Διοίκηση Πληροφορικών Συστημάτων

Ασφάλεια Συστημάτων

Περιεχόμενα

ΣΤΟΧΟΙ ΚΕΦΑΛΑΙΟΥ

Θέμα

Ποιες είναι οι απειλές ασφάλειας για τους οργανισμούς

Πως μπορούμε να διαχειριστούμε τις απειλές αυτές

Στόχος

- Περιγραφή των ακούσιων απειλών που προκαλούνται από αμέλεια ή αφέλεια υπαλλήλων και συνεργατών
- Περιγραφή των σκόπιμων απειλών, εσωτερικών και εξωτερικών που προκαλούνται από κακόβουλους υπάλληλους ή τρίτα μέρη
- Αξιολόγηση των στρατηγικών διαχείρισης κινδύνων ασφάλειας
- Καθορισμός των ελέγχων που πρέπει να διεξάγουν οι οργανισμοί, και των πολιτικών που πρέπει να έχουν σε λειτουργία
- Περιγραφή επιλεγμένων εργαλείων για βελτίωση της ασφάλειας των πληροφοριών και συστημάτων των οργανισμών

ΕΠΙΣΚΟΠΗΣΗ/ΟΡΙΟΘΕΤΗΣΗ ΖΗΤΗΜΑΤΩΝ ΑΣΦΑΛΕΙΑΣ

Ακούσιες απειλές

Φυσικές Καταστροφές
- Σεισμοί, πλημμύρες

Ανθρώπινα Ατυχήματα
- Πυρκαγιές,

Περιβάλλον

Σκόπιμες απειλές

Επιθέσεις από Internet
- Κακόβουλο λογισμικό (ιοί)
- Denial-of-service
- Hackers

Social Engineering
- Phishing
- υφαρπαγή ευαίσθητων πληροφοριών με δόλο

Οργανισμός

Λάθη Υπαλλήλων
- Θύματα social engineering
- Λάθος χειρισμός passwords

Λάθη Προγραμματιστών
- Λάθος εξουσιοδοτήσεις
- Παράκαμψη μεθόδων ασφάλειας

Λογισμικό
- Κενά ασφαλείας
- Μη ενημερωμένο λογισμικό

Κακόβουλοι Υπάλληλοι
- Κλοπή ευαίσθητων πληροφοριών για ίδιο οικονομικό όφελος
- Σκόπιμες καταστροφές για λόγους εκδίκησης

Κακόβουλοι Συνεργάτες
- Μη εξουσιοδοτημένη πρόσβαση / κλοπή από συμβούλους, εργολάβους, εξωτερικούς συνεργάτες

Εξελίξεις

- Διασυνδεδεμένο, ασύρματα **δικτυωμένο επιχειρηματικό περιβάλλον**
- **Νόμος του Moore**: μικρότεροι, ταχύτεροι, φθηνότεροι υπολογιστές και συσκευές αποθήκευσης
- **Διεθνές οργανωμένο έγκλημα** και αύξηση ευκαιριών για αποκομιδή κέρδους
- **Μείωση του πήχη για hacking**, με αυτοματοποιημένα εργαλεία βιομηχανικής κλίμακας

Περιεχόμενα

ΑΝΘΡΩΠΙΝΕΣ ΑΚΟΥΣΙΕΣ ΑΠΕΙΛΕΣ

Πηγή προβλημάτων

Πηγή λαθών	Υπάλληλοι	Τεχνικοί / Προγραμματιστές	Διαδικασίες
Αμέλεια	▪ Λάθος χειρισμός passwords ▪ Χαλαρή ασφάλεια (γραφείο, φορητές συσκευές) ▪ Χρήση προσωπικών USB ▪ Απρόσεκτη περιήγηση στο Internet	▪ Παράκαμψη μεθόδων ασφάλειας, συνήθως με στόχο τη έγκαιρη παράδοση κώδικα/ project/ υπηρεσίας ▪ Μη επικαιροποίηση βιβλιοθηκών λογισμικού, λειτουργικού συστήματος, και άλλου λογισμικού κρίσιμης σημασίας	▪ Απουσία εκπαίδευσης ▪ Απουσία σχεδίου χειρισμού κρίσεων ▪ Απουσία εσωτερικών ελέγχων
Αφέλεια/ Έλλειψη κατάρτισης	▪ Θύματα social engineering ▪ Θύματα phishing ▪ Εκτέλεση εξωτερικού κώδικα στην εταιρία	▪ Εγκατάσταση μη ασφαλούς λογισμικού ▪ Έλλειψη γνώσεων για τις τελευταίες απειλές ▪ Θεώρηση των θεμάτων ασφάλειας ως δευτερεύοντα	▪ Αδυναμία αναγνώρισης των πραγματικών κινδύνων ▪ Μη παροχή κινήτρων για θωράκιση των συστημάτων

