Erasmus Plus Programme – KA2 Strategic Partnerships for higher education

IO1: Industrial Cyber Security Training Course for Technicians in Industry 4.0

Greek Version

Project № 2018-1-ES01-KA203-050493

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

Co-funded by the
Erasmus+ Programme
of the European Union

ΕΝΟΤΗΤΑ 1

Βιομηχανικά συστήματα - Στοιχεία και χαρακτηριστικά

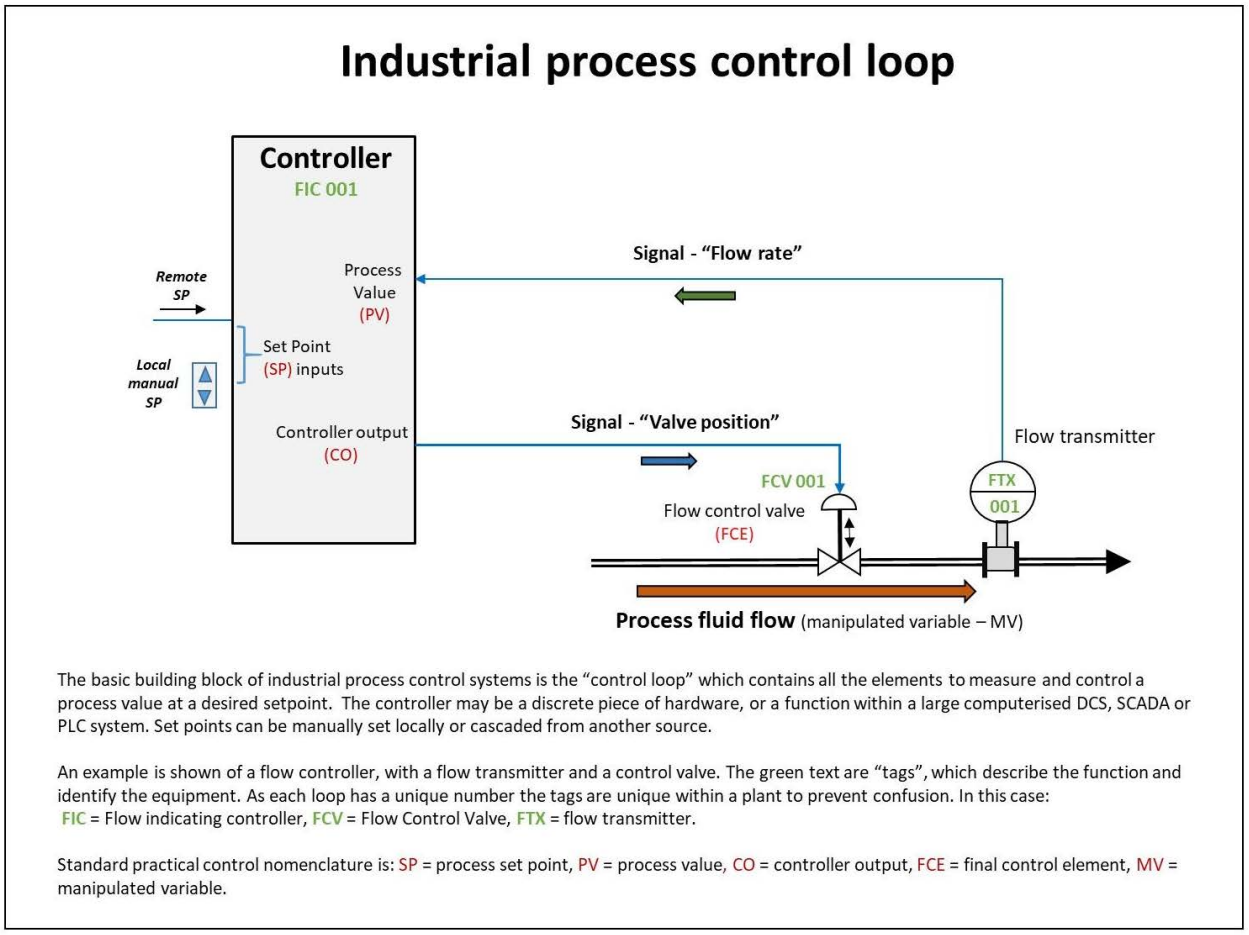
1.1 Στοιχεία ενός Συστήματος Βιομηχανικού Ελέγχου

Description

1.1 Στοιχεία ενός Συστήματος Βιομηχανικού Ελέγχου

Table of contents

Σύστημα Βιομηχανικού Ελέγχου (Industrial Control System) (**ICS**) είναι ένας γενικός όρος που περιλαμβάνει πολλούς τύπους συστημάτων ελέγχου, δικτύων και σχετικών οργάνων, που χρησιμοποιούνται στον έλεγχο της βιομηχανικής διαδικασίας. Όπως φαίνεται στην Εικόνα 1.1, ο έλεγχος της διαδικασίας πραγματοποιείται μέσω της χρήσης βρόχων, στους οποίους η τιμή μιας μετρημένης μεταβλητής (process variable) (PV) τροποποιείται αυτόματα ώστε να ισούται με την επιθυμητή τιμή (set point) (SP). Συμπεριλαμβάνει τον αισθητήρα διαδικασίας, τον ελεγκτή και το τελικό στοιχείο ελέγχου (Final Control Element) (FCE), που απαιτούνται για τον αυτόματο έλεγχο.



Εικόνα 1.1- Βρόχος ελέγχου βιομηχανικής διαδικασίας (Πηγή: Wikipedia)

Τέτοια συστήματα μπορεί να είναι από modular ελεγκτές σε πάνελ μέχρι και μεγάλα, διασυνδεδεμένα και διαδραστικά κατανεμημένα συστήματα ελέγχου, με πολλές χιλιάδες συνδέσεις. Όλα τα συστήματα λαμβάνουν δεδομένα από απομακρυσμένους αισθητήρες, που μετρούν τις μεταβλητές, τις συγκρίνουν με τις καθορισμένες τιμές κι επιλέγουν τις εντολές που χρησιμοποιούνται για τον έλεγχο μιας διαδικασίας μέσω των FCE, όπως είναι οι βαλβίδες ελέγχου.

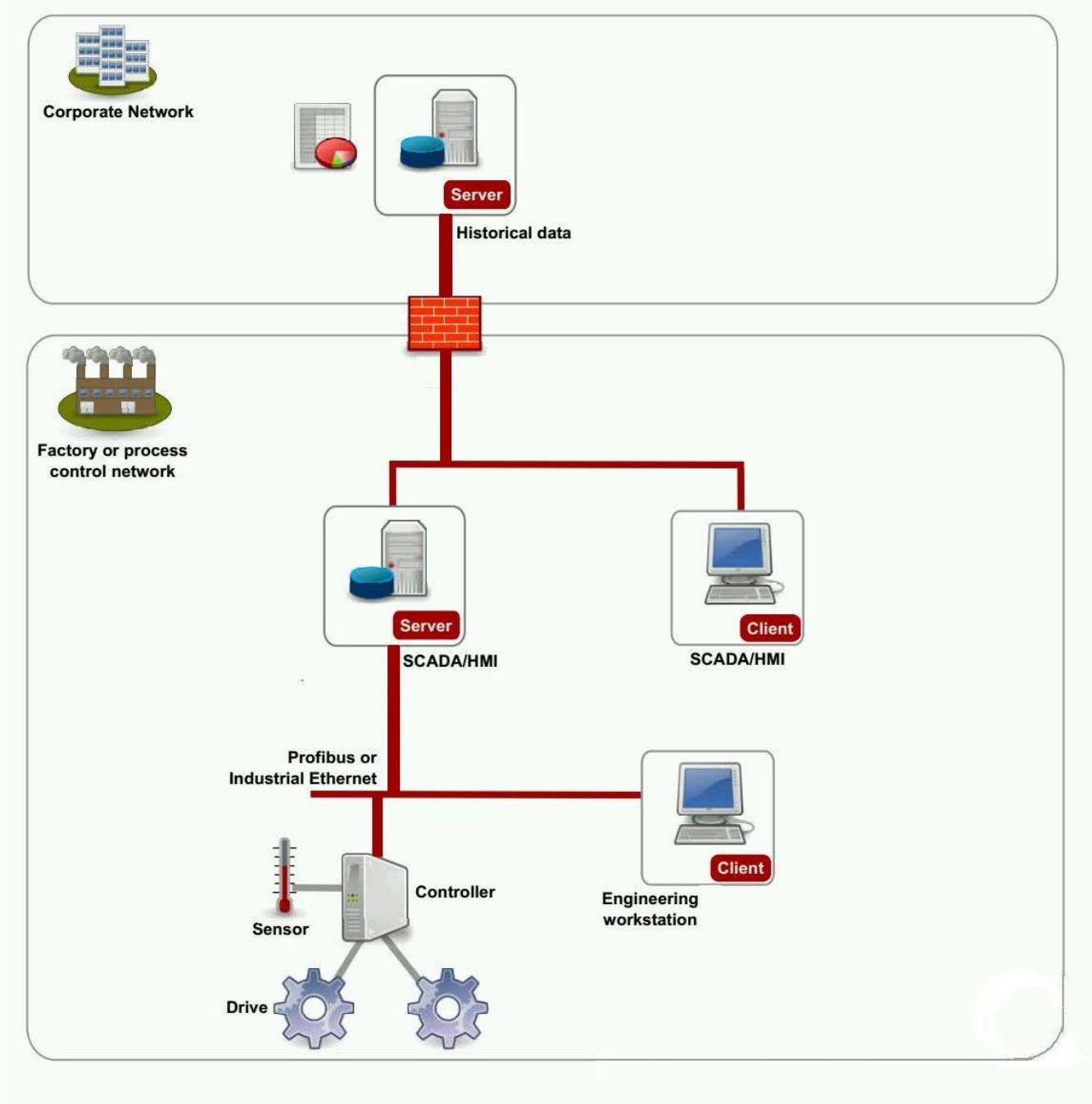
Υπάρχουν πολλοί τύποι ICS και οι πιο κοινοί είναι τα συστήματα **Απόκτησης Δεδομένων κι Εποπτικού Ελέγχου (Supervisory Control and Data Acquisition) (SCADA)** και τα **Συστήματα Κατανεμημένου Ελέγχου (Distributed Control Systems) (DCS)**. Στην πράξη, τα μεγάλα συστήματα SCADA έχουν γίνει παρόμοια σε λειτουργία με τα συστήματα κατανεμημένου ελέγχου, αλλά χρησιμοποιούν πολλαπλά μέσα διασύνδεσης με τα μηχανήματα.

Όπως φαίνεται στην Εικόνα 1.2, τα ICS ενσωματώνονται στις βιομηχανίες όπως δείχνει το ακόλουθο διάγραμμα. Η διοίκηση χρησιμοποιεί δεδομένα από το εργοστάσιο και παίρνει αποφάσεις βασιζόμενη σ' αυτά, ενώ μετά μεταφέρει τα σχέδια σε επίπεδο παραγωγής, για να εκτελεστούν μέσω πόρων που ελέγχονται από τα ICS.

