα και όταν ανακρίνονται.

Κατά τη διάρκεια της εξέτασης οι ερωτήσεις που τίθενται πρέπει να είναι καθαρές και λακωνικές. Πρέπει να τίθενται συστηματικά. Είναι προτιμότερο να υπάρχει κάποια "κεντρική ιδέα" στην εξέταση, παρά να υπάρχει ένας "συγκεκριμένος στόχος". Ό,τι πετύχει ο εξεταστής κατά τη διάρκεια της εξέτασης, θα το πετύχει με την εμπλοκή του εξεταζόμενου. Οι λεπτομέρειες της εξέτασης θα πρέπει να καταγράφονται με κάποιο τρόπο και ο εξεταζόμενος θα πρέπει να το γνωρίζει και να ερωτηθεί γι' αυτό.

Η ΕΜΠΛΟΚΗ ΤΗΣ ΑΣΤΥΝΟΜΙΑΣ

Από τη στιγμή που θα διαπιστωθεί η απάτη, η πολιτική της εταιρίας ίσως να επιβάλλει την παραπομπή του υπαιτίου. Από τη στιγμή που θα αποφασιστεί η παραπομπή, η εμπλοκή της αστυνομίας καθίσταται αναγκαία. Στην περίπτωση αυτή συνίσταται η εμπλοκή της αστυνομίας στην ανάκριση όσο το δυνατόν νωρίτερα.

Από τη στιγμή που η αστυνομία θα αρχίσει τις ανακρίσεις για την εξιχνίαση της απάτης, οι δυνατές ενέργειες της εταιρίας περιορίζονται από τις ανακρίσεις της αστυνομίας. Οι ανακρίσεις δεν βρίσκονται πια κάτω από τον έλεγχο των "εταιρικών ελεγκτών" , τα χέρια της αστυνομίας πρέπει να αφεθούν απολύτως ελεύθερα.

Η πρόωρη εμπλοκή της αστυνομίας είναι ουσιώδης, ώστε να αποφευχθεί η καταστροφή ζωτικών μαρτυριών από κάποιους "ενθουσιώδεις ερασιτέχνες". Οι ανακρίσεις πρέπει πάντα να διεξάγονται με επαγγελματικό τρόπο. Τα πρώτα βήματα της ανάκρισης για την εξιχνίαση μιας απάτης είναι ίσως και τα περισσότερο σημαντικά για την επίλυση του προβλήματος. Θα πρέπει επίσης να λαμβάνεται πάντα υπόψη ότι η αστυνομία δεν θα είναι πρόθυμη να διεξάγει ανακρίσεις για τυχόν απάτες, αν δεν μπορεί να αποδειχθεί ότι έχει διαπραχθεί εγκληματική ενέργεια.

Η αστυνομία έχει υποχρέωση να διερευνήσει κάθε περίπτωση εγκληματικής ενέργειας που της αναφέρεται. Η ανάκριση για την εξιχνίαση της απάτης θα είναι πρόβλημα για έναν κοινό ανακριτή, εκτός αν αυτός είναι μέλος της ειδικής ομάδας (Fraud Squad). Οι πολύπλοκες ιδιαιτερότητες ενός λογιστικού συστήματος που βασίζεται σε υπολογιστές και το οποίο έχει υποστεί κάποια απάτη, είναι δύσκολο να εμπνεύσουν τον ενθουσιασμό στο μέσο αστυνομικό. Ομοίως θα υπάρχουν ελάχιστα κίνητρα για την αστυνομία, ώστε να διεκπεραιώσει μια περίπτωση με υποψία απάτης στην οποία η ζημιά δεν είναι προφανής.

Η αστυνομία δεν είναι η μόνη κρατική υπηρεσία ικανή να βοηθήσει στις έρευνες για την εξιχνίαση μιας περίπτωσης απάτης. Μια απάτη που έχει σχέση με το φόρο ίσως απαιτεί τη βοήθεια της αρμόδιας υπηρεσίας της Εφορίας (Inland Revenue Investigation Branch), μια απάτη που έχει σχέση με το Φ.Π.Α. το ίδιο.

Κυβερνητικές υπηρεσίες όπως π.χ. το Υπουργείο Οικονομικών ή το DHSS (Υπουργείο Κοινωνικών Υπηρεσιών) μπορούν επίσης να εμπλακούν σε αντίστοιχες υποθέσεις. Η απαιτούμενη εμπειρία για την εξιχνίαση μιας απάτης υπάρχει και πρέπει να χρησιμοποιείται από την

εταιρία με σκοπό τη σωστή διεκπεραίωση όλων των υποθέσεων απάτης ή κατάχρησης με υπολογιστή.

Η ΠΟΛΙΤΙΚΗ ΤΗΣ ΠΑΡΑΠΟΜΠΗΣ

Οι διευθυντές οφείλουν να αναπτύξουν μια σχολαστική πολιτική διασφάλισης για την εταιρία τους.

Η πολιτική αυτή θα προσφέρει το πλαίσιο μέσα στο οποίο μπορεί να διαμορφωθεί ο τρόπος διοίκησης για κάθε συγκεκριμένη περίπτωση. Επίσης θα ορίσει το κατάλληλο εναρκτήριο σημείο για κάθε κινητοποίηση που μπορεί να προκύψει από ένα πρόβλημα ασφάλειας (ή άλλο σχετικό πρόβλημα). Η όποια πολιτική πρέπει να θεωρεί δεδομένο ότι οι εργαζόμενοι στην πλειοψηφία τους είναι ειλικρινείς, ενώ πρέπει επίσης να διακηρύσσει την ανάγκη προστασίας των πολύτιμων αγαθών τόσο των εργαζομένων όσο και της εταιρίας. Πρέπει επίσης να διευκρινίζει ότι πρόθεση είναι να καθιερωθεί αποτελεσματική συνεργασία ανάμεσα στο προσωπικό ασφαλείας της εταιρίας, τη διοίκηση, τα συνδικάτα και τη διεύθυνση προσωπικού της εταιρίας.

Ένα παράδειγμα πολιτικής διασφάλισης

Η διασφάλιση του υπολογιστή θεωρείται από την εταιρία ως ένας ουσιώδης παράγων του συνολικού κόστους / αποτελεσματικότητας της λειτουργίας της. Είναι γενικά παραδεκτό ότι η έλλειψη πρόνοιας για τη διασφάλιση μπορεί να έχει δυσμενείς οικονομικές επιπτώσεις στην εταιρία. Συγχρόνως είναι αναγκαίο να διατηρείται κάποια ισορροπία ανάμεσα στη διασφάλιση αφενός και την πρακτικότητα (της πολι-

τικής), καθώς και τα δικαιώματα και διαθέσεις του προσωπικού αφετέρου.

Η ζημιά που οφείλεται σε ανεπαρκή μέτρα διασφάλισης είναι ένας σχετικός όρος, συχνά θέμα υποκειμενικής κρίσης. Το κόστος των ασφαλίστρων κατά των ζημιών είναι συνάρτηση τόσο των προληπτικών μεθόδων όσο και της έκθεσης σε κινδύνους και το κόστος της πρόληψης πρέπει να ενδιαφέρει όλους.

Η εταιρία πρέπει να στοχεύει στα παρακάτω :

- να προστατεύεται από την κλοπή, απάτη και κακόβουλη φθορά,
- να παρέχει "λογική" προστασία στα υπάρχοντα των εργαζομένων κατά το χρόνο της εργασίας τους,
- να καθιερώνει αποτελεσματικά μέτρα, με τη βοήθεια των οποίων επιτυγχάνεται η διασφάλισή της,
- να φροντίζει για την αποτελεσματική συνεργασία ανάμεσα στο προσωπικό ασφαλείας, τους εργαζόμενους και τη διεύθυνση προσωπικού,
- να επιδιώκει την αποτελεσματική συμμετοχή της αστυνομίας, ενώ παράλληλα να διατηρεί το δικαίωμά της να διαχειρίζεται τα θέματα διασφάλισης με τρόπο αποδεκτό από την εταιρία και τους εργαζομένους,
- να εντοπίζει τους υψηλούς τομείς κινδύνου μέσα στην εταιρία και να βεβαιώνεται ότι οι απαραίτητοι έλεγχοι έχουν θεσπιστεί και λειτουργούν σωστά,
- να παρέχει μια συνολική πολιτική της εταιρίας, ενώ παράλληλα να αναγνωρίζει την ανάγκη συνεργασίας του καθενός στα θέματα της διασφάλισής της,
- να παρέχει ένα εκπαιδευτικό πρόγραμμα σε όλα τα μέλη της διοίκησης της εταιρίας, και να βεβαιώνεται ότι υπάρχει εγχειρίδιο διασφάλισης (security manual) εν χρήσει σε όλα τα επίπεδα της

εταιρίας, εφόσον αναγνωρίζει ότι η διασφάλιση είναι καθήκον της διοίκησης,

- να επανεκτιμά τους πιθανούς κινδύνους ανά τακτά χρονικά διαστήματα.