- Οι περισσότερες ακούσιες απειλές είναι δυνατό να ελαχιστοποιηθούν με εξειδικευμένη εκπαίδευση του προσωπικού και των τεχνικών
- Είναι εφικτό για την εταιρία να μετρήσει τον κίνδυνο με «στοχευμένες» δοκιμές

Περιεχόμενα

ΣΚΟΠΙΜΕΣ ΕΠΙΘΕΣΕΙΣ ΣΕ ΕΤΑΙΡΙΕΣ

Ακολουθούν λεπτομέρειες

Τύπος επίθεσης	Περιγραφή
Κατασκοπία	▪ Ανταγωνιστές, οι άλλες εταιρίες έχουν οικονομικό όφελος από πρόσβαση σε ευαίσθητες πληροφορίες της εταιρίας-στόχου
Εκβιασμός	▪ Χρήση ευαίσθητων πληροφοριών ή άλλων απειλών για χρηματικό εκβιασμό. Όλο και συχνότερα με χρήση ηλεκτρονικών νομισμάτων (π.χ. bitcoin)
Βανδαλισμός	▪ Καταστροφές σε υποδομές η υπηρεσίες με σκοπό την εκδίκηση, πολιτικά κίνητρα, ή και χωρίς ιδιαίτερο σκοπό
Κλοπή εξοπλισμού	▪ Αυξανόμενοι κίνδυνοι από κλοπή έξυπνων κινητών και tablets υπαλλήλων που συχνά περιέχουν ευαίσθητα εταιρικά δεδομένα
Κλοπή κωδικών/ ταυτότητας	▪ Η κλοπή κωδικών από υπαλλήλους (π.χ., με phishing) συνήθως οδηγεί σε πρόσβαση σε ευαίσθητες εταιρικές πληροφορίες, ή στην κλοπή περισσότερων κωδικών, ή και στην εγκατάσταση κακόβουλου λογισμικού
Social Engineering	▪ Χρήση κοινωνικών δεξιοτήτων για εξαπάτηση υπαλλήλων με σκοπό την υφαρπαγή πληροφοριών που μπορεί να χρησιμοποιηθούν για μελλοντικές επιθέσεις
Επιθέσεις λογισμικού	▪ Πλήθος διαφορετικών τύπων επιθέσεων, από ιούς και keyloggers, μέχρι denial of service (άρνηση υπηρεσίας) και botnets
Κυβερνοπόλεμος	▪ Σκοπός η πρόκληση ζημιάς και οι καταστροφές στη φυσική υποδομή της εταιρίας (π.χ., επιθέσεις σε συστήματα SCADA) ή στη δυνατότητά της να λειτουργεί κανονικά

SOCIAL ENGINEERING (ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ)

Περιγραφή

Ορισμός

- χρήση κοινωνικών δεξιοτήτων για εξαπάτηση υπαλλήλου/υπαλλήλων προκειμένου να αποσπαστούν εμπιστευτικές πληροφορίες με στόχο την προσπέλαση σε Π.Σ. της εταιρείας, π.χ. κωδικοί πρόσβασης, ονόματα, αριθμός ταυτότητας, κτλ...

Συνήθεις Τεχνικές

- Phishing
- Ο επιτιθέμενος υποδύεται υπάλληλο της εταιρίας από άλλο γραφείο, ανώτερο στέλεχος, εξειδικευμένο προσωπικό, κλπ
- Ο επιτιθέμενος επικοινωνεί με το help-desk ή άλλο τεχνικό προσωπικό και ζητά πρόσβαση σε ευαίσθητες πληροφορίες

Παράδειγμα Phishing

Αποτελεσμα-τικότητα

- Εκτός αν το προσωπικό της εταιρίας έχει εκπαιδευτεί σε τέτοιου είδους επιθέσεις, και εκτός αν γίνονται τακτικά «ασκήσεις» σε ευαίσθητα σημεία όπως το helpdesk, η τακτική αυτή έχει αποδειχθεί εξαιρετικά σημαντική