Εικόνα 1.2 - Ενσωμάτωση ICS σε εταιρεία (Πηγή: Open Security Archive)

Μια ειδική περίπτωση ICS είναι το **σύστημα ασφαλείας με όργανα (Safety Instrumented System) (SIS)**, που αποτελείται τόσο από υλικό όσο κι από λογισμικό, και χρησιμοποιείται ειδικά σε **κρίσιμα συστήματα,** όπως εκείνα

σε **διυλιστήρια** και σε **χημικές και πυρηνικές εγκαταστάσεις** για να προσφέρει προστασία, όπως ν' ανοιγοκλείσει μια κρίσιμη



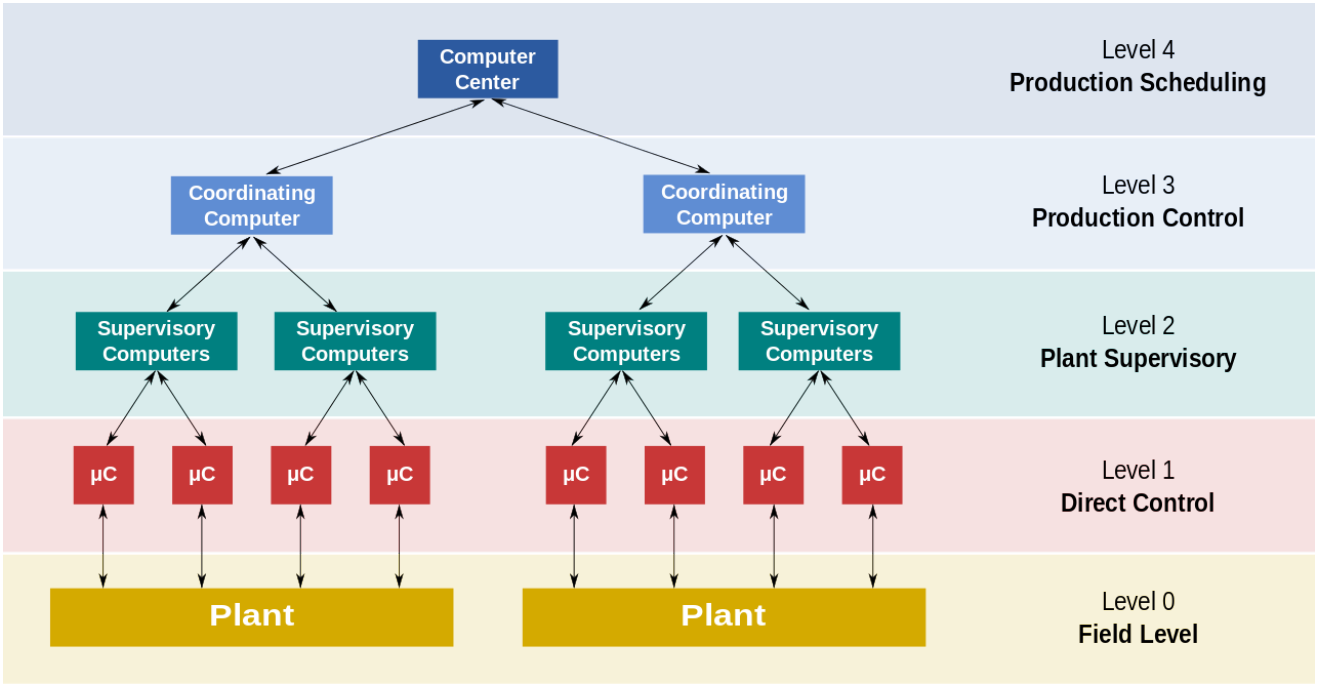
βαλβίδα για να μειωθεί η πίεση επικίνδυνων αερίων ή η υψηλή θερμοκρασία υγρών.

Τα SIS απαρτίζονται από τους ίδιους τύπους στοιχείων ελέγχου (συμπεριλαμβάνοντας αισθητήρες, logic solvers, ενεργοποιητές και άλλον ελεγκτικό εξοπλισμό) όπως ένα Σύστημα Ελέγχου Βασικών Διεργασιών (Basic Process Control System) (BPCS).

Ωστόσο, όλα τα στοιχεία ελέγχου ενός SIS είναι αφιερωμένα αποκλειστικά στη σωστή λειτουργία του SIS. Συστήματα **υποστήριξης**, όπως παροχή ενέργειας, κλιματισμός των οργάνων κι επικοινωνίες, απαιτούνται για τη λειτουργία του SIS. Τα συστήματα υποστήριξης πρέπει να σχεδιαστούν για να παράσχουν την απαιτούμενη **ακεραιότητα και αξιοπιστία.**

Τα ICS διαχωρίζονται τυπικά σε **5 επίπεδα**, όπως φαίνονται στην Εικόνα 1.3. Κάθε επίπεδο έχει τη δική του λειτουργικότητα και πρέπει να επικοινωνεί με τα άλλα επίπεδα για να εκτελέσει τις προγραμματισμένες ενέργειες.

Η συλλογή δεδομένων ξεκινά στο **RTU ή PLC** του 1ου επιπέδου και συμπεριλαμβάνει τις ενδείξεις των οργάνων και τις αναφορές κατάστασης του εξοπλισμού, που μεταδίδονται στο SCADA του 2ου επιπέδου. Τα δεδομένα συγκεντρώνονται και μορφοποιούνται με τέτοιο τρόπο, ώστε να μπορεί ο χειριστής στην αίθουσα ελέγχου, που χρησιμοποιεί την **HMI** (Human Machine Interface) (Διεπαφή Ανθρώπου Μηχανής), να πάρει εποπτικές αποφάσεις για την τροποποίηση ή την παράκαμψη του κανονικού χειρισμού του RTU ή PLC. Τα δεδομένα μπορούν να αποσταλούν και στο ιστορικό, που είναι ενσωματωμένο στο σύστημα διαχείρισης της βάσης δεδομένων, για την πραγματοποίηση κάθε είδους αναλυτικού ελέγχου.

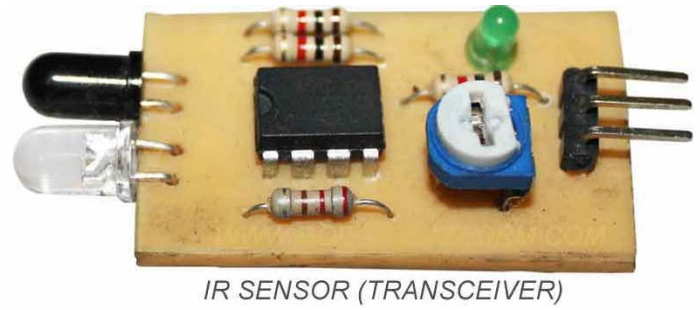


Εικόνα 1.3 - Επίπεδα των ICS (Πηγή: Wikipedia)

Αυτό το επίπεδο περιλαμβάνει τις συσκευές πεδίου, όπως τους **αισθητήρες** και τα τελικά στοιχεία ελέγχου ή **ενεργοποιητές**.

Με την ευρύτερη έννοια, ένας αισθητήρας είναι μια συσκευή, τμήμα ή υποσύστημα, που έχει σκοπό τον εντοπισμό συμβάντων ή αλλαγών στο περιβάλλον του και την αποστολή των πληροφοριών σε άλλες ηλεκτρονικές συσκευές, όπως στον επεξεργαστή ενός υπολογιστή. Ένας αισθητήρας χρησιμοποιείται πάντοτε με άλλες ηλεκτρονικές συσκευές.

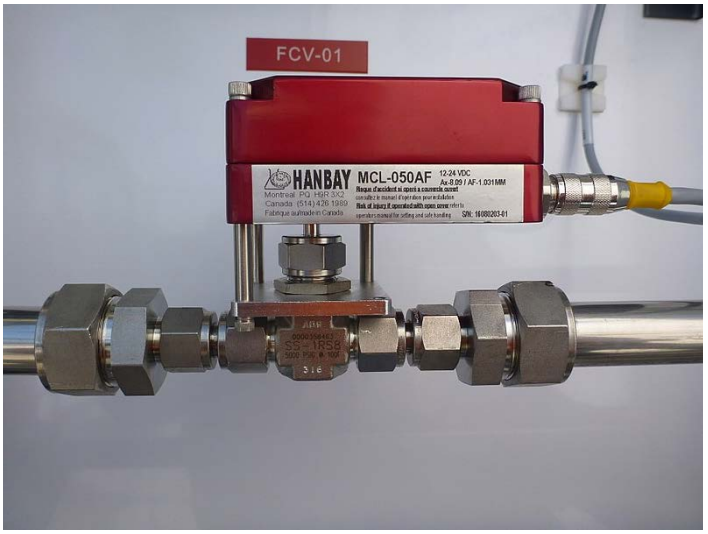
Οι αισθητήρες (η Εικόνα 1.4 δείχνει έναν αισθητήρα υπερύθρων IR) χρησιμοποιούνται σε καθημερινά αντικείμενα, όπως σε πλήκτρα ευαίσθητα στην αφή (αισθητήρας αφής) και σε βιομηχανικές διαδικασίες για τη μέτρηση διαφορετικών μεγεθών (πίεση, θέση, θερμοκρασία...).



Εικόνα 1.4- αισθητήρας IR (Πηγή: Wikipedia)

Ο ενεργοποιητής (η εικόνα 1.5 δείχνει μια υδραυλική βαλβίδα) είναι το εξάρτημα μιας μηχανής που είναι υπεύθυνο για την κίνηση και τον έλεγχο ενός μηχανισμού ή συστήματος, για παράδειγμα το άνοιγμα μιας βαλβίδας. Με απλούς όρους, «μετακινεί».

Ο ενεργοποιητής χρειάζεται σήμα ελέγχου και πηγή ενέργειας. Το σήμα ελέγχου είναι χαμηλής ενέργειας και μπορεί να έχει τη μορφή ηλεκτρικού ρεύματος, πνευματικής ή υδραυλικής πίεσης, ή ακόμα και ανθρώπινης δύναμης. Όταν λάβει σήμα ελέγχου, ο ενεργοποιητής απαντά μετατρέποντας την ενέργεια του σήματος σε μηχανική κίνηση.

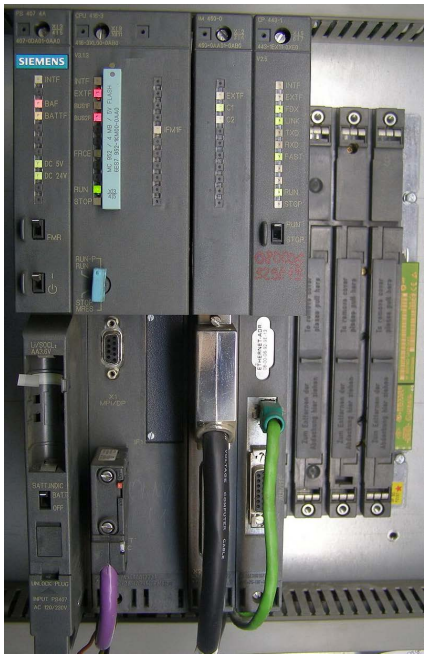


Εικόνα 1.5- Υδραυλική βαλβίδα (Πηγή: Wikipedia)

Αυτό το επίπεδο περιλαμβάνει τις βιομηχανοποιημένες μονάδες εισαγωγής/εξαγωγής (input/output) (I/O) και τους σχετικούς κατανεμημένους ηλεκτρονικούς επεξεργαστές. Περιλαμβάνει τους προγραμματιζόμενους λογικούς ελεγκτές (programmable logic controllers) (PLCs) ή τις απομακρυσμένες τερματικές μονάδες (remote terminal units) (RTUs).