ΔΙΑΔΙΚΑΣΙΕΣ ΠΑΡΑΙΤΗΣΕΩΝ

Σε κάθε εταιρία οι διαδικασίες που έχει καθιερώσει η διεύθυνση προσωπικού ή η οικονομική διεύθυνση της εταιρίας, για τις παραιτήσεις ή τις απολύσεις του προσωπικού πρέπει να ακολουθούνται αυστηρά.

Στο περιβάλλον του υπολογιστικού κέντρου, ιδιαίτερα, και από τη σκοπιά της διασφάλισης, μόλις γνωστοποιηθεί το ενδεχόμενο απόλυσης ή παραίτησης, ο ενδιαφερόμενος εργαζόμενος πρέπει να απομακρύνεται από τις ευαίσθητες περιοχές και να παύει να έχει πρόσβαση σε εμπιστευτικά δεδομένα. Τέτοιες ευαίσθητες περιοχές είναι για παράδειγμα :

- ο προγραμματισμός για την ανάπτυξη εφαρμογών,
- ο προγραμματισμός για τη συντήρηση εφαρμογών,
- ο προγραμματισμός για επείγουσες περιπτώσεις,
- ο χώρος του υπολογιστή,
- οι βιβλιοθήκες.

ΚΕΦΑΛΑΙΟ 7ο

ΠΕΡΙΠΤΩΣΕΙΣ ΑΠΑΤΗΣ

ΝΟΜΟΣ - ΔΕΟΝΤΟΛΟΓΙΑ

Ένα από τα σημαντικότερα χαρακτηριστικά της απάτης με υπολογιστές γενικά, αλλά και της εισβολής ειδικότερα, είναι το ότι η ευαισθησία για τα θέματα της δεοντολογίας αναιρείται μπροστά στην επίδειξη τεχνικής δεξιοτεχνίας. Για παράδειγμα στην ταινία "War Games" ταυτιζόμαστε με το νεαρό που παράνομα αλλάζει τους βαθμούς του στις εξετάσεις.

Ειδικά έλεγαν ότι αν μπορείς να χειριστείς τον υπολογιστή με δεξιοτεχνία ανάγεσαι υπεράνω της κοινής ηθικής.

Ομοίως κάποιοι επιδέξιοι εισβολείς που έδρασαν το 1983 στις Δυτικές Ακτές των Η.Π.Α. "αναγορεύτηκαν" σε "σαΐνια", "πάνσοφους" κ.λ.π. Μπορεί να διαβάζουμε ότι στην Αμερική το FBS καταδιώκει τους εισβολείς, αλλά δεν είναι εύκολο να θεωρήσεις αυτούς τους ανθρώπους απατεώνες και ανυπόληπτα κοινωνικά στοιχεία. Υπάρχει ο πειρασμός να θεωρηθεί ότι η "τεχνική επιδεξιότητα δικαιολογεί αυτό που σαφώς είναι αντικοινωνική συμπεριφορά". Το παραπάνω πρέπει να ληφθεί σοβαρά υπόψιν, όταν οργανώνεται ο τρόπος αντιμετώπισης της εισβολής και των λοιπών περιπτώσεων παράνομης συμπεριφοράς στο χώρο των ηλεκτρονικών υπολογιστών.

Στην πραγματικότητα χρειάστηκαν πολύς χρόνος και προσπάθεια για να μετατραπεί η εισβολή σε αδίκημα.

Η εισβολή άρχισε να ποινικοποιείται στις περισσότερες πολιτείες των Η.Π.Α. μετά το 1985 και μετά από συνεχή κρούσματα εισβολής στον χώρο των υπολογιστών.

Κάτι ανάλογο συνέβη και στην Μ. Βρετανία, χώρες που γνώρισαν γρήγορα την ανάπτυξη και τον εκσυγχρονισμό στον τομέα της Πληροφορικής, γι' αυτό και γίνεται ιδιαίτερος λόγος γι' αυτές, αφού αντιπροσωπεύουν τα πιο κλασσικά και ζωντανά παραδείγματα.

Σημειώνοντας αυτή τη δικομματική προσέγγιση δόθηκε έμφαση στο γεγονός ότι οι υπολογιστές κατάφεραν να δημιουργήσουν μια νέα γενιά αδικημάτων. Είναι προφανές ότι η ανάπτυξη συστημάτων που στηρίζονται σε υπολογιστές καθιστά αναγκαία την επανεκτίμηση πολλών παραδοσιακών νομικών θεμάτων και τοποθετήσεων.

Σήμερα αναγνωρίζεται πια ότι η εισβολή αποτελεί μια παράνομη πράξη και πρέπει να αποτρέπεται και από το Νόμο.

Θεωρείται πλημμέλημα και τιμωρείται όποιος εκ προθέσεως αποκτά πρόσβαση σε πληροφοριακό σύστημα εν γνώσει της απαγόρευσης πρόσβασης, εκτός και αν κάποιος ενεργεί στο πλαίσιο της εργασίας του.

Επιπλέον τιμωρείται ειδικά η πρόσβαση με σκοπό την απάτη, εκβίαση, ιδιοποίηση περιουσίας ή πληροφοριών ή απλώς την αχρήστευση Η/Υ. Έτσι σε κάθε χώρα ψηφίζονται νέοι νόμοι για να αντιμετωπισθεί το φαινόμενο της εισβολής (Η.Π.Α.) ή η υπάρχουσα νομοθεσία ερμηνεύεται κάτω από τα νέα γεγονότα (Μ. Βρετανία).

Πρέπει να τονίσουμε ότι δημιουργείται ένα νομοθετικό πρόβλημα του τρόπου προσέγγισης του (hacking) εισβολή, γιατί δεν συνδέεται αναγκαστικά με πρόκληση βλάβης από πρόθεση ή αλλιώς.

Αποτέλεσμα αυτού του ιδιαίτερου χαρακτηριστικού του hacking είναι να προβληματίζει το νομοθέτη. Υπάρχει η δυνατότητα ποινικοποίησης του hacking χωρίς περιορισμούς, δηλαδή της

ποινικοποίησης και αυτής της απλής πράξης εισόδου, χωρίς άδεια σε πληροφοριακά συστήματα (άρθρο 21 του Σουηδικού Νόμου που ισχύει από το 1973) δίχως αναφορά στο σκοπό ή στο αποτέλεσμα της δράσης.

Πιο περιορισμένη αντιμετώπιση υφίσταται στο Γερμανικό "Δεύτερο Νόμο για την καταστολή του Οικονομικού εγκλήματος", ο οποίος τιμωρεί την χωρίς άδεια πρόσβαση σε δεδομένα, που γενικά δεν απευθύνονταν στον εισβολέα και για την προστασία των οποίων είχαν ληφθεί συγκεκριμένα μέτρα.

Περαιτέρω περιορισμός είναι να απαιτείται συγκεκριμένος σκοπός (Καναδάς), απόκτηση, τροποποίηση ή καταστροφή δεδομένων. Το hacking έχει γίνει αντικείμενο ιδιαίτερης νομικής ρύθμισης στο Ελληνικό Δίκαιο. Το (νέο) άρθρο 370Γ, παρ. 2 Π.Κ. τιμωρεί όποιον αποκτά πρόσβαση σε στοιχεία πληροφοριακού συστήματος, εφόσον δεν είχε δικαίωμα, "ιδίως" με παραβίαση μέτρων ασφαλείας.

Αν η πράξη αφορά τις διεθνείς σχέσεις ή την ασφάλεια του κράτους τιμωρείται ως κατασκοπεία (148, 146 Π.Κ.). Είναι προφανές ότι προτιμήθηκε η ποινικοποίηση της απλής πράξης πρόσβασης, χωρίς περιορισμούς ως προς την πρόθεση ή τα αποτελέσματα της πρόσβασης.

Η ειδική αναφορά σε θέματα ασφαλείας και διεθνών σχέσεων προφανώς εκπηγάζει από τη μεγάλη δημοσιότητα που παίρνουν τέτοιες περιπτώσεις. Έτσι η "πληροφοριακή ειρήνη" θεωρείται απόλυτα προστατευόμενο αγαθό.

ΠΑΡΑΔΕΙΓΜΑΤΑ ΑΠΑΤΗΣ

Παραθέτουμε πιο κάτω μερικά χαρακτηριστικά παραδείγματα "απάτης" και σε κάποιες απ' αυτές υπάρχει χρηματικό κίνητρο, ενώ

κάποιες άλλες έλαβαν χώρα μόνο και μόνο για να απαντηθεί το ερώτημα : "μπορεί να σπάσει το σύστημα ; ".