ΕΠΙΘΕΣΕΙΣ ΛΟΓΙΣΜΙΚΟΥ (1/2)

Τύπος επίθεσης	Περιγραφή	Λεπτομέρειες
Ιοί	▪ Κακόβουλο πρόγραμμα που λειτουργεί εν άγνοια του χρήστη ▪ Συνήθως προσπαθεί να δημιουργήσει αντίγραφα του εαυτού του (ιός) σε άλλους υπολογιστές μέσω δικτύου ή άλλων μέσων (π.χ., USB drives) ▪ Πιθανή επαφή με κέντρο ελέγχου για οδηγίες (π.χ., μετάλλαξη)	• **Attack vector** (τρόπος εισόδου) μπορεί να είναι άλλος ιός, κενό ασφάλειας στο λειτουργικό σύστημα, μολυσμένο website, κλπ • Το **payload** (σκοπός/λειτουργία) μπορεί να αποσκοπεί στη συλλογή στοιχείων, click fraud, botnets, ID theft, ransomware, κλπ • Οι εταιρίες antivirus φαίνεται πως είναι ένα βήμα πίσω (μικρό ποσοστό ανιχνευσιμότητας των επικίνδυνων ιών όπως τα rootkits)
Denial of Service	▪ Ο επιτιθέμενος χρησιμοποιεί επίτηδες τους πόρους της εταιρίας σε τεράστια κλίμακα, με σκοπό να είναι αδύνατη η εξυπηρέτηση νόμιμων χρηστών. Π.χ. 10,000 requests το δευτερόλεπτο στο website της εταιρίας που συνήθως έχει τόσες επισκέψεις την ημέρα ▪ Οι επιθέσεις είναι συνήθως κατανεμημένες (π.χ., με χρήση botnets) προκειμένου να είναι αδύνατο για το στόχο απλά να αγνοήσει την πηγή	• Συνήθη κίνητρα αποτελούν πολιτικά κίνητρα, βανδαλισμός, χρηματικός εκβιασμός, διευκόλυνση άλλων (ταυτόχρονων) επιθέσεων • Πιθανή άμυνα (ως ένα βαθμό) αποτελούν οι εταιρίες Content Delivery Networks (π.χ. Akamai) με χρήση proxies και άλλων μεθόδων που αφαιρούν το βάρος της επίθεσης από τον ευαίσθητο πόρο (π.χ. από το website της εταιρίας)

ΕΠΙΘΕΣΕΙΣ ΛΟΓΙΣΜΙΚΟΥ (2/2)

Τύπος επίθεσης	Περιγραφή	Λεπτομέρειες
Password attack	▪ Δοκιμή μεγάλου αριθμού από passwords μέχρι να βρεθεί ο σωστός κωδικός ▪ Διευκολύνεται από το γεγονός πως οι περισσότεροι χρήστες επιλέγουν passwords που είναι μικρές παραλλαγές λέξεων που υπάρχουν στο λεξικό ▪ Brute force για passwords μέχρι 8-10 χαρακτήρες	• Μπορεί να είναι online (live) ή offline (αν έχει υποκλαπεί το αρχείο με τα κωδικοποιημένα passwords) • Πιθανή άμυνα: απενεργοποίηση λογαριασμών μετά από λάθος καταχωρήσεις. Αρνητικά: επιτρέπει σε κακόβουλους να απενεργοποιήσουν όλους τους λογαριασμούς των χρηστών και δεν βοηθά σε offline επιθέσεις • Προωθείται όλο περισσότερο η λύση του "two-factor authentication"
Παρασιτικό λογισμικό	▪ Λαθραίο λογισμικό που εγκαθίσταται σε έναν υπολογιστή συνήθως μέσω 3ου λογισμικού - Adware - Spamware - Cookies (με μοναδικό σκοπό την καταγραφή της δραστηριότητας στο Internet)	• Συνήθως αποτελεί «ενόχληση» με σκοπό το βομβαρδισμό του χρήστη με διαφημίσεις και αμφιβόλου ποιότητας προσφορές • Σε πολλές όμως περιπτώσεις μπορεί να αποτελεί πραγματικό κίνδυνο. Π.χ., μπορεί να περιλαμβάνει spyware (π.χ., keystroke loggers) που θέτουν σε κίνδυνο τις οικονομικές συναλλαγές του χρήστη, ή μπορεί να αποτελέσει τρόπο εισόδου για ιούς

CASE STUDY: ΕΠΙΘΕΣΗ ΛΟΓΙΣΜΙΚΟΥ ΣΤΗΝ TARGET (ΝΟΕΜΒΡΙΟΣ-ΔΕΚΕΜΒΡΙΟΣ 2013)

Ελλιπής Προστασία

Η "βιτρίνα" της Target

- Η Target ακολουθούσε και διαφήμιζε το PSI πρότυπο για τη διαχείριση πιστωτικών καρτών (π.χ., μη αποθήκευση αριθμών πελατών στους servers της εταιρίας)

Και οι διάτρητοι εσωτερικοί μηχανισμοί...