Ένας **προγραμματιζόμενος λογικός ελεγκτής** (**PLC**) είναι ένας ψηφιακός βιομηχανικός υπολογιστής, που έχει γίνει πιο ανθεκτικός κι έχει τροποποιηθεί για τον έλεγχο των παραγωγικών διαδικασιών, όπως τις γραμμές παραγωγής, τις ρομποτικές συσκευές, ή κάθε άλλη δραστηριότητα που απαιτεί έλεγχο υψηλής αξιοπιστίας, ευκολία στον προγραμματισμό και διάγνωση σφαλμάτων στις διεργασίες.

Ένα PLC (Εικόνα 1.6) αποτελεί παράδειγμα ενός συστήματος πραγματικού χρόνου, αφού τα αποτελέσματα εξαγωγής πρέπει να παραχθούν σύμφωνα με τις προδιαγραφές εισαγωγής και μέσα σε ορισμένο χρόνο, αλλιώς θα προκύψει αθέλητη λειτουργία.



Εικόνα 1.6- Προγραμματιζόμενος Λογικός Ελεγκτής (Πηγή: Wikipedia)

Η εικόνα 1.7 δείχνει μια **απομακρυσμένη τερματική μονάδα (RTU),** που είναι μια συσκευή που ελέγχεται από μικροεπεξεργαστή. Συνδέει αντικείμενα του φυσικού κόσμου με ένα σύστημα DCS ή SCADA, μέσω της μετάδοσης τηλεμετρίας στο κεντρικό σύστημα και μέσω της χρήσης μηνυμάτων από το κεντρικό σύστημα επιτήρησης για τον έλεγχο συνδεδεμένων αντικειμένων. Άλλοι όροι που μπορούν να χρησιμοποιηθούν για τα RTU είναι απομακρυσμένες μονάδες τηλεμετρίας και απομακρυσμένες μονάδες τηλεχειρισμού.

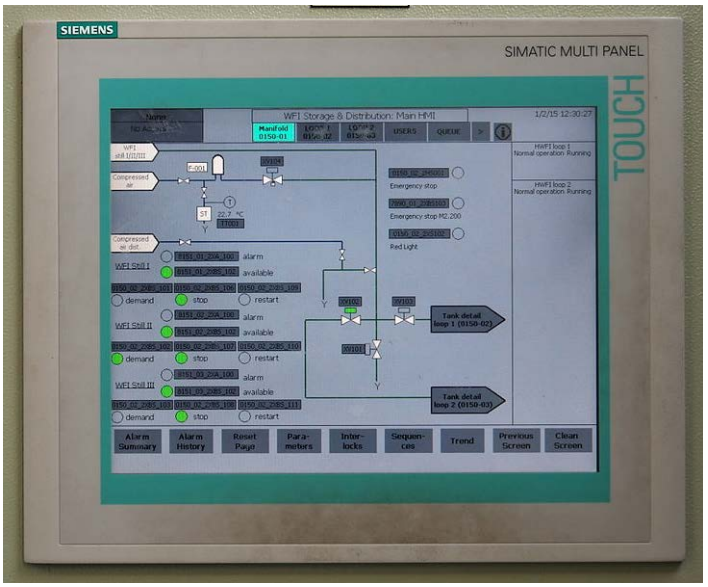
Εικόνα 1.7- Απομακρυσμένη Τερματική Μονάδα (Πηγή: Wikipedia)

Σε αυτό το επίπεδο είναι οι **υπολογιστές επιτήρησης**, που συγκρίνουν πληροφορίες από τους κόμβους επεξεργασίας του συστήματος και παρέχουν οθόνες ελέγχου στον χειριστή.

Το 2^{ο} επίπεδο περιέχει το λογισμικό του **SCADA** και την υπολογιστική πλατφόρμα. Το λογισμικό του SCADA υπάρχει μόνο σε αυτό το επίπεδο επιτήρησης, αφού οι ενέργειες ελέγχου πραγματοποιούνται αυτόματα από τα RTU ή τα PLC του 1^{ου} επιπέδου. Οι ελεγκτικές λειτουργίες του SCADA συνήθως περιορίζονται σε βασική παράκαμψη ή σε παρέμβαση επιπέδου επόπτη. Για παράδειγμα, ένα PLC μπορεί να ελέγξει τη ροή του νερού του συστήματος ψύξης μιας βιομηχανικής διαδικασίας βάσει μιας προκαθορισμένης τιμής, αλλά το λογισμικό του συστήματος SCADA θα επιτρέψει στους χειριστές ν' αλλάξουν τις προκαθορισμένες τιμές της ροής.

Το SCADA επιτρέπει και την ύπαρξη συνθηκών **συναγερμού**, όπως τη μείωση της ροής ή την υψηλή θερμοκρασία, που προβάλλονται και καταγράφονται. Ένας **βρόχος ανάδρασης** ελέγχεται απευθείας από το RTU ή το PLC, αλλά το λογισμικό του SCADA παρακολουθεί τη συνολική απόδοση του βρόχου.

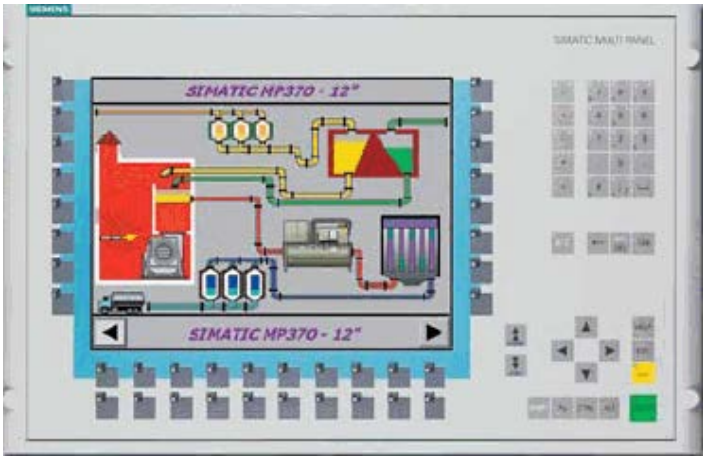
Η **διεπαφή ανθρώπου μηχανής (HMI)** (η εικόνα 1.8 δείχνει ένα τυπικό HMI πάνελ αφής) είναι το παράθυρο του χειριστή για το σύστημα εποπτείας. Παρουσιάζει πληροφορίες της εργοστασιακής μονάδας στους χειριστές υπό τη μορφή διαγραμμάτων, δηλαδή μιας σχηματικής αναπαράστασης του ελέγχου της μονάδας, καθώς και σελίδες καταχώρησης ανησυχητικών συμβάντων. Το HMI συνδέεται στον εποπτικό υπολογιστή SCADA για να παράσχει ζωντανά δεδομένα για τα διαγράμματα, τις οθόνες συναγερμού και τις γραφικές παραστάσεις. Σε πολλές εγκαταστάσεις το HMI είναι το γραφικό σύστημα χειρισμού για τον χειριστή, και συγκεντρώνει όλα τα δεδομένα από εξωτερικές συσκευές, δημιουργεί αναφορές, στέλνει ειδοποιήσεις κλπ.



Εικόνα 1.8- HMI πάνελ αφής (Πηγή: Wikimedia)

Η καρδιά του συστήματος SCADA είναι το **Supervisory Workstation (ο εποπτικός σταθμός εργασίας)**, που συγκεντρώνει τα δεδομένα των διεργασιών και στέλνει εντολές στις συνδεδεμένες συσκευές. Είναι ο υπολογιστής και το λογισμικό που είναι υπεύθυνος για την επικοινωνία με τους ελεγκτές στο πεδίο, δηλαδή τα RTUs και τα PLCs, και περιλαμβάνει το λογισμικό HMI που τρέχει στους σταθμούς εργασίας των χειριστών.

Σε μικρότερα συστήματα SCADA, ο εποπτικός υπολογιστής μπορεί να αποτελείται από ένα μόνο PC, οπότε το HMI είναι τμήμα αυτού του υπολογιστή. Σε μεγαλύτερα συστήματα SCADA, ο κεντρικός σταθμός εργασίας μπορεί να περιλαμβάνει πολλαπλά HMIs σε διάφορους υφιστάμενους υπολογιστές, πολλαπλούς σέρβερ για την απόκτηση δεδομένων, κατανεμημένα προγράμματα και σημεία ανάκτησης για την περίπτωση καταστροφής. Για την αύξηση της ακεραιότητας του συστήματος, οι πολλαπλοί σέρβερ συνήθως ρυθμίζονται σε διπλό εφεδρικό σχηματισμό ή σε σχηματισμό αναμονής, προσφέροντας συνεχή έλεγχο και παρακολούθηση στην περίπτωση βλάβης κάποιου σέρβερ.

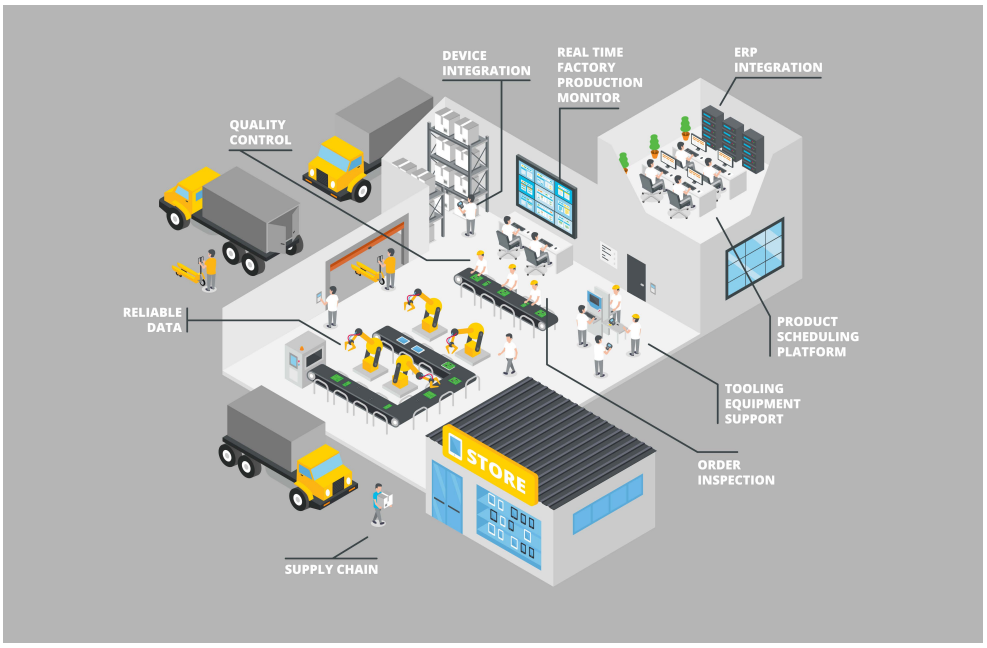


Εικόνα 1.9- Οθόνη SCADA (Πηγή: Wikimedia)

Τα επίπεδα 3 και 4 δεν αφορούν αποκλειστικά στον έλεγχο διεργασιών με την παραδοσιακή έννοια. Σε αυτά ελέγχεται η παραγωγή και γίνεται ο προγραμματισμός της.

Αυτό το επίπεδο δεν ελέγχει ευθέως τη διαδικασία, αλλά αφορά στην **παρακολούθηση της παραγωγής και των στόχων**. Περιλαμβάνει συστήματα MES, CMMS και WMS.