1. Στις Η.Π.Α. τα μέλη της "Milwaukee 4145" μιας ομάδας νεαρών από την ομώνυμη πόλη το Milwaukee, εισχώρησαν σε έναν αριθμό συστημάτων μέσω ενός αμερικανικού δικτύου μεταγωγής πακέτων μηνυμάτων (PSS).
2. Τέσσερις 13χρονοι μαθητές στο Γυμνάσιο Dalton της Νέας Υόρκης συνελήφθησαν, όταν εισχώρησαν σε 21 υπολογιστές στον Καναδά μέσω ενός δικτύου τηλεπικοινωνιών. Οι εταιρίες που υπέστησαν την εισβολή χρησιμοποιούσαν ευρέως υλικό της DEC όπως και το Γυμνάσιο των μαθητών. Σε μερικά από τα συστήματα είχαν διατηρηθεί οι τοπικές ταυτότητες και συνθηματικά που ήταν γνωστά και στους μαθητές από την εμπειρία τους με τους υπολογιστές της DEC.
3. Οι μαθητές ενός Γυμνασίου στο San Diego των Η.Π.Α. μπήκαν στον υπολογιστή του σχολείου τους και άλλαξαν τα συνθηματικά με αποτέλεσμα να μην μπορούν οι καθηγητές να μπουν στο σύστημα. Επίσης άλλαξαν τη βαθμολογία των εξετάσεων και γενικά πλαστογράφησαν όλα τα αρχεία.
4. Δύο υπάλληλοι λογιστηρίου εξαπάτησαν μια μεγάλη βιομηχανία. Ο ένας εξέδιδε ψευδή τιμολόγια για τεράστιες ποσότητες αγαθών, ενώ ο συνεργάτης του προετοίμαζε βεβαιώσεις παραλαβής με τις οποίες εκκαθαρίζονταν τα τιμολόγια. Το σύστημά τους δούλεψε με επιτυχία 4 χρόνια μέχρις ώτου αποκαλυφθούν.
5. Ένα στέλεχος μεγάλου οργανισμού διακίνησης κεφαλαίων, συνδετικός κρίκος ανάμεσα στον οργανισμό και στο σύστημα του υπολογιστή που χρησιμοποιούσε ο οργανισμός, εξαπάτησε τους εργοδότες του υποβάλλοντας ψευδείς συναλλαγές που αντιστοιχούσαν σε φανταστικά ονόματα. Ο συγκεκριμένος

εργαζόμενος είχε αναρριχηθεί από κατώτατη θέση της εταιρίας, με αποτέλεσμα να γνωρίζει πλήρως τις διοικητικές διαδικασίες της. Ήταν επίσης αρμόδιος να τηρεί το "βιβλίο τίτλων" και το "βιβλίο ταμείου", της εταιρίας.

6. Ένας επιχειρηματίας δημιούργησε γύρω στις 50 εταιρίες χωρίς εμπορική δραστηριότητα. Στη συνέχεια έστελνε πλαστά παραστατικά στην Εφορία απαιτώντας επιστροφή Φ.Π.Α. Σε μία περίοδο 13 μηνών εισέπραξε με αυτόν τον τρόπο 128.000 λίρες Αγγλίας.

   Η εμπειρία του στον τρόπο με τον οποίο γίνεται ο διακανονισμός του Φ.Π.Α. του επέτρεψε να αποκομίσει ένα σεβαστό ποσό.

7. Ένας αναλυτής συστημάτων μιας καπνοβιομηχανίας τροποποίησε ένα πρόγραμμα, ώστε να εκτυπώνει πλασματικά κουπόνια τα οποία στη συνέχεια στέλνονταν σε κάποια ταχυδρομική διεύθυνση.

   Ο αναλυτής τα παραλάμβανε και τα αντάλλασε με διάφορα αγαθά.

8. Ο υπεύθυνος βάρδιας ενός κέντρου επεξεργασίας δεδομένων στην Ολλανδία έκλεψε 500 δέσμες δίσκων. Ζητήθηκαν λύτρα 290.000 λίρες Αγγλίας αλλά η είσπραξη του ποσού στο Λονδίνο δεν πέτυχε.

   Ο υπεύθυνος βάρδιας έκλεψε τους δίσκους, ενώ του είχε κοινοποιηθεί η απόλυσή του από τον εργοδότη του.

9. Μια 19χρονη έπεισε το φίλο της να κλέψει αντίγραφα προγραμμάτων από τον εργοδότη του, μια εταιρία παραγωγής λογισμικού. Στη συνέχεια προσπάθησε να πουλήσει τα προγράμματα στους πελάτες της εταιρίας.

10. Ένας εργαζόμενος σε Κέντρο Επεξεργασίας Δεδομένων έκλεψε το ιστορικό αρχείο ενός πελάτη του εργοδότη, το οποίο στη συνέχεια χρησιμοποίησε για δικές του δραστηριότητες.

11. Ο υπεύθυνος για τις μαγνητικές ταινίες του μηχανογραφικού κέντρου μιας ασφαλιστικής εταιρίας απολύθηκε με προειδοποίηση

30 ημερών. Στη διάρκεια αυτού του διαστήματος αντικατέστησε τις περισσότερες μαγνητικές ταινίες με άγραφες.

ΔΙΚΑΣΤΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ

Η υπόθεση Gold / Schifreen

Στις 24 Απριλίου 1986 το Δικαστήριο του Southwark στο Νότιο Λονδίνο, έκρινε ένοχους με την κατηγορία της εισβολής δύο δημοσιογράφους, τους Steve Gold και Rob Schifreen, που έκαναν ελεύθερο ρεπορτάζ για υπολογιστές.

Η δίκη που υπολογίζεται πως κόστισε πάνω από 1 εκατομμύριο λίρες Αγγλίας, θεωρήθηκε σταθμός στα νομικά χρονικά και κατά μία εκδοχή η απόφαση μετέτρεψε τον κόσμο των επικοινωνιών σε ένα νομικό ναρκοπέδιο. Το Δικαστήριο του Southwark αποφάσισε ότι οι δημοσιογράφοι διέπραξαν αδικήματα, παραβιάζοντας την ασφάλεια του αγγλικού συστήματος διαλογικής επεξεργασίας Prestel του αγγλικού οργανισμού τηλεπικοινωνιών σε εννέα διαφορετικές περιπτώσεις μεταξύ Οκτωβρίου 1984 και Ιανουαρίου 1985. Οι κατηγορούμενοι καταδικάστηκαν με το Νόμο κατά της Πλαστογραφίας και της Παραποίησης του 1981.

Κρίθηκε ότι υπέπεσαν στο αδίκημα της πλαστογραφίας για να επιτύχουν μη εξουσιοδοτημένη πρόσβαση στους υπολογιστές. Απαγγέλθηκαν πολλές κατηγορίες, μία εκ των οποίων ότι ο Schifreen μπήκε παράνομα σε ιδιωτική γραμματοθυρίδα του Prestel που ανήκε στον Δούκα του Εδιμβούργου και γι' αυτό πήρε ιδιαίτερη δημοσιότητα.

Τα γεγονότα που οδήγησαν στη δίκη άρχισαν πολύ εντυπωσιακά. Ο Schifreen ενώ δοκίμαζε μια συσκευή του εμπορίου συμπτωματικά

πληκτρολόγησε μια σειρά από 2 ζητώντας να συνδεθεί με το σύστημα Prestel.

Αυτό έγινε αποδεκτό από το σύστημα όπως και η πρόβλεψη ότι συνθηματικό ήταν το1234, η οποία αποδείχθηκε σωστή.

Ορισμένες ακόμα επιτυχείς προβλέψεις επέτρεψαν στο Schifreen να μπει στο σύστημα ως G. Reynolds, ο οποίος ήταν ένας υπάλληλος της British Telecom με προνομιακή πρόσβαση στο σύστημα. Αργότερα το Σεπτέμβριο ο Schifreen συνδέθηκε με έναν υπολογιστή και κατάφερε να βρει δύο ταυτότητες και συνθηματικά που ανήκαν στον "διευθυντή συστήματος" της Prestel και στον "επιμελητή συστήματος" του ίδιου οργανισμού.

Ο Schifreen συζήτησε τηλεφωνικά για το επίτευγμά του με το φίλο του Steve Gold στο Σέφιλντ, ενώ αργότερα το τηλέφωνό του άρχισε να παρακολουθείται από την British Telecom.

Ενημέρωσε επίσης και την Prestel, ενώ οι δύο δημοσιογράφοι συμφώνησαν πως η διαρροή θα έπρεπε να σταματήσει.

'Ομως ο Schifreen δεν μπόρεσε να αντισταθεί στον πειρασμό, συνέχισε να γράφει ανώνυμα άρθρα σε περιοδικά υπολογιστών και να δίνει πληροφορίες για διάφορα τηλεοπτικά ντοκυμαντέρ.