- Χρήση απλών μαγνητικών καρτών (χωρίς PIN/chip)
- Εσωτερικά συστήματα της Target δεν είχαν ενημερωθεί για γνωστά κενά ασφαλείας
- Οι hackers χρησιμοποιούσαν τεχνικές ανίχνευσης εσωτερικών αδυναμιών χωρίς να ασχοληθεί κανείς με τη δράση τους για μεγάλο χρονικό διάστημα
- Οι hackers δημιούργησαν δικό τους superuser στο σύστημα χωρίς να γίνουν αντιληπτοί

Επίθεση Λογισμικού

Attack Vector

- Η επίθεση ξεκίνησε με τη μόλυνση του υπολογιστή ενός υπαλλήλου της Fazio Mechanical Services (με phishing), που προμήθευε την Target με εξοπλισμό κλιματισμού
- Από εκεί οι hackers κλιμάκωναν συνεχώς την πρόσβασή τους μέχρι τον τελικό στόχο

Payload

- (ανάμεσα σε άλλα σημεία) και στις μηχανές POS όπου οι αριθμοί πιστωτικών καρτών υποκλέπτονταν πριν κρυπτογραφηθούν για μετάδοση προς τα πιστωτικά ιδρύματα

Αποτέλεσμα

Πελάτες

- Προσωπικά στοιχεία 100 εκ. πελατών
- 40 εκ. πιστωτικές κάρτες (πωλήθηκαν σε καλές τιμές online γιατί περιείχαν και ταχυδρομικούς κώδικες χρήσης)

Εταιρία

- Μέσα σε λίγους μήνες είχαν παραιτηθεί οι CEO και CIO
- Πτώση εσόδων 46%
- Δισεκατομμύρια πτώση στη χρηματιστηριακή αξία της εταιρίας

Αβέβαιο μέλλον

- Η δυσκολία αποτροπής παρόμοιων επιθέσεων αποδεικνύεται από την ανακάλυψη παρόμοιας επίθεσης λογισμικού στη Home Depot

CASE STUDY: STUXNET / ΚΥΒΕΡΝΟΠΟΛΕΜΟΣ (2009-10)

Στόχος Επίθεσης

Εμπλουτισμός Ουρανίου

- Κυρίως στο εργοστάσιο Natanz με 7,000 φυγοκεντριτές
- Το Ιραν ισχυρίζεται πως γίνεται χαμηλός εμπλουτισμό για παραγωγή ενέργειας σε πυρηνικό εργοστάσιο
- Δυτικές χώρες ανησυχούν πως πρόκειται για υψηλό εμπλουτισμό για κατασκευή πυρηνικών όπλων

Τεχνολογία και μέτρα ασφάλειας

- Τεχνολογία SCADA (Siemens) για έλεγχο του μηχανικού εξοπλισμού
- Συνεχής παρακολούθηση των συστημάτων από ειδικούς
- Απομόνωση των εργοστασίων από το Internet
- Αυστηρά μέτρα ελέγχου πρόσβασης στρατιωτικού τύπου

Μέθοδος

Attack Vector

- Χρήση πολλαπλών 0-days και πλαστών πιστοποιητικών
- Αρχική μόλυνση σε συσχετι-ζόμενα εργοστάσια & εταιρίες
- Μόλυνση laptop (Windows) εργαζόμενου-συντηρητή των μονάδων ελέγχου
- Περαιτέρω μολύνσεις με USB και τοπικά (μόνο) δίκτυα

Payload

- Ενεργοποίηση μόνο όταν ο ιός ταυτοποιούσε το περιβάλλον ως το εργοστάσιο Natanz
- Αυτόνομη λειτουργία και λεπτομερή γνώση του περιβάλλοντος
- Συστηματική καταστροφή φυγοκεντριτών με αλλαγές στην περιστροφή τους και αυξομειώσεις της πίεσης