Τα συστήματα διαχείρισης παραγωγής (Manufacturing execution systems) (MES) είναι υπολογιστικά συστήματα που χρησιμοποιούνται στην παραγωγή για την παρακολούθηση και καταγραφή της μεταμόρφωσης των πρώτων υλών σε τελικά προϊόντα. Τα MES προσφέρουν πληροφορίες που βοηθούν τους λήπτες αποφάσεων να καταλάβουν πώς μπορούν να βελτιστοποιηθούν οι υπάρχουσες συνθήκες στην παραγωγική μονάδα για να αυξηθεί ο όγκος παραγωγής. Τα MES λειτουργούν σε ζωντανό χρόνο για να επιτρέψουν τον έλεγχο πολλαπλών στοιχείων της παραγωγικής διαδικασίας. Η εικόνα 1.10 δείχνει τα διάφορα τμήματα ενός συστήματος MES.



Εικόνα 1.10- Οργάνωση εταιρείας για διαχείριση μέσω MES (Πηγή: Wikimedia)

Το σύστημα διαχείρισης αποθήκης (Warehouse management system) (WMS) είναι λογισμικό που σχεδιάστηκε για την υποστήριξη και βελτιστοποίηση της λειτουργικότητας της αποθήκης και τη διαχείριση του κέντρου διανομής. Αυτά τα συστήματα διευκολύνουν τη διοίκηση στον καθημερινό σχεδιασμό, στην οργάνωση, στην ανάθεση εργασιών, στη διεύθυνση και στον έλεγχο των διαθέσιμων πόρων, για τη μεταφορά και την αποθήκευση υλικών μέσα κι έξω από μια αποθήκη, υποστηρίζοντας παράλληλα το προσωπικό στη μετακίνηση κι αποθήκευση υλικών.

Το σύστημα διαχείρισης συντήρησης (Computerized maintenance management system) (CMMS), είναι ένα λογισμικό που διατηρεί βάση δεδομένων με πληροφορίες για τις εργασίες συντήρησης ενός οργανισμού. Αυτές οι πληροφορίες θα βοηθήσουν τους συντηρητές να κάνουν πιο αποτελεσματικά τη δουλειά τους (να βρουν, για παράδειγμα, ποιες μηχανές χρειάζονται συντήρηση και ποιες αποθήκες έχουν τα ανταλλακτικά που χρειάζονται) και θα βοηθήσουν τη διοίκηση να πάρει ενημερωμένες αποφάσεις (για παράδειγμα, να συγκρίνει το κόστος μιας επισκευής με το κόστος προληπτικής συντήρησης του κάθε μηχανήματος, για την καλύτερη κατανομή των διαθέσιμων πόρων).

Αυτό το επίπεδο περιλαμβάνει τα συστήματα ERP και η κύρια λειτουργία του είναι να παράσχει πληροφορίες και υποστήριξη στο διοικητικό προσωπικό.

Ο όρος, **συστήματα προγραμματισμού επιχειρησιακών πόρων (Enterprise resource planning) (ERP)** αναφέρεται συνήθως σε μια κατηγορία εταιρικού λογισμικού διαχείρισης – συνήθως μια σουίτα εφαρμογών – μέσω των οποίων ένας οργανισμός θα συλλέξει, θα αποθηκεύσει, θα διαχειριστεί και θα ερμηνεύσει δεδομένα σε ζωντανό χρόνο, μέσα από όλες αυτές τις επιχειρηματικές δραστηριότητες. Προσφέρει ενοποιημένη και συνεχώς ανανεωμένη εικόνα στις κύριες επιχειρηματικές διεργασίες, χρησιμοποιώντας τις κοινές βάσεις δεδομένων του συστήματος διαχείρισης βάσεων.

Τα συστήματα ERP παρακολουθούν τους επιχειρηματικούς πόρους - μετρητά, πρώτες ύλες, παραγωγική ικανότητα – και την κατάσταση των επιχειρηματικών δεσμεύσεων: παραγγελίες, εντολές αγοράς και μισθοδοσία. Οι εφαρμογές που απαρτίζουν το σύστημα μοιράζονται τα δεδομένα με όλα τα τμήματα (παραγωγή, αγορές, πωλήσεις, λογιστήριο, κλπ.) που παρέχουν τα δεδομένα.

Εικόνα 1.11- Τμήματα του ERP σύμφωνα με την εταιρική δομή (Πηγή: Wikipedia)

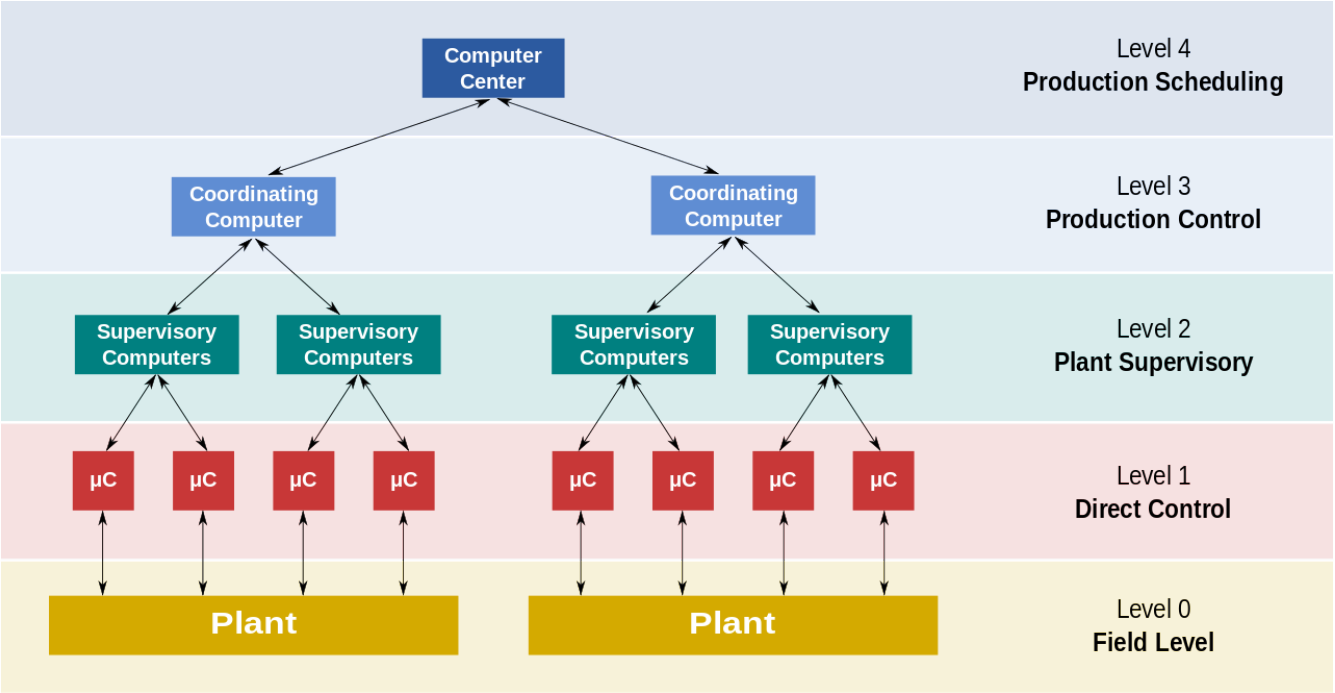
1.2 Σχεδιασμός δικτύου και αρχιτεκτονική

Description

1.2 Σχεδιασμός δικτύου και αρχιτεκτονική

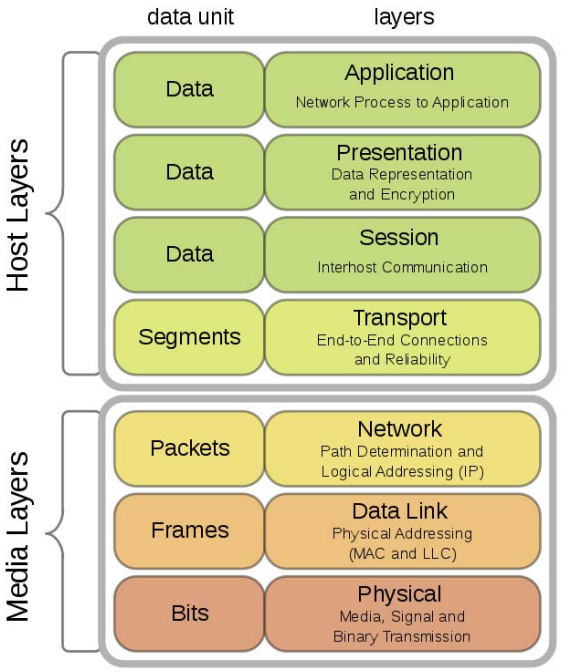
Table of contents

Στο προηγούμενο κεφάλαιο αναφέραμε ότι τα Συστήματα Βιομηχανικού Ελέγχου (Εικόνα 1.12) αποτελούνται από διασυνδεδεμένες συσκευές που μοιράζονται και μεταδίδουν πληροφορίες μεταξύ τους. Σε αυτό το κεφάλαιο θα μελετήσουμε τις πιο κοινές δικτυακές δομές και τα χαρακτηριστικά τους.



Εικόνα 1.12- Επίπεδα ICS (Πηγή: Wikipedia)

Γι' αυτό τον σκοπό, θα ξεκινήσουμε με τη μελέτη **του μοντέλου Διασύνδεσης Ανοιχτών Συστημάτων (Open Systems Interconnection model)** (**OSI model**), ενός εννοιολογικού μοντέλου που χαρακτηρίζει και τυποποιεί τις λειτουργίες επικοινωνίας ενός συστήματος τηλεπικοινωνιών ή ενός υπολογιστικού συστήματος, ασχέτως της εσωτερικής δομής του και της τεχνολογίας του. Στόχος του είναι η διαλειτουργικότητα των ποικίλων επικοινωνιακών συστημάτων με τυποποιημένα πρωτόκολλα. Το μοντέλο διαχωρίζει ένα σύστημα επικοινωνίας σε αφηρημένα επίπεδα. Η αρχική έκδοση του μοντέλου καθόρισε εφτά επίπεδα.



Εικόνα 1.13- Επίπεδα OSI (Πηγή: Wikipedia)

- Το **φυσικό επίπεδο** ευθύνεται για τη μετάδοση και τη λήψη αδόμητων ανεπεξέργαστων δεδομένων ανάμεσα σε μια συσκευή και ένα φυσικό μέσο μετάδοσης.

Μετατρέπει τα ψηφιακά μπιτ σε ηλεκτρικά, ραδιοφωνικά ή οπτικά σήματα. Οι προδιαγραφές του επιπέδου καθορίζουν χαρακτηριστικά, όπως την ηλεκτρική τάση, τον χρονισμό της αλλαγής τάσεως, τον φυσικό ρυθμό μετάδοσης δεδομένων, τη μέγιστη απόσταση μετάδοσης, το σύστημα διαμόρφωσης, τη μέθοδο πρόσβασης καναλιού και τα φυσικά βύσματα.

- Το επίπεδο **ζεύξης δεδομένων** (**data link)** παρέχει μεταφορά δεδομένων από κόμβο σε κόμβο. Χωρίζεται σε δύο υποστρώματα:

- Το επίπεδο **Ελέγχου Πρόσβασης Μέσων (Media Access Control) (MAC)** – Ελέγχει την πρόσβαση των συσκευών ενός δικτύου σε ένα μέσο και το αν επιτρέπεται να μεταδώσουν δεδομένα.