Το αποτέλεσμα ήταν να προκαλέσει την οργή της British Telecom, στελέχη της οποίας συνόδεψαν την αστυνομία για να συλλάβει τους δύο το Μάρτιο του 1985, ενώ άρχισε να διαφαίνεται και η πιθανότητα φυλάκισής τους.

Μετά το τέλος της δίκης κρίθηκαν ένοχοι, επιβλήθηκε ποινή 150 λιρών Αγγλίας για κάθε μία από τις εννέα κατηγορίες και 1.000 λίρες ορίστηκαν τα έξοδα της δίκης.

Στα τέλη του 1986 άσκησαν έφεση και η απόφαση ανατράπηκε στο Εφετείο και στη Βουλή των Λόρδων επικυρώθηκε η απόφαση του Εφετείου. Ο Λόρδος Brandon υποστηρίζοντας την απόφαση του Εφετείου

είπε ότι λέξεις "καταχωρείται" και "αποθηκεύεται" έχουν την έννοια διαδικασίας διαρκούς και συνεχούς φύσεως και επομένως δεν καλύπτουν τη στιγμιαία ύπαρξη του αριθμού ταυτότητας του πελάτη και του συνθηματικού του.

Ο Πρόεδρος του Δικαστηρίου Λόρδος Lane συμφώνησε λέγοντας ότι ενώ η συμπεριφορά των hackers ουσιαστικά αποτελούσε ανέντιμη πρόσβαση στο αρχείο δεδομένων του Prestel, αυτό δεν ήταν ποινικό έγκλημα γιατί είχε εξαπατηθεί μια μηχανή.

Πρέπει να τονίσουμε εδώ ότι σκόπιμα αναφερθήκαμε σε γεγονός του παρελθόντος, για να δείξουμε το κλίμα που επικρατούσε τότε στο χώρο των υπολογιστών και πώς αντιμετωπίζονταν προβλήματα εισβολής από τη νομική πλευρά τους, αφού σήμερα το φαινόμενο της εισβολής είναι καθιερωμένο ευρύτερα, αποτελεί κοινότυπο καθημερινό φαινόμενο και οι παραβάτες διώκονται ποινικά.

Οι περιπτώσεις απάτης και εισβολής στο χώρο των υπολογιστών σήμερα αποτελεί ακόμα και τρόπο ζωής για άτομα που εργάζονται σε αυτό το περιβάλλον, σε αντίθεση με το παρελθόν που ένα τέτοιο φαινόμενο αποτελούσε είδηση για τους δημοσιογράφους και για τα δικαστήρια της εποχής.

Η υπόθεση Michael Thompson :

Ένα "σχεδόν τέλειο έγκλημα" κατέληξε με έναν ειδικό στους υπολογιστές να φυλακίζεται για 15 μήνες με την κατηγορία ότι καρπώθηκε με απάτη το ποσό των 45.000 λιρών Αγγλίας από την "Commercial Bank of Kuwait". Μετά την έκδοση της απόφασης ο δικαστής που έκρινε την υπόθεση πληροφορήθηκε ότι η τράπεζα ξεκίνησε τη διαδικασία για την αποζημίωσή της, εκποιώντας το σπίτι του υπαιτίου.

'Εχοντας υπογράψει ένα μονοετές συμβόλαιο εκσυγχρονισμού του υπολογιστικού συστήματος της τράπεζας ο Michael Thompson έγραψε ένα πρόγραμμα το οποίο μετέφερε χρηματικά ποσά από τους λογαριασμούς πλουσίων πελατών της τράπεζας σε δικούς του λογαριασμούς στο Kuwait.

Ο Thompson φρόντιζε ώστε η συναλλαγή να γίνεται ενώ ο ίδιος πετούσε προς την Αγγλία. Φρόντιζε επίσης να εξαφανίζει από την μνήμη του υπολογιστή όλα τα ενοχοποιητικά στοιχεία.

Τα χρήματα ξοδεύτηκαν σε δύο μήνες, κύρια για την αποπληρωμή ενός στεγαστικού δανείου και για βελτιώσεις στο σπίτι του δράστη.

Η υπόθεση καταγγέλθηκε και προκάλεσε νομικό πρόβλημα, εμπλέκοντας το νόμο και τους υπολογιστές. Ο κατηγορούμενος προσέφυγε στο Εφετείο και εκεί αποκαλύφθηκαν όλα τα στοιχεία της υπόθεσης.

Ο Thompson καταδικάσθηκε πρωτόδικα για το αδίκημα της "κλοπής" γιατί καρπώθηκε περιουσιακά στοιχεία με απατηλό τρόπο.

Με δόλο προγραμμάτισε υπολογιστές στο εξωτερικό να πιστώνουν ξένους τραπεζικούς λογαριασμούς. Από το αγγλικό έδαφος ζητήθηκε η μεταφορά των ποσών σε αγγλικούς λογαριασμούς. Το ερώτημα ήταν κατά πόσο είχε καρπωθεί τα περιουσιακά στοιχεία σε Βρετανικό έδαφος.

Ο Thompson υπέβαλε έφεση εναντίον της απόφασης, υποστηρίζοντας ότι το Βρετανικό Κακουργοδικείο δεν είχε δικαιοδοσία να εκδικάσει και να πάρει απόφαση στο σύνολο του κατηγορητηρίου ή σε επιμέρους κεφάλαιά του, γιατί η κτήση των αναφερόμενων περιουσιακών στοιχείων στην πράξη ήταν μια "υπό κατηγορίαν" κτήση περιουσιακών στοιχείων τα οποία ο ίδιος είχε ήδη αποκτήσει στο Κουβέϊτ και όχι εντός της δικαιοδοσίας του Κακουργοδικείου.

Έτσι ο δικαστής που εξεδίκασε πρωτόδικα την υπόθεση έσφαλλε, απορρίπτοντας σχετική αίτηση της υπεράσπισης και στη συνέχεια αφού καθοδήγησε το σώμα των ενόρκων να δεχθεί ότι το δικαστήριο είχε τη δικαιοδοσία να εκδικάσει την υπόθεση. Τελικά όμως η καταδίκη επικυρώθηκε.

ΚΕΦΑΛΑΙΟ 8ο

ΕΤΑΙΡΙΚΟΙ ΕΛΕΓΚΤΕΣ

Ο ΡΟΛΟΣ ΤΩΝ ΕΤΑΙΡΙΚΩΝ ΕΛΕΓΚΤΩΝ

Οι εταιρικοί ελεγκτές εκδηλώνουν πάντα ενδιαφέρον για το ενδεχόμενο απάτης ή κατάχρησης. Αναλώνουν χρόνο και ενεργητικότητα στην παρακολούθηση συνεδρίων με θέματα που σχετίζονται με τα εγκλήματα των "χαρτογιακάδων". Συζητούν θέματα που σχετίζονται με την απάτη, τόσο με τους συναδέλφους τους όσο και σε συσκέψεις με ελεγκτές άλλων εταιριών.

Αναπτύσσουν αντίμετρα και σχέδια τα οποία θα ενεργοποιηθούν / εφαρμοστούν, όταν αποκαλυφθεί κάποια απάτη στην εταιρία τους.

Όλη αυτή η ενεργητικότητα όμως είναι λίγο πολύ αμυντική, γιατί όταν αποκαλυφθεί μια απάτη ή μια κατάχρηση η πρώτη ερώτηση που τίθεται είναι: "γιατί δεν αποκαλύφθηκε στον τελευταίο έλεγχο;".

Ένας καλός ελεγκτής πάντα ανησυχεί για κάτι που δεν πρόσεξε στην διάρκεια του ελέγχου. Έχει ειπωθεί ότι η συζήτηση γύρω από τα εγκλήματα των "χαρτογιακάδων" είναι μια περιττή πολυτέλεια. Αντίστοιχα ο εταιρικός έλεγχος χαρακτηρίζεται ως εγκληματολογική ανάκριση χωρίς το έγκλημα.

Οι εταιρικοί ελεγκτές οφείλουν να δείχνουν την απαιτούμενη φροντίδα κατά την διάρκεια του ελέγχου, δεν πρέπει όμως να έχουν παράλληλα και διοικητικά καθήκοντα, για το λόγο ότι η απάτη μπορεί κάλλιστα να προέρχεται και από τη διοίκηση.

Πρέπει όμως να σημειωθεί ότι η μη αποκάλυψη μιας απάτης κατά τον έλεγχο δεν σημαίνει ότι δεν έχει διαπραχθεί κάποια απάτη.

Κάθε φορά που υπάρχουν υποψίες για ανωμαλίες σε κάποια περιοχή πρέπει να ακολουθεί εξονυχιστικός έλεγχος.