Αποτέλεσμα

Πυρηνικό πρόγραμμα του Ιραν

- Ο ιός κατέστρεφε συστηματικά τους φυγοκεντριτές για μεγάλο χρονικό διάστημα στέλνοντας ψευδή στοιχεία στο monitoring room και αποφεύγοντας να αποκαλύψει την παρουσία του
- Μέχρι το Νοέμβρη του 2010, λιγότεροι από 4,000 φυγοκεντριτές παρέμειναν σε χρήση
- Το οικονομικό κόστος είναι άγνωστο, αλλά ειδικοί πιστεύουν πως προκάλεσε 2ετή καθυστέρηση

Ευρύτερες συνέπειες

- Επιπτώσεις για ασφάλεια εργοστασίων πυρηνικής ενέργειας, αεροδρομίων, χημικών εγκαταστάσεων, κλπ

Περιεχόμενα

ΣΤΡΑΤΗΓΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΙΝΔΥΝΟΥ

Ακολουθούν λεπτομέρειες

Περιγραφή

Αποδοχή

- Ο οργανισμός αποδέχεται πως δεν μπορεί να κάνει πολλά για την προστασία του, ή αυτά που μπορεί να κάνει είναι ασύμφορα από οικονομική άποψη

Μεταβίβαση

- Ο οργανισμός προσπαθεί να μεταβιβάσει τον κίνδυνο σε άλλες εταιρίες, όπως ασφαλιστικές εταιρίες, εταιρίες διαχείρισης πληρωμών, κλπ

Περιορισμός

- Εκπόνηση σχεδίου για αντιμετώπιση κρίσεων που σχετίζονται με την ασφάλεια
  - Υλοποίηση ελέγχων για την αποτροπή αναγνωρισμένων απειλών
  - Ανάπτυξη ενός μέσου ανάκτησης σε περίπτωση που η απειλή γίνει πραγματικότητα
  - Πολιτικές

ΕΛΕΓΧΟΙ

Περιγραφή

Φυσικοί Έλεγχοι

- Εμποδίζουν μη εξουσιοδοτημένα άτομα να προσπελαύνουν τις εγκαταστάσεις της εταιρείας (προστατευμένοι χώροι, φύλακες, συστήματα παρακολούθησης και συναγερμού)

Έλεγχοι Πρόσβασης

- Περιορίζουν τη χρήση πόρων σε εξουσιοδοτημένα άτομα
  - *Αυθεντικοποίηση:* χρήση κωδικών, ταυτοτήτων βιομετρικών στοιχείων, κλπ
  - *Εξουσιοδότηση:* ο κάθε (ταυτοποιημένος) υπάλληλος ή εξωτερικός συνεργάτης της εταιρίας έχει πρόσβαση μόνο στις πληροφορίες εκείνες που χρειάζονται για τη δουλειά του

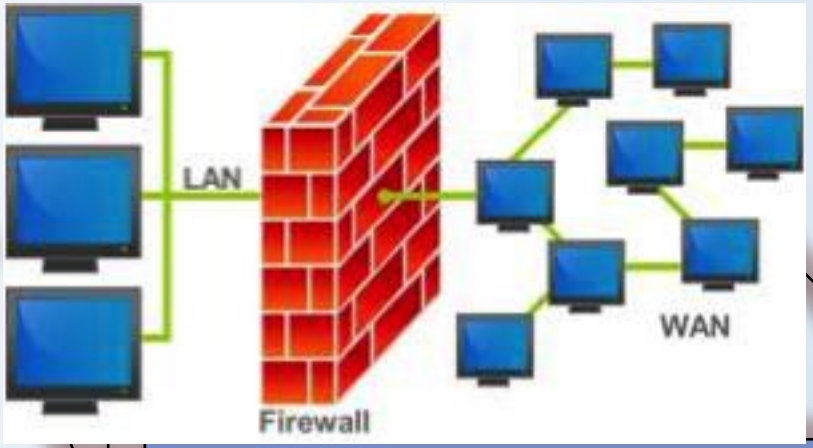
Έλεγχοι Επικοινωνιών

- Διασφαλίζουν τη μετακίνηση των δεδομένων μέσω δικτύων,
  - Τείχη προστασίας (firewalls)
  - VPN
  - Λογισμικό antivirus
  - Κρυπτογραφία
  - Ψηφιακά πιστοποιητικά
  - Λευκές/Μαύρες λίστες πρόσβασης
  - SSL
  - Καταγραφή προσπαθειών πρόσβασης