- Το επίπεδο **Ελέγχου Λογικής Ζεύξης (LLC)** – Αναγνωρίζει κι ενθυλακώνει τα πρωτόκολλα δικτύου κι ελέγχει τη διάγνωση σφαλμάτων και τον συγχρονισμό πλαισίου.

Τα πρωτόκολλα **802.3 Ethernet** και **802.11 Wi-Fi**, λειτουργούν στο επίπεδο ζεύξης δεδομένων.

- Το **επίπεδο δικτύου** ευθύνεται για τη **μεταφορά** αλληλουχιών δεδομένων (λέγονται **πακέτα**) από έναν κόμβο σε έναν άλλο, που είναι συνδεδεμένοι σε "**διαφορετικά δίκτυα**".

Αυτοί οι κόμβοι ταυτοποιούνται από μια διεύθυνση του 3ου επιπέδου, που συνήθως είναι **διεύθυνση IP**.

Τα Routers αναλαμβάνουν τη μεταφορά πακέτων στους κόμβους προορισμού, βρίσκοντας τον δρόμο τους μέσα από τα διάφορα δίκτυα.

- Το **επίπεδο μεταφοράς** ευθύνεται για τη **μεταφορά** αλληλουχιών δεδομένων (λέγονται **τμήματα**) από μια πηγή προς έναν εξυπηρετητή, διατηρώντας παράλληλα την **ποιότητα υπηρεσίας** (**quality of service)**. Πρωτόκολλα όπως το **TCP** και το **UDP** λειτουργούν σε αυτό το επίπεδο. **Οι θύρες** αυτού του επιπέδου είναι τα σημεία εισόδου στις δημόσιες υπηρεσίες του server.

- Το **επίπεδο συνόδου** ελέγχει **τους διαλόγους** (επίσης γνωστούς κι ως συνδέσεις ή συνόδους) ανάμεσα στους υπολογιστές (ανάμεσα σε τοπικές κι απομακρυσμένες εφαρμογές).

- Το **επίπεδο παρουσίασης** επιτρέπει την επικοινωνία ανάμεσα σε συστήματα με διαφορετική **σύνταξη** και σημασιολογία (για παράδειγμα, οι κώδικες **ASCII** και EBCDIC, η συμπίεση βίντεο **MPEG** ή η δομή δεδομένων XML).

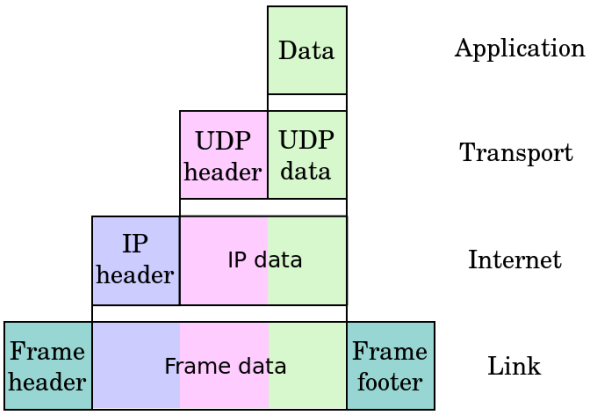
- Το **επίπεδο εφαρμογής** αλληλεπιδρά με **λογισμικό εφαρμογής** που ενσωματώνει κάποιο στοιχείο επικοινωνίας. Τέτοια προγράμματα (για παράδειγμα **FTP** server/clients, πλοηγοί διαδικτύου...) δεν εμπίπτουν στο πεδίο εφαρμογής του μοντέλου OSI.

Μερικά πολύ γνωστά πρωτόκολλα 7ου επιπέδου είναι τα **HTTP** και **Modbus.**

Στα δίκτυα ηλεκτρονικών υπολογιστών, **η ενθυλάκωση** είναι μια μέθοδος σχεδιασμού δομοστοιχειακών πρωτοκόλλων επικοινωνίας, όπου το κάθε επίπεδο φτιάχνει μια μονάδα δεδομένων πρωτοκόλλου (protocol data unit) (PDU) προσθέτοντας κεφαλίδα (μερικές φορές και υποσέλιδο) με τις πληροφορίες ελέγχου για το PDU από το πάνω επίπεδο.

Το φυσικό επίπεδο ευθύνεται για τη φυσική μετάδοση των δεδομένων, η ενθυλάκωση ζεύξης επιτρέπει την τοπική δικτύωση, το διαδικτυακό πρωτόκολλο (Internet Protocol) (IP) δίνει παγκόσμια διεύθυνση στον κάθε υπολογιστή, και το πρωτόκολλο ελέγχου μετάδοσης (Transmission Control Protocol) (TCP) επιλέγει τη διεργασία ή εφαρμογή, δηλαδή τη θύρα που καθορίζει η υπηρεσία, όπως ένας σέρβερ Web ή TFTP.

Παραδείγματος χάρη, στη σουίτα πρωτοκόλλων διαδικτύου, τα περιεχόμενα μιας σελίδας web είναι ενθυλακωμένα με κεφαλίδα HTTP, μετά με κεφαλίδα TCP, κεφαλίδα IP, και στο τέλος, με κεφαλίδα πλαισίου και υποσέλιδο. Το πλαίσιο προωθείται στον κόμβο προορισμού σε μορφή ροής από μπιτ, όπου γίνεται αντιστροφή της ενθυλάκωσης στο κάθε PDU και ερμηνεία του στο κάθε επίπεδο του κόμβου που λαμβάνει.



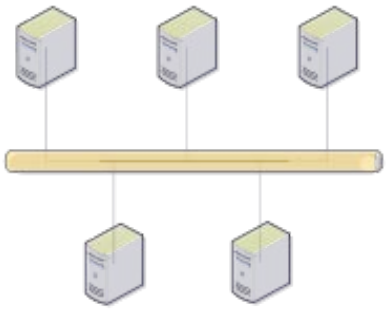
Εικόνα 1.14- Ενθυλάκωση δεδομένων (Πηγή: Wikipedia)

Τοπολογία δικτύου είναι η διάταξη των στοιχείων (ζεύξεις, κόμβοι, κλπ.) ενός δικτύου επικοινωνίας.

Φυσική τοπολογία είναι η τοποθέτηση των διάφορων στοιχείων ενός δικτύου (θέση συσκευών κι εγκαταστάσεις καλωδίων), ενώ η λογική τοπολογία απεικονίζει τη ροή των δεδομένων μέσα σ' ένα δίκτυο. Οι αποστάσεις ανάμεσα στους κόμβους, οι φυσικές διασυνδέσεις, οι ρυθμοί μετάδοσης, ή οι τύποι των σημάτων μπορεί να διαφέρουν ανάμεσα σε δύο διαφορετικά δίκτυα, αλλά οι τοπολογίες τους μπορεί να είναι ολόιδιες.

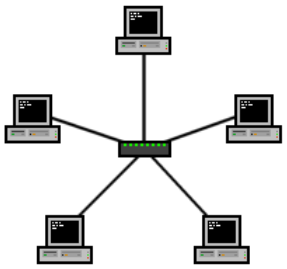
Η φυσική τοπολογία ενός δικτύου αφορά στο φυσικό επίπεδο του μοντέλου OSI.

Στην τοπολογία διαύλου, οι σταθμοί εργασίας συνδέονται απευθείας σε μια κοινή, γραμμική ζεύξη εναλλάξ διπλής κατεύθυνσης, με κάποιο μέσο, όπως ένα συνεστραμμένο ζεύγος ή ένα ομοαξονικό καλώδιο, και λαμβάνουν όλη την κίνηση που δημιουργείται στον κάθε σταθμό. Στο τέλος της γραμμής χρειάζονται τερματικό αντιστάτη, που θα εξαλείψει τις αναπηδήσεις των σημάτων.



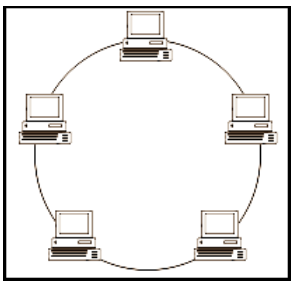
Εικόνα 1.15- Τοπολογία διαύλου (Πηγή: Wikipedia)

Σε ένα δίκτυο αστέρα, κάθε εξυπηρετητής συνδέεται σε έναν κεντρικό διανομέα (συνήθως ένας μεταγωγέας (switch)), που αναμεταδίδει μηνύματα από σταθμούς αποστολής σε σταθμούς λήψης. Είναι μία από τις πιο κοινές τοπολογίες δικτύου ηλεκτρονικών υπολογιστών.



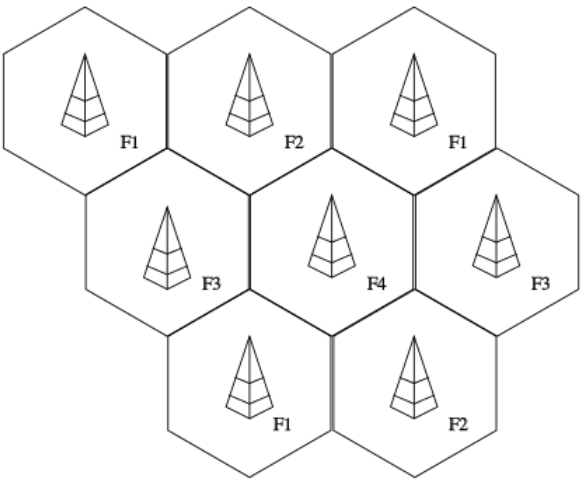
Εικόνα 1.16- Τοπολογία αστεριού (Πηγή: Wikipedia)

Ένα δίκτυο δακτυλίου είναι μια τοπολογία δικτύου στην οποία ο κάθε κόμβος συνδέεται ακριβώς με άλλους δύο κόμβους, σχηματίζοντας ένα μεμονωμένο συνεχές πέρασμα σημάτων από τον κάθε κόμβο. Τα δεδομένα ταξιδεύουν από κόμβο σε κόμβο, και ο κάθε κόμβος διαχειρίζεται κάθε πακέτο.



Εικόνα 1.17- Τοπολογία δακτυλίου (Πηγή: Wikimedia)

Ένα κυψελοειδές δίκτυο είναι ένα δίκτυο επικοινωνίας, όπου ο τελευταίος κρίκος είναι ασύρματος. Το δίκτυο κατανέμεται σε περιοχές που λέγονται κυψέλες, με την καθεμιά να έχει τουλάχιστον ένα σημείο πρόσβασης. Αυτοί οι κόμβοι παρέχουν στην κυψέλη κάλυψη δικτύου, που χρησιμοποιείται για τη μετάδοση φωνής, δεδομένων και περιεχομένου άλλων τύπων.