Η επιβεβαίωση ότι δεν έχουν γίνει ή δεν γίνονται απάτες στο σύστημα είναι ευθύνη της διοίκησης, ακριβώς επειδή και ο αποτελεσματικός έλεγχος είναι ευθύνη δική της. Επίσης ο ρόλος του εταιρικού ελέγχου μπορεί να μεταβληθεί μετά από σχετική εντολή της διεύθυνσης.

Υπάρχουν διάφοροι λόγοι για τους οποίους εμπλέκεται ο εταιρικός έλεγχος στις ανακρίσεις για τον εντοπισμό μιας απάτης.

Πρώτον, το πρόβλημα της απάτης σε μια εταιρία είναι υπαρκτό και είναι ευθύνη των εταιρικών ελεγκτών η αντιμετώπιση τέτοιων προβλημάτων.

Δεύτερον οι τοπικές διωκτικές αρχές (Αστυνομία) δεν έχουν τις ιδιαίτερες γνώσεις και ικανότητες που απαιτούνται για την αντιμετώπιση των εγκλημάτων των "χαρτογιακάδων". Η αστυνομία συνήθως ασχολείται με άλλου είδους εγκληματικές δραστηριότητες.

Τέλος ο εταιρικός ελεγκτής είναι αυτός που θα εγκρίνει τα συστήματα της εταιρίας, αυτός είναι το τελικό εμπόδιο στην απάτη.

ΕΤΑΙΡΙΚΟΙ ΕΛΕΓΚΤΕΣ (ΑΝΑΚΡΙΤΕΣ) - ΚΙΝΔΥΝΟΙ - ΕΛΕΓΧΟΙ

Οι εταιρικοί ελεγκτές συνήθως δεν εκπαιδεύονται στις ανακριτικές μεθόδους. Στους κύκλους των ελεγκτών η τάση είναι να αποφεύγεται η στάση του "ανακριτού" στην οποία ο ελεγκτής ή ο "ανακριτής" είναι αυστηρός με την ερευνούμενη περιοχή και να

υιοθετείται μια στάση ομαδικής προσπάθειας των ελεγκτών και της διοίκησης.

Η σημερινή προσέγγιση στον έλεγχο είναι : συνεργασία και αντικειμενικότητα. Κατά συνέπεια οι εταιρικοί ελεγκτές δεν προσφέρονται για τις ανακρίσεις επί εγκληματικών ενεργειών. Ο εταιρικός έλεγχος συνήθως παρέχει απλώς μία "διαβεβαίωση εγκυρότητας" ότι τα λογιστικά βιβλία παρουσιάζουν σωστά τις δραστηριότητες της εταιρίας. Συγχρόνως όμως οι ελεγκτές έχουν πρόσβαση σε μια μεγάλη ποικιλία πληροφοριών που σχετίζονται με τον εντοπισμό και την πρόληψη της απάτης.

Κατά τη διάρκεια των μαρτυρικών καταθέσεων ενώπιον του δικαστηρίου, οι καταθέσεις θα πρέπει να αποδεικνύουν ή να διαψεύδουν τις "υπό εξέτασιν" κατηγορίες. Το δικαστήριο θα καθορίσει τί είναι ουσιώδες και σχετικό.

Η συλλογή μαρτυρικών καταθέσεων απαιτεί διαφορετική τεχνική από την παραδοσική άποψη της "εγκυρότητας" από την οποία διακατέχονται οι εταιρικοί ελεγκτές. Υπάρχουν ενδείξεις ότι μια νέα άποψη διαφαίνεται.

Πριν εδραιωθεί μια συγκεκριμένη προσέγγιση όσον αφορά τις ανακρίσεις για απάτη οι εταιρικοί ελεγκτές πρέπει πρώτα να εκτιμήσουν κατά πόσο οι ζημιές ήταν εκούσιες ή ακούσιες.

Τα σφάλματα και τα λανθασμένα στοιχεία που απορρίπτονται από ένα σύστημα είναι συχνά οι πρώτες ενδείξεις μιας απάτης. Η απάτη συνεπάγεται σκόπιμη πλάνη. Κάθε έλεγχος πρέπει να διαχωρίζει το σκόπιμο από το ακούσιο. Οι ελεγκτές πρέπει να είναι προληπτικοί και όχι "κατασταλτικοί".

Λάθη μπορούν να συμβούν σε κάθε σύστημα ή διαδικασία. Αν θέλουμε να αποφύγουμε τη σπατάλη πόρων και χρόνου είναι αναγκαίο να αναγνωρίσουμε, να εντοπίσουμε το σύστημα της εταιρίας που

βρίσκεται σε μεγαλύτερο κίνδυνο. Ποιό σύστημα δηλαδή αν παραβιαστεί συνεπάγεται τη μεγαλύτερη απώλεια περιουσιακών στοιχείων ή τη μεγαλύτερη απώλεια ακεραιότητας;

Όπου δεν υπάρχουν έλεγχοι πρέπει να θεσπιστούν και όπου υπάρχουν θα δείξουν απλώς ότι έλαβε χώρα μια απάτη ή θα μπορέσουν και να αναγνωρίσουν το χρήστη που τη διέπραξε;

Ένα αποδεκτό σύστημα εκτίμησης των κινδύνων είναι αναγκαίο. Η ύπαρξη ενός τέτοιου συστήματος θα κάνει δυνατή την ανά τακτά χρονικά διαστήματα εκτίμηση των περιοχών υψηλού κινδύνου, ώστε να διαβεβαιωθεί ότι οι προτεραιότητες των εταιρικών ελέγχων είναι επαρκείς.

Η επανεκτίμηση επιβεβαιώνει ότι οι σχετικοί έλεγχοι παραμένουν σε λειτουργία. Στην περίπτωση που τα σφάλματα τα οποία αναφέρει το σύστημα δεν μπορούν να καταγραφούν από το χρήστη, τότε ο εταιρικός έλεγχος πρέπει να ερευνήσει σε βάθος τις συνθήκες κάτω από τις οποίες έλαβαν χώρα αυτά. Αν ένα σφάλμα αποδειχθεί ότι είναι ασήμαντο, τότε μπορεί να ληφθεί πρόνοια ώστε ο εταιρικός έλεγχος να παραβλέπει αυτά τα γνωστά σφάλματα. Αν όμως ένα σφάλμα παραμένει, τότε ίσως αποτελεί ένδειξη απάτης.

Αν η ζημιά είναι σημαντική τότε προφανώς απαιτείται πλήρης έρευνα. Ο ορισμός του τί θεωρείται σημαντικό εξαρτάται από το συγκεκριμένο σύστημα και τις προτεραιότητες της εταιρίας.

Οι εταιρικοί ελεγκτές είναι σε θέση να προσδιορίσουν το σύνολο της ζημιάς που προέκυψε από ένα συγκεκριμένο συμβάν.

Μπορούν επίσης να δώσουν πληροφορίες που θα βοηθήσουν ώστε να αποδειχθεί η ζημιά με στοιχεία και μπορούν ακόμα να βοηθήσουν στην ανάπτυξη των αναγκαίων ελέγχων, ώστε να αποφευχθεί η επανάληψη του συγκεκριμένου προβλήματος.

Η ΘΕΣΗ ΤΟΥ ΕΤΑΙΡΙΚΟΥ ΕΛΕΓΚΤΗ

Η υπηρεσία του εταιρικού ελεγκτή βρίσκεται σε μια μοναδική θέση μέσα στην εταιρία. Οι εταιρικοί ελεγκτές ερευνούν για τον εντοπισμό των ασθενών σημείων του συστήματος και εισηγούνται τη διόρθωσή τους. Επιθεωρούν το σύνολο της εταιρίας και έτσι ο εταιρικός ελεγκτής βρίσκεται σε μια απαράμιλη θέση για τη διάπραξη απάτης.

Μια πρόσφατη τάση στους κύκλους των εταιρικών ελεγκτών είναι ο λεγόμενος ομότιμος έλεγχος, δηλαδή η επιθεώρηση της υπηρεσίας εταιρικού ελέγχου από επισκέπτες ελεγκτές. Υπάρχουν τρεις τύποι ομότιμου ελέγχου.

- Επιθεώρηση από εταιρικούς ελεγκτές άλλης εταιρίας του ίδιου κλάδου.
- Επιθεώρηση από εταιρικούς ελεγκτές από άλλες εταιρίες διαφορετικού κλάδου.
- Επιθεώρηση από πεπειραμένους ορκωτούς ελεγκτές που προέρχονται από εξωτερικό επαγγελματικό σώμα, το οποίο εξειδικεύεται στην διεκπεραίωση ομότιμων ελέγχων.