FIREWALLS

Ορισμός/ Υλοποίηση

- Συσκευή ή λογισμικό η οποία περιορίζει τις συνδέσεις σε ένα δίκτυο για λόγους ασφάλειας
- Οι συνδέσεις περιορίζονται με βάση προκαθορισμένων κανόνων
- Σε εταιρικά περιβάλλοντα, χρησιμοποιούνται γρήγοροι firewall servers, από τους οποίους εξαρτάται η ασφάλεια όλων των δεδομένων της εταιρίας
- Προσωπικά firewalls είναι διαθέσιμα στα modems/routers των απλών χρηστών, καθώς και ως λογισμικό λειτουργικού συστήματος (π.χ., windows firewall)



Επιτρέπονται μόνο συνδέσεις ορισμένων προγραμμάτων ή υπολογιστών με το διαδίκτυο

Επιτρέπονται μόνο συνδέσεις με πρωτοβουλία εσωτερικών υπολογιστών.

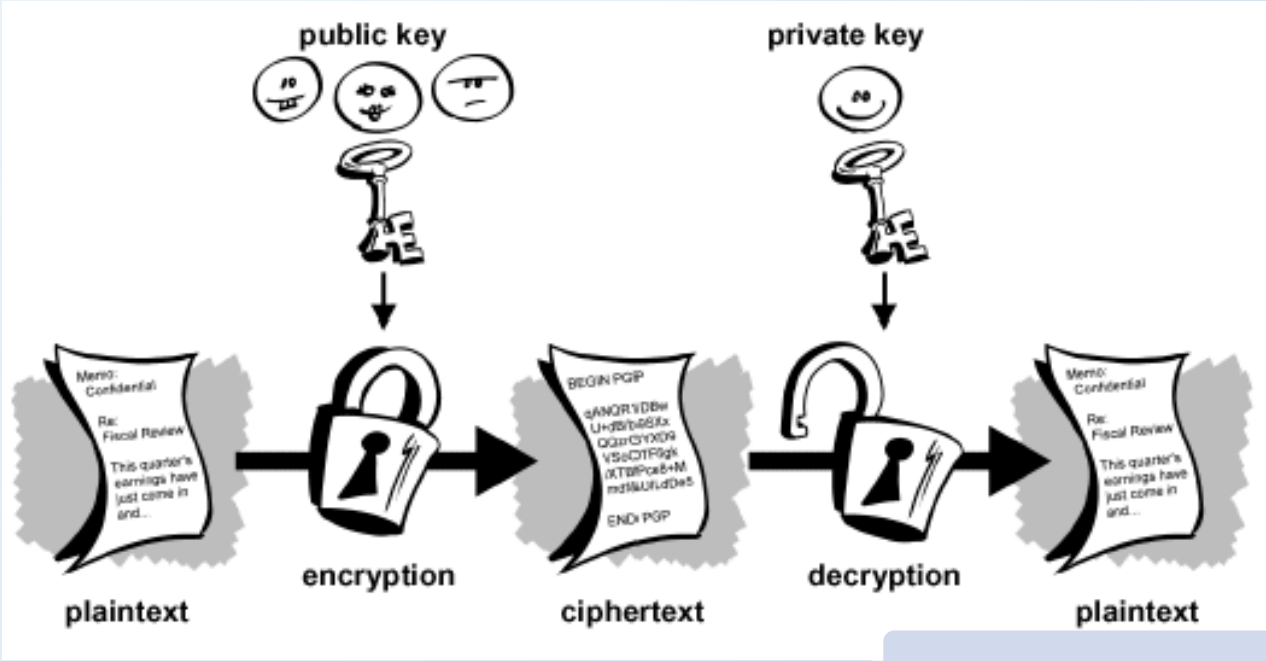
Π.χ., όταν ένας υπολογιστής στο LAN ζητήσει εξωτερική σύνδεση, (π.χ., web browsing), καταγράφεται η διεύθυνση του εξωτερικού υπολογιστή, ώστε να του επιτραπεί να απαντήσει

Συνδέσεις που γίνονται με πρωτοβουλία εξωτερικών υπολογιστών απορρίπτονται

PUBLIC KEY CRYPTOGRAPHY (ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ)