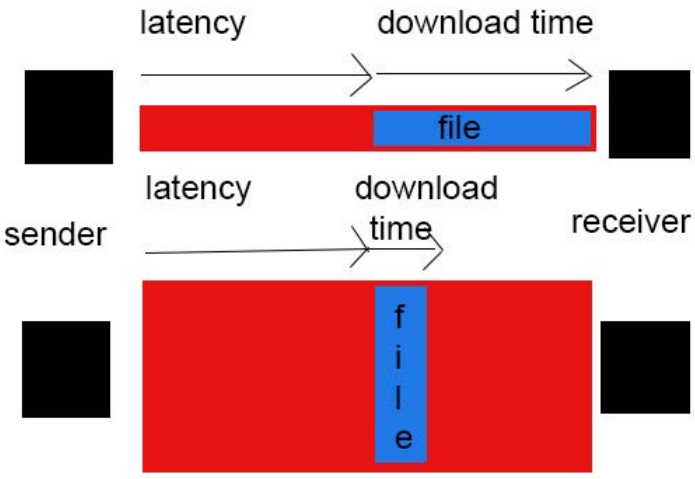


Εικόνα 1.18- Κυψελοειδής τοπολογία (Πηγή: Wikipedia)

Το **εύρος ζώνης (bandwidth)** και η **καθυστέρηση μεταφοράς** (**latency)** (Εικόνα 1.19) είναι δύο από τα σημαντικότερα χαρακτηριστικά ενός ψηφιακού δικτύου.

Η καθυστέρηση μεταφοράς εκφράζεται με μονάδα μέτρησης χρόνου, συνήθως milliseconds (ms). Η καθυστέρηση μεταφοράς είναι ο χρόνος που χρειάζονται τα δεδομένα για να ταξιδέψουν από το ένα σημείο στο άλλο. Εξαρτάται από τη φυσική απόσταση που πρέπει να ταξιδέψουν τα δεδομένα μέσω καλωδίων, δικτύων κλπ. για να φτάσουν στον προορισμό τους.

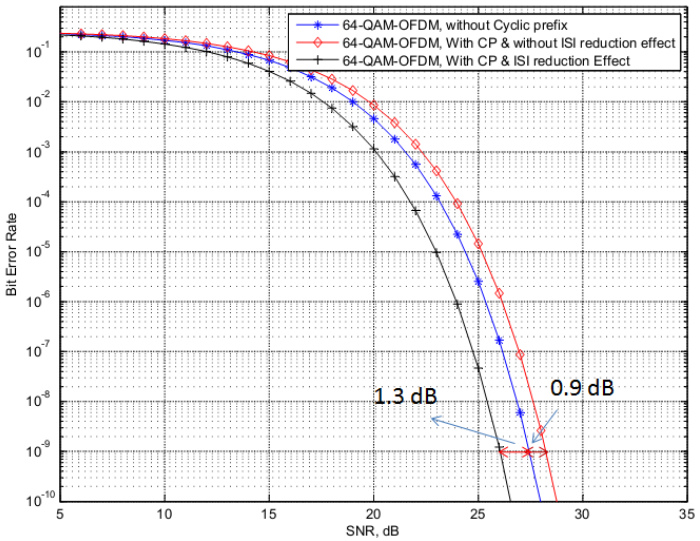
Το εύρος ζώνης εκφράζεται σε μπιτ ανά δευτερόλεπτο (bps). Αφορά στον όγκο δεδομένων που μπορεί να μεταφερθεί μέσα σε ένα δευτερόλεπτο. Προφανώς, όσο πιο φαρδιά είναι η διοχέτευση (pipeline), τόσο πιο πολλά μπιτ μπορούν να μεταφερθούν ανά δευτερόλεπτο. Αν υπάρχει συμφόρηση στο εύρος ζώνης αυξάνεται η καθυστέρηση μεταφοράς.



Εικόνα 1.19- Καθυστέρηση μεταφοράς και εύρος ζώνης (Πηγή: Wikipedia)

Στην ψηφιακή μετάδοση, ο **ρυθμός σφαλμάτων μπιτ (bit error rate)** (**BER**) είναι ο αριθμός των σφαλμάτων μπιτ ανά μονάδα χρόνου. Η αναλογία σφαλμάτων μπιτ (**bit error ratio)** (επίσης **BER**) είναι ο αριθμός των σφαλμάτων μπιτ διαιρεμένος με τον συνολικό αριθμό των μπιτ που μεταφέρθηκαν σε συγκεκριμένο χρονικό μεσοδιάστημα. Η αναλογία σφαλμάτων μπιτ μετράει την απόδοση αλλά δεν έχει μονάδα μέτρησης. Συνήθως εκφράζεται ως ποσοστό.

Τα μπιτ που ελήφθησαν σε ένα κανάλι επικοινωνίας μπορεί να αλλοιωθούν λόγω θορύβου, παρεμβολών, παραμόρφωσης ή λόγω σφάλματος συγχρονισμού των μπιτ. Ο λόγος σήματος προς θόρυβο (Signal To Noise Ratio) (SNR) δείχνει την αναλογία των μη επιθυμητών σημάτων σε σχέση με το σήμα που μεταδίδει την πληροφορία. Όπως δείχνει η Εικόνα 1.20, όσο πιο υψηλό είναι το SNR (καλύτερο σήμα) τόσο πιο χαμηλό είναι το BER (λιγότερα λάθη κατά τη μετάδοση).



Εικόνα 1.20- SNR vs BER (Πηγή: Wikipedia)

Ένα **τοπικό δίκτυο** (**local area network)** (**LAN**) είναι ένα δίκτυο υπολογιστών, που διασυνδέει υπολογιστές σε μια περιορισμένη περιοχή, όπως σε μια οικία, ένα σχολείο, ένα εργαστήριο, μια πανεπιστημιούπολη ή ένα γραφείο.

Το **Ethernet** και το **Wi-Fi** είναι οι δύο πιο κοινές τεχνολογίες που χρησιμοποιούνται στα τοπικά δίκτυα.

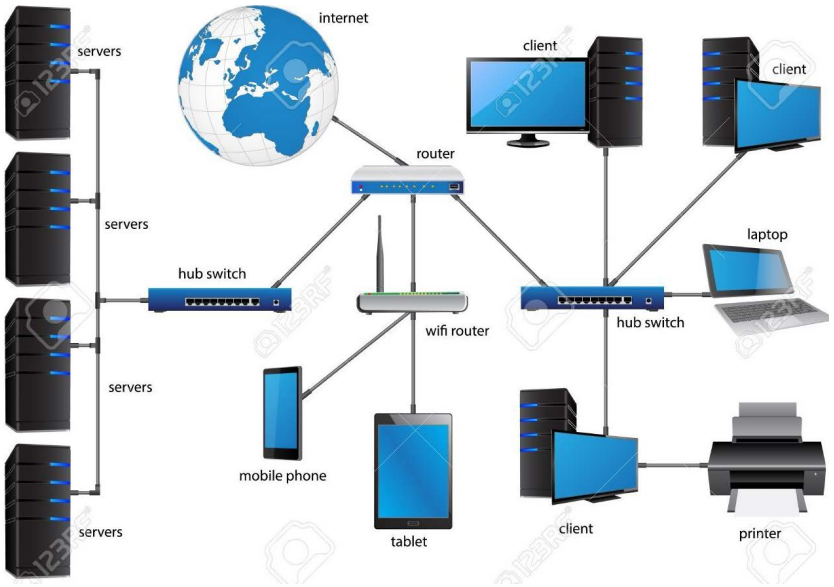
Η **1000BASE-T** και η **δομημένη καλωδίωση** είναι οι βάσεις των περισσότερων μοντέρνων εμπορικών LAN. Ενώ η χρήση οπτικής ίνας είναι συνηθισμένη στις ζεύξεις ανάμεσα στους μεταγωγείς (switches) του δικτύου, σπανίζει στους επιτραπέζιους υπολογιστές.

Σε ένα ασύρματο **LAN**, οι χρήστες έχουν απεριόριστη ελευθερία κίνησης στην καλυπτόμενη περιοχή. Τα ασύρματα δίκτυα έχουν γίνει δημοφιλή σε κατοικίες και σε μικρές εταιρείες, λόγω της ευκολίας στην εγκατάστασή τους. Τα περισσότερα ασύρματα LAN χρησιμοποιούν Wi-Fi, αφού είναι ενσωματωμένο σε κινητά, tablets, και φορητούς υπολογιστές. Οι επισκέπτες συνήθως αποκτούν πρόσβαση στο διαδίκτυο μέσω υπηρεσίας hotspot.

Τα απλά LANs συνήθως αποτελούνται από την καλωδίωση κι ένα ή περισσότερα switches. Το switch μπορεί να συνδεθεί σε router, σε modem τεχνολογίας cable, ή σε ADSL modem για πρόσβαση στο διαδίκτυο.

Ένα LAN μπορεί να περιλαμβάνει μια μεγάλη ποικιλία άλλων συσκευών δικτύου, όπως **τείχη προστασίας** (**firewalls)**, ισορροπιστές φορτίου κι ανιχνευτές εισβολής στο δίκτυο. Τα πιο προχωρημένα LANs χαρακτηρίζονται από τη χρήση παραπανίσιων ζεύξεων με switches που χρησιμοποιούν το spanning tree protocol για την αποφυγή βρόχων, από την ικανότητά τους να διαχειριστούν διαφορετικούς τύπους κίνησης μέσω του quality of service (QoS), κι από την ικανότητά τους να διαχωρίσουν την κίνηση με τα **VLANs**.

Στα πιο υψηλά επίπεδα των δικτύων, πρωτόκολλα όπως τα NetBEUI, IPX/SPX, AppleTalk και άλλα, ήταν κάποτε κοινά, αλλά η συλλογή πρωτοκόλλων επικοινωνίας (**TCP/IP**) έχει επικρατήσει ως η πιο διαδεδομένη.



Εικόνα 1.21- Δομή τοπικού δικτύου LAN (Πηγή: Wikimedia)

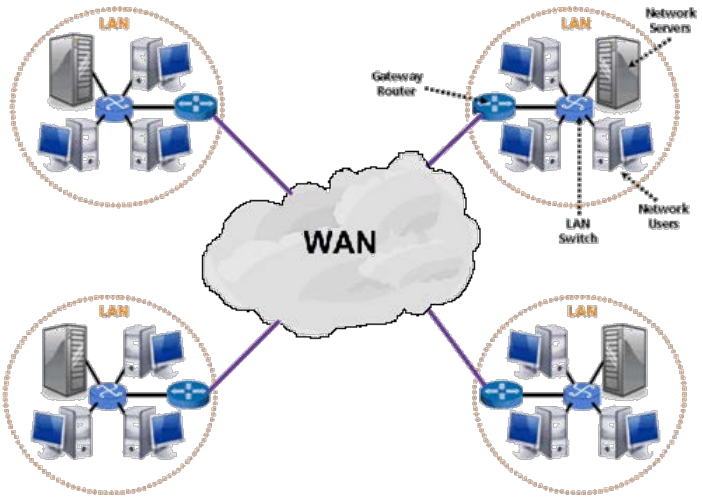
Τα δίκτυα LAN μπορούν να διατηρήσουν συνδέσεις με άλλα δίκτυα LAN μέσω μισθωμένων γραμμών, υπηρεσιών μίσθωσης ή μέσω του διαδικτύου, χρησιμοποιώντας τεχνολογίες **εικονικού ιδιωτικού δικτύου (virtual private network) (VPN)**. Ανάλογα με το πώς δημιουργήθηκαν κι ασφαλίστηκαν οι συνδέσεις, καθώς και τη μεταξύ τους απόσταση, τέτοια συνδεδεμένα δίκτυα LAN μπορούν να ταξινομηθούν κι ως μητροπολιτικά δίκτυα (metropolitan area network) (MAN) ή δίκτυα ευρείας περιοχής (wide area network)

(WAN).