Το κύριο πλεονέκτημα της επιθεώρησης από εταιρικούς ελεγκτές άλλης εταιρίας του ίδιου κλάδου, είναι το ότι θα έχουν πείρα του τρόπου λειτουργίας της εταιρίας. Έτσι θα καταλάβουν τα προβλήματα που αντιμετωπίζουν οι επιθεωρούμενοι εταιρικοί ελεγκτές. Το κύριο μειονέκτημα είναι αυτό της εμπιστευτικότητας ή του εμπορικού μυστικού. Αυτό το είδος της επιθεώρησης φαίνεται να είναι λιγότερο δημοφιλές από την απευθείας επιθεώρηση που εκτελείται από εξωτερικούς ορκωτούς λογιστές. Η επιθεώρηση από εταιρκούς ελεγκτές άλλων εταιριών διαφορετικού κλάδου είναι η λιγότερο

δημοφιλής λόγω της σπουδαιότητας που αποδίδεται στη γνώση του συγκεκριμένου κλάδου.

Ο τρόπος τρόπος επιθεώρησης που χρησιμοποιεί ένα εξειδικευμένο επαγγελματικό σώμα ορκωτών λογιστών παρουσιάζει ως κύριο πλεονέκτημα το ότι αποτελεί ένα θεσμοθετημένο έλεγχο και ότι ξεπερνά τα προβλήματα της εμπιστευτικότητας και του εμπορικού μυστικού. Η ποιότητα του ελέγχου που εκτελείται από τα σώματα των ορκωτών λογιστών θεωρείται εγγυημένη. Και ως η πιο εφαρμόσιμη εναλλακτική μέθοδος επιθεώρησης έναντι των συνηθισμένων επιθεωρήσεων.

ΚΕΦΑΛΑΙΟ 9ο

ΤΕΧΝΙΚΕΣ

ΤΕΧΝΙΚΕΣ ΕΛΕΓΧΟΥ ΑΡΧΕΙΩΝ

Ο εντοπισμός και η πρόληψη της απάτης μπορεί να υποβοηθηθεί από ένα αριθμό τεχνικών για το έλεγχο των αρχείων. Μερικές από τις τεχνικές αυτές αναφέρουμε πιο κάτω.

- *Η μέθοδος των δοκιμαστικών δεδομένων :* Με τη μέθοδο αυτή επιβεβαιώνεται η ορθότητα και ακρίβεια των προγραμμάτων των εφαρμογών με τη βοήθεια δοκιμαστικών δεδομένων (test data) για τα οποία τα ορθά αποτελέσματα είναι γνωστά.

  Η μέθοδος αυτή παρέχει ένα σύστημα για την επαλήθευση των προγραμμάτων, αποτελεί δε ένα ευκολόχρηστο εργαλείο, διότι τα δεδομένα μπορούν να χρησιμοποιηθούν είτε για τον έλεγχο ενός συγκεκριμένου προγράμματος, είτε για τον έλεγχο του πακέτου προγραμμάτων συνολικά.
- *Η εκτίμηση της τυπικής περίπτωσης :* Με την τεχνική αυτή ένα τυπικό σύνολο δεδομένων χρησιμοποιείται για τον έλεγχο της εφαρμογής. Το τυπικό σύνολο των δεδομένων ορίζεται από το χρήστη του συστήματος ως οδηγός για τον έλεγχο της ορθής λειτουργίας της εφαρμογής. Αυτή η τεχνική ελέγχου χρησιμοποιείται ευρέως για την επικύρωση των συστημάτων παραγωγής.
- *Παράλληλη λειτουργία :* Με τη μέθοδο αυτή χρησιμοποιούνται ένα ή περισσότερα προγράμματα για την επεξεργασία πραγματικών

δεδομένων και την προσομείωση την "κανονικής" λειτουργίας του υπολογιστή.

Η μέθοδος αυτή χρησιμοποιεί πραγματικά δεδομένα με δοκιμαστικά προγράμματα. Τα προγράμματα παράλληλης εκτέλεσης αφορούν την "λογική" της εφαρμογής, τους υπολογισμούς και τους ελέγχους που σχετίζονται με το συγκεκριμένο θέμα που ενδιαφέρει τον εταιρικό έλεγχο. Μεγάλα τμήματα μιας βασικής εφαρμογής μπορούν συχνά να προσομειωθούν με σκοπό το λογιστικό έλεγχο με ένα απλό πρόγραμμα παράλληλης εκτέλεσης. Η παράλληλη λειτουργία επιτρέπει στον ελεγκτή να επαληθεύσει ανεξάρτητα, σύνθετα και "κρίσιμα" προγράμματα εφαρμογών.

- *Επιλογή συναλλαγών :* Η τεχνική της επιλογής συναλλαγών με σκοπό τον έλεγχο, χρησιμοποιεί ένα ανεξάρτητο πρόγραμμα για την επιλογή των προς επιθεώρηση συναλλαγών. Η μέθοδος αυτή επιτρέπει στον ελεγκτή να εξετάσει και να αναλύσει τους "όγκους" των συναλλαγών και τους "ρυθμούς" των σφαλμάτων.

  Επίσης του δίνει τη δυνατότητα να πάρει στατιστικά δείγματα συγκεκριμένων συναλλαγών. Το λογισμικό για την επιλογή των συναλλαγών είναι ανεξάρτητο από το λογισμικό των εφαρμογών.
- *Προγράμματα γενικευμένου ελέγχου :* Η χρήση των προγραμμάτων γενικευμένου ελέγχου αποτελεί τη συχνότερη χρησιμοποιούμενη τεχνική για τον έλεγχο των εφαρμογών του υπολογιστή. Τα προϊόντα αυτά επιτρέπουν στον ελεγκτή να αναλύσει ανεξάρτητα κάθε αρχείο μιας εφαρμογής. Τα περισσότερα πακέτα γενικευμένου ελέγχου είναι αξιόπιστα, ευέλικτα και καλά τεκμηριωμένα.

  Παρέχουν έτσι στον ελεγκτή πολλές δυνατότητες για τον ουσιαστικό έλεγχο του συστήματος. Σε γενικές γραμμές οι τεχνικές αυτές χρησιμοποιούνται για τον έλεγχο των αρχείων δεδομένων.

- *Διάγραμμα ελέγχου :* Σε ένα σύνθετο επιχειρηματικό περιβάλλον είναι δύσκολο να κατανοηθεί με λεπτομέρεια το όλο σύστημα ελέγχου του οργανισμού μέσα στο συνολικό επιχειρηματικό και λειτουργικό περιβάλλον. Μια γραφική τεχνική ή ένα διάγραμμα για την απλοποίηση και τον εντοπισμό των αμοιβαίων σχέσεων των διαφόρων ελέγχων μπορεί να αποδειχθεί μεγάλο βοήθημα στην εκτίμηση της επάρκειας των ελέγχων, καθώς και στην εκτίμηση των επιπτώσεων των μεταβολών του συστήματος στο συνολικό έλεγχο. Τα διαγράμματα ελέγχου βοηθάνε τον ελεγκτή να κατανοήσει τους ελέγχους καθώς και να διαπιστώσει εάν οι έλεγχοι λειτουργούν σύμφωνα με τις προδιαγραφές τους.
- *Συγκριτική εξέταση κώδικα :* Με τον όρο αυτό περιγράφεται η σύγκριση δύο αντιγράφων του αυτού προγράμματος μιας συγκεκριμένης εφαρμογής, τα οποία έχουν ληφθεί σε διαφορετικές χρονικές στιγμές.

  Στόχος αυτής της τεχνικής είναι να επαληθευτεί ότι έχουν τηρηθεί επακριβώς οι διαδικασίες μετατροπών και συντήρησης του προγράμματος, καθώς και οι διαδικασίες των βιβλιοθηκών του συστήματος. Ο ελεγκτής χρησιμοποιεί τα αποτελέσματα της σύγκρισης, με σκοπό να εντοπίσει τις μετατροπές που έχει υποστεί το πρόγραμμα στο χρονικό διάστημα που μεσολάβησε μεταξύ της λήψης του πρώτου και του δεύτερου αντιγράφου.

  Η τεχνική αυτή προσφέρεται για τον έλεγχο της τήρησης των διαδικασιών,αλλά δεν μπορεί να αποτελέσει την ουσιαστική μέθοδο ελέγχου.

  Η σύγκριση του κώδικα είναι ιδιαίτερα χρήσιμη για τον έλεγχο προγραμμάτων, τα οποία αφενός εκτελούν κρίσιμες λειτουργίες της επιχείρησης, αφετέρου δε υπόκεινται σε συνεχείς μετατροπές.

- *Έλεγχος ακεραιότητας αρχείων :* Τα συστήματα υπολογιστών, πρέπει να υφίστανται τακτικό έλεγχο με σκοπό να επιβεβαιώνεται ότι διατηρούν ένα ελάχιστο επίπεδο χαρακτηριστικών τα οποία συνεισφέρουν στην ακεραιότητα και αποδοτικότητά τους. Κατά πρώτον απαιτούνται έλεγχοι ώστε να επιβεβαιωθεί ότι όλες οι ασυνήθεις περιπτώσεις, που αντιμετωπίζονται από ένα αυτοματοποιημένο σύστημα, αναφέρονται από το λογισμικό του συστήματος με σκοπό τον εντοπισμό, την αναφορά και την αντιμετώπιση κάθε ανωμαλίας, με τρόπο που να μην διακόπτεται η ροή του συστήματος, ενώ εξασφαλίζεται παράλληλα η ακεραιότητά του.