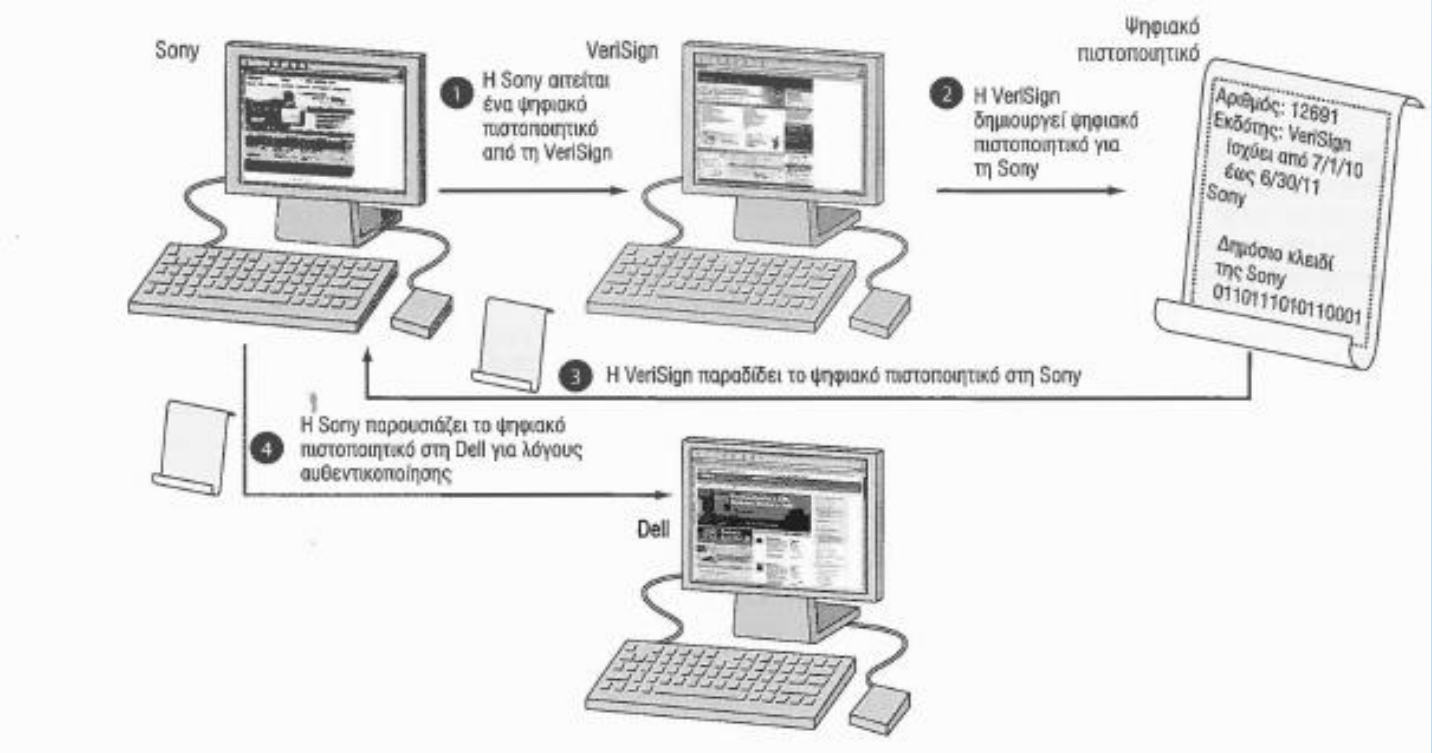
- **Μέθοδος**
  - Όποιος θέλει να λάβει ασφαλώς μηνύματα δημιουργεί 2 *κλειδιά (keys)*
  - Το *δημόσιο κλειδί (public key)* το μοιράζει ελεύθερα. Το χρησιμοποιούν όσοι θέλουν να του στείλουν μηνύματα
  - Το *ιδιωτικό κλειδί (private key)* το γνωρίζει μόνο εκείνος και μόνο με αυτό μπορεί να διαβαστούν τα μηνύματα
  - Η μέθοδος ονομάζεται και *ασύμμετρη* κρυπτογράφηση

- **Πλεονεκτήματα**
  - Το ιδιωτικό κλειδί μένει πάντα καλά προστατευμένο. Σε συμμετρικά συστήματα (όπου το ίδιο κλειδί χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση) η μετάδοσή του μπορεί να υποκλαπεί
- **Χρήσεις**
  - ασφαλές email (π.χ. με PGP)
  - ψηφιακές υπογραφές (απόδειξη ταυτότητας)
  - λίγο-πολύ ολόκληρη η ασφάλεια του internet βασίζεται έμμεσα ή άμεσα στην κρυπτογράφηση δημοσίου κλειδιού



ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

- **Σκοπός**
  - Να βεβαιώσουν πως το δημόσιο κλειδί μιας εταιρίας έχει πραγματικά εκδοθεί από την ίδια (π.χ., ώστε να δεχθούμε να κάνουμε το update που φαίνεται πως μας το στέλνει η Microsoft)
  - Αλλιώς κάποιος μπορεί να μας ξεγελάσει και να μας πείσει να κρυπτογραφούμε τα μηνύματά μας με τρόπο που μπορεί να τα διαβάσει
- **Μέθοδος**
  - Ένα Certification Authority που το εμπιστεύονται όλοι (π.χ. VeriSign) εκδίδει κλειδιά επί πληρωμή και βεβαιώνει για την κυριότητα των public keys
  - Με αυτόν τον τρόπο μπορούμε π.χ., να εμπιστευτούμε πως το πρόγραμμα που ετοιμαζόμαστε να εγκαταστήσουμε έχει όντως «υπογραφεί» από την Adobe



ΠΟΛΙΤΙΚΕΣ: ΧΡΗΣΤΕΣ ΚΑΙ ΥΠΟΣΤΗΡΙΞΗ ΑΠΟ ΤΟΝ ΟΡΓΑΝΙΣΜΟ

Υποχρεώσεις Χρηστών

- Να χρησιμοποιούν σωστά τους κωδικούς πρόσβασης
  - να κρατούν τους κωδικούς πρόσβασης τους ιδιωτικούς
  - να αποφεύγουν τους εύκολους κωδικούς πρόσβασης
  - να χρησιμοποιούν διαφορετικούς κωδικούς πρόσβασης σε διαφορετικά συστήματα
- Να ξέρουν πώς να χρησιμοποιήσουν το σύστημα με λογική και ασφάλεια (π.χ., να αποσυνδέονται από τον σταθμό εργασίας, ακόμα και σε ολιγόλεπτες απουσίες)
- Να κρυπτογραφούν τα ευαίσθητα αρχεία
- Να γνωρίζουν πως ένας υπάλληλος μπορεί να θέσει σε κίνδυνο όλη την εταιρία

Υποστήριξη από τον Οργανισμό

- Μεγαλύτερη ενημέρωση σχετικά με θέματα ασφάλειας
  - οργανωμένα εκπαιδευτικά προγράμματα και συχνά updates
  - online tests των γνώσεων των υπαλλήλων
  - έμφαση στο «κοινό καλό»
- Χρήση εξειδικευμένων εργαλείων για ελέγχους
- Τακτικοί έλεγχοι πως οι πολιτικές εφαρμόζονται, και αξιολόγηση (Auditing and Review)
- Ύπαρξη σχεδίων έκτακτης ανάγκης (Incident Response & Disaster Contingency Plan), και Ανάκτησης & Συνέχισης Λειτουργίας (Recovery)

ΣΧΕΔΙΟ ΑΝΑΚΤΗΣΗΣ ΚΑΙ ΣΥΝΕΧΙΣΗΣ ΛΕΙΤΟΥΡΓΙΑΣ

Σκοπός

- Να προνοήσει για όλα όσα χρειάζονται για τη συνέχιση της λειτουργίας της επιχείρησης μετά από μία καταστροφή
- Να παρέχει καθοδήγηση και τα κατάλληλα εργαλεία στους ανθρώπους που θα αναλάβουν να συνεχίσουν τη λειτουργία

Στρατηγικές

- Αυστηρή πολιτική back-up
  - Χρήση πολιτικής storage με ιεράρχηση δεδομένων (για έλεγχο κόστους)
  - Back-up εκτός εταιρίας (π.χ., cloud storage)
- **Hot/Cold Sites για συνέχιση λειτουργίας μετά από μεγάλη καταστροφή**: τοποθεσίες εκτός οργανισμού που περιλαμβάνουν τις εγκαταστάσεις, συστήματα, δίκτυα, και άλλους πληροφοριακούς πόρους που χρειάζονται για να λειτουργήσουν μετά από μια καταστροφή στην κυρίως τοποθεσία, είτε αμέσως (hot site, μεγάλο κόστος) είτε μετά από εύλογο χρονικό διάστημα (cold site, μικρότερο κόστος)