Ένα **δίκτυο ευρείας περιοχής** (**WAN**) είναι ένα δίκτυο τηλεπικοινωνιών που εκτείνεται σε μεγάλες γεωγραφικές αποστάσεις, με πρωταρχικό σκοπό τη δικτύωση υπολογιστών. Τα WAN δημιουργούνται συνήθως με μισθωμένα κυκλώματα τηλεπικοινωνιών.

Εταιρείες, μορφωτικά ιδρύματα και κυβερνητικές υπηρεσίες χρησιμοποιούν τα WAN για να μεταφέρουν δεδομένα στο προσωπικό, στους φοιτητές, στους πελάτες, στους αγοραστές και στους προμηθευτές από διάφορες τοποθεσίες σε ολόκληρο τον κόσμο. Στην ουσία, αυτός ο τρόπος τηλεπικοινωνίας επιτρέπει σε μια εταιρεία να πραγματοποιήσει την καθημερινή της λειτουργία ανεξαρτήτως τοποθεσίας. Το διαδίκτυο μπορεί να θεωρηθεί ως WAN.

Πολλά WANs φτιάχνονται για έναν συγκεκριμένο οργανισμό και είναι ιδιωτικά, συνδέοντας, για παράδειγμα, τα διάφορα γραφεία μιας εταιρείας με τα κεντρικά. Άλλα, που φτιάχνονται από παρόχους υπηρεσιών διαδικτύου (Internet service providers) (ISPs), παρέχουν συνδέσεις από το LAN ενός οργανισμού προς το διαδίκτυο.

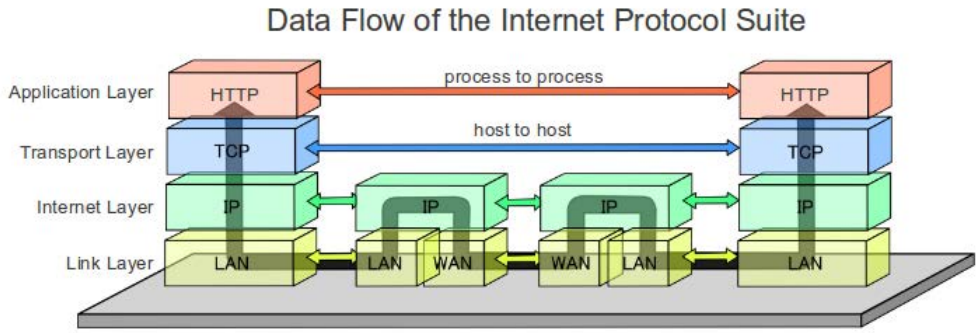


Εικόνα 1.22- Δίκτυο WAN (Πηγή: Wikimedia)

Υπάρχουν πολλές διαθέσιμες τεχνολογίες για ζεύξεις WAN, όπως τηλεφωνικές γραμμές μεταγωγής κυκλώματος (circuit-switched), μετάδοση ραδιοφωνικών κυμάτων και οπτικές ίνες.

Η τυποποιημένη μέθοδος μέσω της οποίας μεταδίδουν πληροφορίες οι κόμβοι στον δίαυλο ή στην καλωδίωση του δικτύου, λέγεται **πρωτόκολλο**. Το πρωτόκολλο καθορίζει τους κανόνες, τη σύνταξη, τη σημασιολογία, τον συγχρονισμό της επικοινωνίας και πιθανές μεθόδους επαναφοράς λόγω σφάλματος. Τα πρωτόκολλα ενσωματώνονται μέσω υλικού, λογισμικού ή μέσω συνδυασμού και των δύο.

Πολλαπλά πρωτόκολλα συχνά περιγράφουν διαφορετικές πτυχές μιας μεμονωμένης επικοινωνίας. Μια ομάδα πρωτοκόλλων που σχεδιάστηκαν για να λειτουργούν μαζί, είναι γνωστά ως σουίτα πρωτοκόλλου.

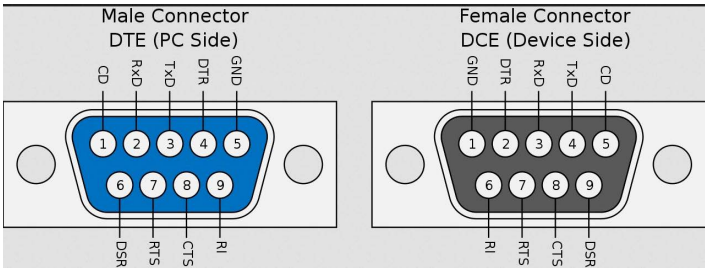


Εικόνα 1.23- Σουίτα πρωτοκόλλου TCP/IP (Πηγή: Wikimedia)

Στη μετάδοση δεδομένων, **σειριακή επικοινωνία** είναι η διαδικασία αποστολής δεδομένων με ένα μπιτ τη φορά, διαδοχικά, σε ένα κανάλι επικοινωνίας ή δίαυλο υπολογιστή. Είναι πολύ κοινή στα βιομηχανικά δίκτυα λόγω απλότητας, και τα RS-232 και RS-485 είναι τα πιο διαδεδομένα πρωτόκολλα σειριακής επικοινωνίας. Αυτά τα πρωτόκολλα αντιστοιχούν στο φυσικό επίπεδο του μοντέλου OSI.

Το **RS-232** αφορά σε πρότυπο για σειριακή μετάδοση δεδομένων. Καθορίζει επίσημα τα σήματα ανάμεσα σε ένα **DTE** (data terminal equipment) (τερματικός εξοπλισμός) όπως έναν τερματικό υπολογιστή, και τον **DCE** (data circuit-terminating equipment ή data communication equipment) (εξοπλισμός μετάδοσης δεδομένων), όπως ένα modem. Άρα δεν μπορεί να θεωρηθεί δικτυακό πρωτόκολλο, αλλά πρωτόκολλο επικοινωνίας από σημείο σε σημείο.

Το πρότυπο καθορίζει τα ηλεκτρικά χαρακτηριστικά και τον χρονισμό των σημάτων, τη σημασία των σημάτων, καθώς και το φυσικό μέγεθος και τη διάταξη των ακίδων των βυσμάτων. Το πρότυπο RS-232 χρησιμοποιούταν πολύ στις **σειριακές θύρες** των ηλεκτρονικών υπολογιστών.



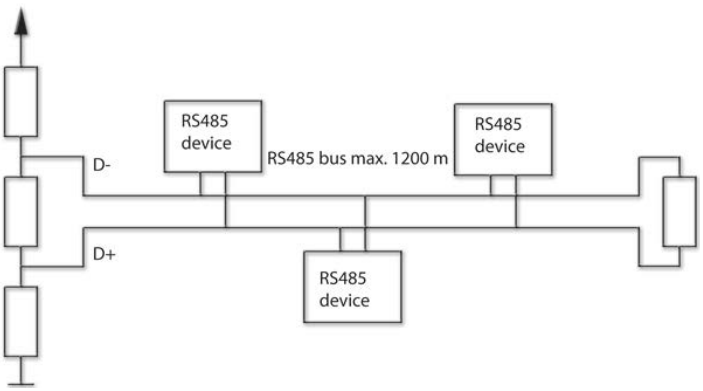
Εικόνα 1.24- Διάταξη ακίδων σε βύσμα RS-232 (Πηγή: Wikimedia)

Το RS-232, συγκριτικά με μετέπειτα διεπαφές, όπως το RS-485 και το Ethernet, έχει λιγότερες δυνατότητες. Στους μοντέρνους προσωπικούς ηλεκτρονικούς υπολογιστές, το USB έχει αντικαταστήσει το RS-232 στα περισσότερα περιφερειακά. Αλλά χάρη στην απλότητά του, το RS-232 εξακολουθεί να χρησιμοποιείται – ειδικά σε βιομηχανικά μηχανήματα, όπου αρκεί μια καλωδιακή σύνδεση μικρής εμβέλειας, από σημείο σε σημείο, και χαμηλής ταχύτητας.

Το **RS-485** είναι ένα πρότυπο που καθορίζει τα ηλεκτρικά χαρακτηριστικά των οδηγών και των δεκτών που χρησιμοποιούνται σε συστήματα σειριακής επικοινωνίας.

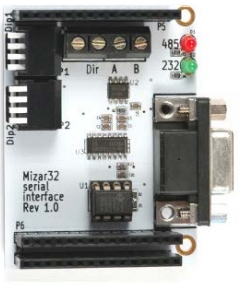
Τα ψηφιακά δίκτυα επικοινωνίας που ενσωματώνουν το πρότυπο μπορούν να χρησιμοποιηθούν αποτελεσματικά σε μεγάλες αποστάσεις και σε περιβάλλοντα με ηλεκτρικό θόρυβο.

Σε ένα τέτοιο δίκτυο μπορούν να συνδεθούν **πολλαπλοί δέκτες** σε γραμμικό, πολυτερματικό δίαυλο. Αυτά τα χαρακτηριστικά κάνουν το RS-485 χρήσιμο σε ICS κι αντίστοιχες εφαρμογές.



Εικόνα 1.25- Δομή δικτύου RS-485 (Πηγή: Wikimedia)

Οι προσωπικοί υπολογιστές ίσως χρειαστούν μετατροπείς δικτύου (συνήθως από RS232 σε RS485 ή από USB σε RS485) για να συνδεθούν σε ένα δίκτυο RS485.

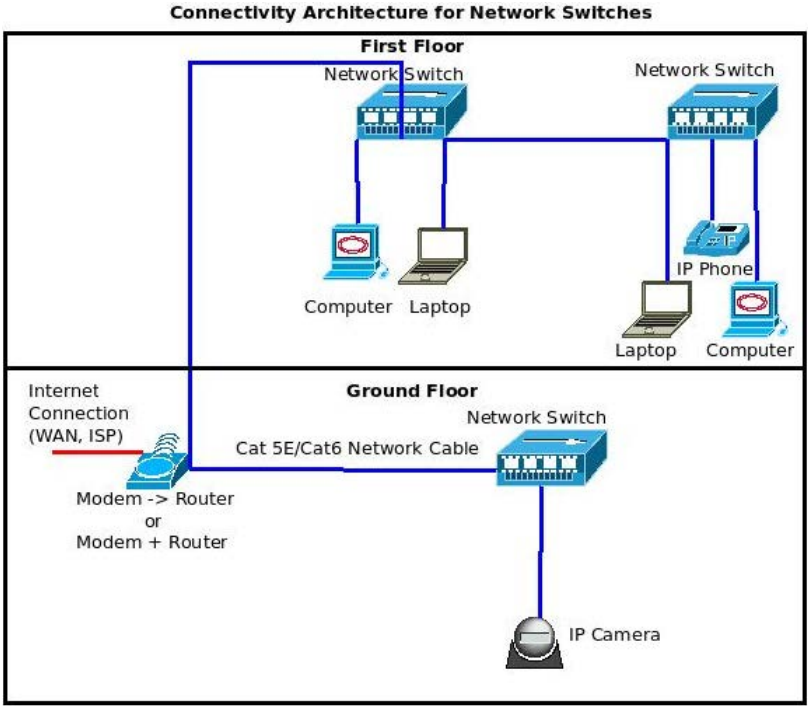


Εικόνα 1.26- Μετατροπέας RS-485/RS-232 (Πηγή: Wikimedia)

Ethernet λέγεται μια οικογένεια δικτυακών τεχνολογιών, που χρησιμοποιούνται κυρίως σε τοπικά δίκτυα (LAN). Οι νεότερες εκδοχές του Ethernet χρησιμοποιούν συνεστραμμένα ζεύγη (**καλώδια UTP και βύσματα RJ45**) και οπτικές ίνες, ή συνεστραμμένα ζεύγη σε συνδυασμό με **switches**. Τα πρότυπα Ethernet αποτελούνται από πολλές καλωδιώσεις κι εκδοχές σημάτων του **φυσικού επιπέδου** OSI που χρησιμοποιείται στο Ethernet.