  Η ελεγκτική συνέχεια είναι η έμμονη ιδέα κάθε εταιρικού ελεγκτή. Όλα τα συστήματα πρέπει να διαθέτουν διαδικασίες ελεγκτικής συνέχειας, τόσο για τις χειροκίνητες όσο και για τις αυτοματοποιημένες λειτουργίες τους.

  Οι έλεγχοι που γίνονται στο σύστημα πρέπει να έχουν τη δυνατότητα να εντοπίζουν και να αναφέρουν το τέλος της εργασίας, είτε αυτό είναι επιτυχές είτε είναι ανώμαλο. Οι περιοχές λειτουργίας του υπολογιστή πρέπει να εκτιμώνται και να καταγράφονται με σκοπό την αναφορά και καταγραφή των ενδεχόμενων σφαλμάτων ή ανωμαλιών που λαμβάνουν χώρα κατά την επεξεργασία. Πρέπει επίσης να διατηρούνται όπου είναι δυνατό μόνιμες εγγραφές των σφαλμάτων και των παραλείψεων που εντοπίζονται κατά τη λειτουργία του υπολογιστή, ώστε να είναι διαθέσιμες για μελλοντική εξέταση.

ΚΕΦΑΛΑΙΟ 10ο

ΠΡΟΣΤΑΣΙΑ - ΑΠΟΖΗΜΙΩΣΗ ΑΠΟ ΑΠΑΤΗ ΣΤΟ ΧΩΡΟ ΤΩΝ Η/Υ

ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΕΝΔΕΧΟΜΕΝΗ ΑΠΑΤΗ

Η εργοδοσία πρέπει να λαμβάνει τα παρακάτω μέτρα, ώστε να προστατεύεται από κλοπές και απάτες :

- να ερευνά όλα τα παράπονα και τις ανωμαλίες,
- να χρησιμοποιεί μέτρα φυσικής διασφάλισης (physical security), ώστε να μειώνονται οι κίνδυνοι,
- να χρησιμοποιεί κατάλληλες μεθόδους επιλογής προσωπικού,
- να μεταθέτει το προσωπικό, ώστε να αναλαμβάνει διάφορους τομείς ευθυνών,
- να εμποδίζει την πρόσβαση στα φυλασσόμενα αρχεία,
- να ευαισθητοποιείται από τα παράπονα των πελατών και τα προβλήματα των εργαζομένων,
- να γνωρίζει τα μέλη του προσωπικού που είναι δυσαρεστημένα,
- να αναθέτει την ευθύνη για την ασφάλεια σε κάποιο συγκεκριμένο άτομο,
- να επεμβαίνει όταν δημιουργούνται προβλήματα,
- να ενθαρρύνει τη συμμετοχή των εργαζομένων σε θέματα ασφαλείας,
- να έχει καλές σχέσεις με την αστυνομία,
- να στηρίζει τα πρότυπα και τις διαδικασίες της εταιρίας, χωρίς φόβο ή διακρίσεις,
- να προβλέπει τα προβλήματα.

ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΑΠΟΤΡΟΠΗ ΤΗΣ ΕΙΣΒΟΛΗΣ

Υπάρχουν ορισμένες διαδικασίες που μπορούν να υιοθετηθούν, ώστε να δυσκολέψουν την μη εξουσιοδοτημένη εισβολή και τις οποίες θα σας παρουσιάσουμε :

1. Η δυνατότητα των συνδέσεων μέσω επιλεγόμενης γραμμής πρέπει να περιοριστεί στο ελάχιστο. Αν υπάρχει τέτοια δυνατότητα θα πρέπει να κρατηθεί έξω από το σύστημα. Δηλαδή θα πρέπει η επιλογή της σύνδεσης με τον υπολογιστή να γίνεται μετά από τηλεφωνική επαφή του χρήστη με τον υπεύθυνο του συστήματος, ώστε να επιβεβαιωθεί το δικαίωμα σύνδεσης. Στη συνέχεια ο χρήστης πρέπει να κληθεί από το σύστημα, ως μία περαιτέρω επιβεβαίωση του ότι η αίτηση σύνδεσης προέρχεται από έναν εξουσιοδοτημένο αριθμό.

   Πρέπει εντούτοις να αναγνωρισθεί ότι σε ορισμένες συνθήκες ο αριθμός των αιτώμενων συνδέσεων είναι τόσο μεγάλος, που τέτοιος έλεγχος είναι αδύνατος.
2. Οι τηλεφωνικοί αριθμοί του συστήματος, οι αριθμοί ταυτότητας χρήστη δικτύο (NUI) και οι διεθύνσεις χρήστη δικτύου (NUA) του PSS πρέπει να φυλάσσονται όσο το δυνατόν σχολαστικότερα.
3. Θα πρέπει να εξετασθεί το ενδεχόμενο χρήσης της ειδικής συσκευής, η οποία καλεί τον "αιτούντα σύνδεση".
4. Οι τυπικοί αριθμοί ταυτότητος χρήστη δικτύου (NUI) δεν πρέπει να χρησιμοποιούνται.
5. Μια σειρά από ελέγχους πρέπει να εφαρμόζεται αναφορικά με τα συνθηματικά. Τα συνθηματικά πρέπει :
   - να έχουν μήκος τουλάχιστον 6 αλφαρηθμητικών χαρακτήρων,
   - να αλλάζουν τακτικά,

- να μην σχετίζονται με κανένα τρόπο με το χρήστη, ώστε να μην είναι εύκολο να τα μαντέψει κάποιος.

6. Οι απόπειρες μη εξουσιοδοτημένης προσπέλασης πρέπει να ελέγχονται και να ερευνώνται. Μετά από δύο ανεπιτυχείς απόπειρες, ο χρήστης πρέπει να αποσυνδέεται από το σύστημα και η ταυτότητά του να ακυρώνεται.

ΠΙΣΤΗ ΕΡΓΑΖΟΜΕΝΩΝ ΚΑΙ ΑΣΦΑΛΙΣΗ

Οι υπολογιστές εκλετούν πολλές και ποικίλες εργασίες, μερικές από τις οποίες είναι τρομερά περίπλοκες. Οι υπολογιστές επίσης έχουν δημιουργήσει μια τεράστια ποικιλία νεών δυνατοτήτων για εγκληματικές πράξεις, δυνατότητες που πριν ήταν αδιανόητες και υπάρχουν άνθρωποι δόλιοι που εργάζονται συνεχώς για την εκμετάλλευση αυτών των δυνατοτήτων.

Οι μεγάλοι οικονομικοί οργανισμοί, ειδικότερα οι τράπεζες, είναι αυτοί που κύρια θίγονται, μιας και βασίζονται σε περίπλοκα δίκτυα υπολογιστών (computers networks) που έχουν επεκταθεί σε όλο τον κόσμο συνδέοντας πολλές τράπεζες μεταξύ τους. Οι τράπεζες προσπαθώντας να προσφέρουν στους πελάτες τους τις υπηρσίες που αυτοί απαιτούν, αναγκάζονται να επιταχύνουν το ρυθμό διεκπεραίωσης των συναλλαγών. Οι συναλλαγές δεν εγκρίνονται πια μόνο με την υπογραφή, όπως στις επιταγές. Όλο και περισσότερο η έγκριση γίνεται με τη βοήθεια των επικοινωνιών, των τέλεξ και των εντολών του υπολογιστή. Ο μη ειδικός πολύ δύσκολα μπορεί να αντιληφθεί την κλίμακα και τον όγκο αυτών των λειτουργιών.

Οι τράπεζες απολαμβάνουν ιδιαίτερης μεταχείρισης όσον αφορά τη γενική ασφαλιστική κάλυψη, λόγω του ότι το εμπόρευμά τους είναι πολύ διαφορετικό από αυτό των άλλων επιχειρήσεων.

Το εμπόρευμα των τραπεζών είναι πολύτιμα περιουσιακά στοιχεία όπως ρευστό, επιταγές, νομίσματα, χρυσός, χρεώγραφα και κάθε μορφή μεταβιβάσιμου αξιόγραφου.

Για να ικανοποιήσει τις ιδιαίτερες ανάγκες των τραπεζών, ο ασφαλιστικός κλάδος κατέστρωσε ένα συμβόλαιο κάλυψης, γνωστό ως "Bankers' Blanket Bond".

Το συμβόλαιο αυτό αποσκοπεί στο να καλύψει συγκεκριμένους κινδύνους από εγκληματικές ενέργειες όπως για παράδειγμα ανέντιμες πράξεις εργαζομένων, κλοπές, κλοπές μεταφερόμενων αγαθών, απάτες και πλαστογραφίες.

Η εμπλοκή της Πληροφορικής και της τεχνολογίας των υπολογιστών έχει δημιουργήσει πολλά παραθυράκια στην κάλυψη που παρέχει το παραπάνω συμβόλαιο.

Για παράδειγμα οι έννοιες της "ιδιοκτησίας", του "εργαζόμενου" και της "πλαστογραφίας" έχουν διερευνηθεί ώστε να αποκτήσουν ασφαλιστική κάλυψη για τις περιπτώσεις των αδικημάτων που διαπράττονται με τον υπολογιστή ή και των αδικημάτων που σχετίζονται με αυτόν.

Ο ασφαλιστικός κλάδος ανταποκρίθηκε, αναγνωρίζοντας ότι η κάλυψη των συστημάτων ηλεκτρονικής διακίνησης χρήματος απαιτεί μια τελείς διαφορετική προσέγγιση από αυτή του συμβολαίου "Banker's Blanket Bond".

Τον Οκτώβριο του 1981 παρουσιάστηκε το ασφαλιστήριο συμβόλαιο γνωστό ως "Lloyd's Electronic and Computer Crime Insurance Policy". Το συμβόλαιο αυτό απευθύνεται στα χρηματιστικά ιδρύματα και πιο ειδικά στις Τράπεζες, αλλά και σε άλλους εμπορικούς

οργανισμούς. Σχηματίστηκε μια κοινοπραξία χρηματιστών με σκοπό την υποστήριξη της αναγκαίας έρευνας και ανάπτυξης (R & D) για την αντιμετώπιση των αναγκών της νέας ασφαλιστικής κάλυψης.

Η ερευνητική ομάδα μελέτησε την αύξηση του αριθμού των εγκατεστημένων υπολογιστών για μια περίοδο 10 ετών και έκανε μια πρόβλεψη για την αύξηση στα επόμενα 5 χρόνια.

Η έκθεση της ομάδας διαιρούσε τις υπηρεσίες των οικονομικών οργανισμών σε διάφορες κατηγορίες και η κάθε κατηγορία διαιρείτο στις συνισταμένες λειτουργίες για τον εντοπισμό των αντίστοιχων κινδύνων. Με λίγα λόγια επιχειρήθηκε μια εκτίμηση των κινδύνων. Εντοπίστηκαν οι ενδεχόμενοι κίνδυνοι τόσο στο σύστημα του υπολογιστή όσο και στη λειτουργία του.

Το αποτέλεσμα ήταν να εντοπισθεί μεγάλος αριθμός κινδύνων, από τους οποίους όλοι συνεπάγονταν ζημιές για τις οποίες το συμβόλαιο "Banker's Blanket Bond" ήταν τελείως ακατάλληλο. Το νέο προτεινόμενο συμβόλαιο λοιπόν, εκλήθη να καλύψει αυτά τα παραθυράκια. Παρέχεται κάλυψη για ζημιές που οφείλονται σε δόλια εισαγωγή δεδομένων, σε μη εξουσιοδοτημένη πρόσβαση στα τερματικά του υπολογιστή, σε δόλια δεδομένα και προγράμματα, ή και για ζημιές που οφείλονται σε υποκλοπές στα τραπεζικά δίκτυα υπολογιστών.

Η πίστη των εργαζομένων εξακολουθεί να καλύπτεται από το συμβόλαιο "Banker's Blanket Bond". Το παρόν ασφαλιστήριο συμβόλαιο καλύπτει και τις ζημιές που οφείλονται σε δόλιες ενέργειες, όπου δεν υπάρχει σκόπιμο χρηματικό όφελος από μέρους του υπαιτίου.

Το συμβόλαιο "Electronic and Computer Crime Insurance Policy" πιθανότατα υφίσταται συνεχείς μεταβολές στην κάλυψη, καθώς οι ασφαλιστές αναθεωρούν συνεχώς τους ενδεχόμενους κινδύνους. Οι ασφαλιστές, έχοντας πλήρη συναίσθηση όλων των πιθανών επιπτώσεων της απάτης και του αδικήματος με υπολογιστή, είναι

πεπεισμένοι ότι αυτό το ειδικό συμβόλαιο θα ικανοποιήσει τις ανάγκες των χρηστών.

ΤΟ ΔΙΚΑΙΩΜΑ ΤΗΣ ΑΠΟΖΗΜΙΩΣΗΣ

Κάθε εταιρία που έχει πέσει θύμα απάτης, λογικό είναι να επιθυμεί να αποζημιωθεί. Πρέπει όμως να λαμβάνεται υπόψη ότι αυτή η αποζημίωση μπορεί να απαιτεί μια ιδιαίτερα χρονοβόρα διαδικασία. Οι ένοχοι κλοπής συχνά είναι προετοιμασμένοι να αποδεχθούν την απόλυσή τους, μπορεί ακόμα και να βοηθήσουν στην υποβολή μήνυσης αποδεχόμενοι την ενοχή τους για τις κατηγορίες. Θα υποχωρήσουν όμως όταν αντιμετωπίσουν το ενδεχόμενο της οικονομικής αποζημίωσης που πιθανότατα θα υπερκαλύπτει το σύνολο των περιουσιακών τους στοιχείων.

Η απόφαση της διοίκησης να διατηρήσει στο προσωπικό της εταιρίας τους ενόχους μικροαδικημάτων μπορεί να είναι μια φρόνιμη απόφαση.

Η απόλυση κάθε υπαιτίου μπορεί κάλλιστα να οδηγήσει την εταιρία σε πλήρη ακινησία ή απλώς να είναι μια ενέργεια αντιπαραγωγική. Όσον αφορά τους ενόχους μικροαδικημάτων που παραμένουν στην εταιρία, πρέπει να γίνει κατανοητό από όλους τους εμπλεκόμενους ότι θα πρέπει να έχουν συμφωνηθεί αμοιβαία η ενδεχόμενη αποζημίωση και το ύψος της. Στις περιπτώσεις που η διοίκηση εκτιμά ότι ο ένοχος απάτης έχει περιουσιακά στοιχεία τέτοια που μπορούν να καλύψουν την οφειλή, η διοίκηση ίσως προσφύγει στην δικαιοσύνη. Στην περίπτωση "ενόχων με πρότερο έντιμο βίο", το δικαστήριο πιθανότατα θα θεωρήσει την αποζημίωση ως προϋπόθεση, προκειμένου να επιβάλλει ποινή με "αναστολή".

Εντούτοις η διοίκηση δεν πρέπει να εμφανίσει ενώπιον του δικαστηρίου ότι χρησιμοποιεί τα ποινικά δικαστήρια για να αποζημιωθεί, κάτι που θα μπορούσε να επιδιώξει μέσω των αστικών δικαστηρίων. Δεν πρέπει να γίνεται κατάχρηση των δικαστικών υπηρεσιών και η μετατροπή τους σε υπηρεσίες είσπραξης οφειλών.

Η διοίκηση θα μπορούσε να υιοθετήσει τη θέση ότι το κύριο ενδιαφέρον της είναι η επιβολή της δικαιοσύνης, ενώ το ενδιαφέρον της για αποζημίωση είναι δευτερεύον. Το σύστημα ποινικής δίωξης μπορεί να βοηθήσει την θιγείσα εταιρία, ενώ στην συνέχεια και μετά το πέρας της έρευνας και της δίωξης για το έγκλημα, μπορεί να διεκδικήσει αποζημίωση μέσω των αστικών δικαστηρίων.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Κύριες πηγές που χρησιμοποιήθηκαν είναι ονομαστικά :

1. Βασιλάκη Ειρήνη : "Πειρατεία Προγραμμάτων και Άρθρα 16, 17 Ν. 146/14".

2. Μυλωνοπούλου Χρ. : "Η εγκληματικότητα στο χώρο των υπολογιστών) (Οικ. Ταχ. 24/11/1988).

3. Σπενέλλη Α. : "Κίνδυνοι των πληροφοριακών συστημάτων από ανθρώπινη συμπεριφορά και τρόποι ποινικής προστασίας" (Γραπτή εισήγηση στη Διεθνή Ημερίδα για την ασφάλεια και προστασία των πληροφοριακών συστημάτων, στο Ζάππειο).

4. Πιπεράκη Α. : "Η ποινική προστασία του Λογισμικού στην Μ. Βρετανία" (Ισχύον Δίκαιο).

5. Hugo Cornwall : "Το νέο εγχειρίδιο του εισβολέα". "Αποσπάσματα από Οικ. Ταχυδρόμος και από άρθρα που αφορούν την νομική προστασία των πληροφοριακών συστημάτων".