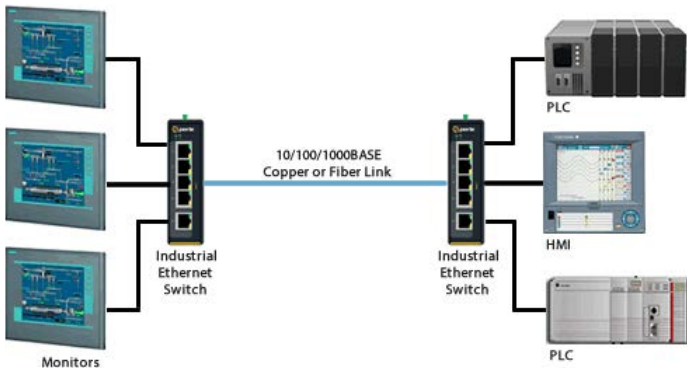
Εικόνα 1.28 – Καλώδιο Ethernet (UTP+RJ45) (Πηγή: Wikimedia)

Η πιο κοινή φυσική τοπολογία για δίκτυα Ethernet είναι η τοπολογία **δακτυλίου,** που βασίζεται σε switches.



Εικόνα 1.29- Τοπολογία δακτυλίου σε δίκτυο Ethernet (Πηγή: Wikipedia)

Τα ICSs στη βιομηχανία βασίζονται συχνά στο πρωτόκολλο Ethernet, που διευκολύνει την κατανομή πληροφοριών ανάμεσα σε συσκευές OT και σταθμούς εργασίας IT. Τα βιομηχανικά switches χρησιμοποιούνται για τη σύνδεση εξοπλισμού OT, όπως PLCs, HMI και οθόνες (Εικόνα 1.30)

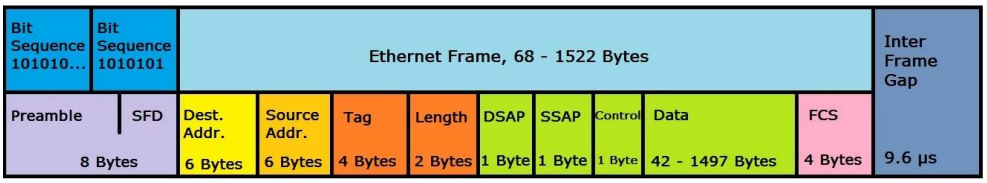


Εικόνα 1.30- Δομή βιομηχανικού δικτύου Ethernet

Κάθε κόμβος (υπολογιστές, PLCs...) που συνδέεται σε δίκτυο Ethernet χρειάζεται μια ειδική κάρτα **(Κάρτα Διεπαφής Δικτύου)** (**Network Interface Controller**, **NIC**) που παρέχει τη φυσική διεπαφή και τη λογική διαδικασία (**CSMA/CD**) που απαιτείται για την πρόσβαση και την ανταλλαγή πληροφοριών σε εκείνο το δίκτυο.

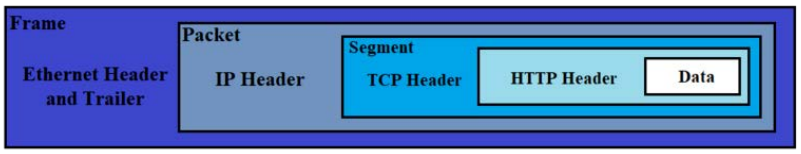
Εικόνα 1.31- Ethernet NIC (Πηγή: Wikipedia)

Τα συστήματα που επικοινωνούν μέσω Ethernet διαχωρίζουν τη ροή δεδομένων σε μικρότερα κομμάτια, που λέγονται **πλαίσια**. Κάθε πλαίσιο περιλαμβάνει διευθύνσεις πηγής και προορισμού (48 bit **MAC address**), και δεδομένα ελέγχου σφάλματος, για τον εντοπισμό και την απόρριψη των κατεστραμμένων πλαισίων. Σύμφωνα με το μοντέλο OSI, το Ethernet παρέχει υπηρεσίες που συμπεριλαμβάνονται στο **επίπεδο ζεύξης δεδομένων.**



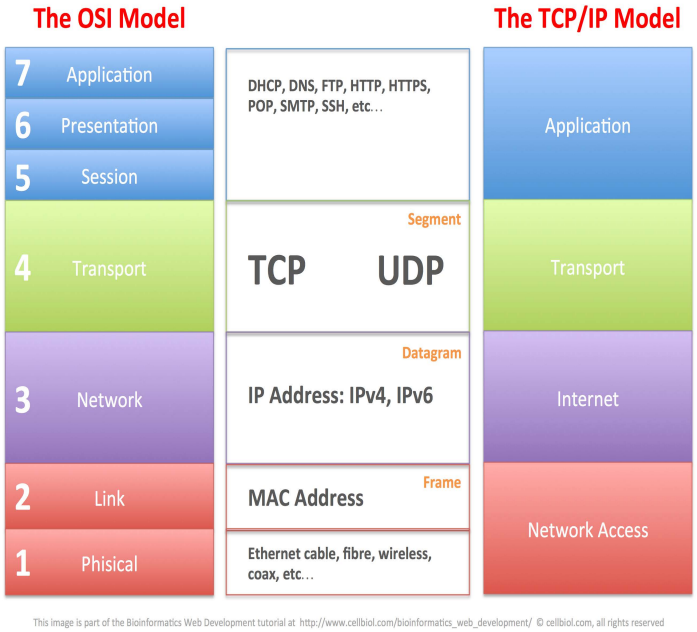
Εικόνα 1.31- Πλαίσιο Ethernet (Πηγή: Wikipedia)

Το πρωτόκολλο διαδικτύου (Internet Protocol) (IP) μεταφέρεται μέσω Ethernet και θεωρείται μία από τις κύριες τεχνολογίες που συνθέτουν το διαδίκτυο.



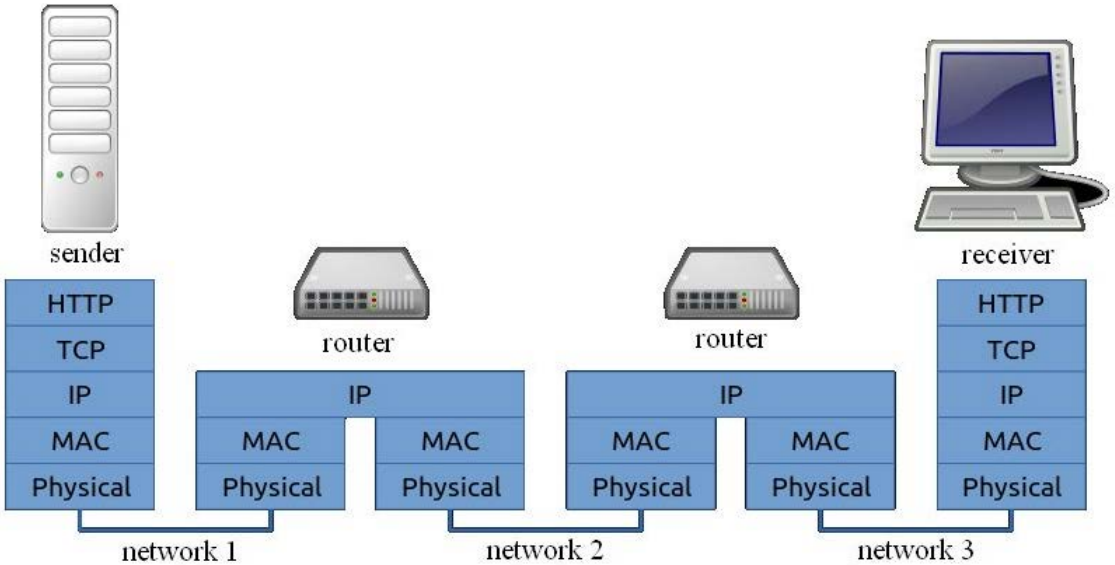
Εικόνα 1.32- Πακέτο IP ενθυλακωμένο σε πλαίσιο Ethernet (Πηγή: Wikimedia)

Η **σουίτα πρωτοκόλλου διαδικτύου** είναι το εννοιολογικό μοντέλο και το σετ πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται στο διαδίκτυο και σε παρόμοια δίκτυα υπολογιστή. Είναι κοινά γνωστή ως **TCP/IP,** διότι τα θεμελιώδη πρωτόκολλα της σουίτας είναι το Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol) (TCP) και το Πρωτόκολλο Διαδικτύου (IP). Η εικόνα 1.33 συγκρίνει το μοντέλο OSI με την υλοποίηση TCP/IP, όπου τα πρωτόκολλα του επιπέδου εφαρμογής (FTP...) χρησιμοποιούν τις υπηρεσίες μεταφοράς που παρέχουν τα πρωτόκολλα TCP/IP.



Εικόνα 1.33- Στοίβα πρωτοκόλλου επικοινωνίας (Πηγή: blog.pythian.com)

Το TCP/IP παρέχει επικοινωνία δεδομένων **end-to-end** και καθορίζει το πακετάρισμα, τη διεύθυνση, τη μετάδοση, τη δρομολόγηση και τη λήψη δεδομένων. Αυτή η λειτουργικότητα οργανώνεται σε **τέσσερα αφηρημένα επίπεδα**. Από το χαμηλότερο ως το ψηλότερο, τα επίπεδα είναι το **επίπεδο ζεύξης δεδομένων** (βασίζεται συνήθως στο Ethernet), που εμπεριέχει μεθόδους επικοινωνίας για τα δεδομένα που απομένουν σε ένα μεμονωμένο τμήμα του δικτύου (link); το **επίπεδο διαδικτύου** (βασίζεται στο πρωτόκολλο IP) , που παρέχει διαδικτύωση ανάμεσα σε ανεξάρτητα δίκτυα; το **επίπεδο μεταφοράς** (βασίζεται στο πρωτόκολλο TCP), που διαχειρίζεται την επικοινωνία host-to-host, και το **επίπεδο εφαρμογών** (πρωτόκολλα όπως το HTTP και το FTP καθορίζονται σε αυτό το επίπεδο), που προσφέρει process-to-process ανταλλαγή δεδομένων για τις εφαρμογές.

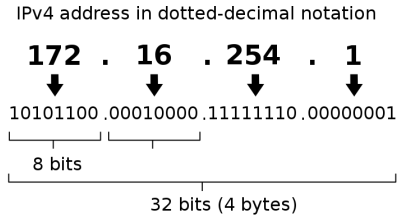


Εικόνα 1.34- Δομή σύνδεσης TCP/IP (Πηγή: Wikimedia)

Το **router** είναι μια συσκευή δικτύωσης που προωθεί πακέτα δεδομένων ανάμεσα σε δίκτυα υπολογιστών. Τα δεδομένα που στέλνονται μέσω του διαδικτύου, όπως μέσω μιας σελίδας web ή μέσω email, έχουν τη μορφή πακέτων δεδομένων. Ένα πακέτο προωθείται συνήθως από ένα router σε ένα άλλο router μέσω των δικτύων που απαρτίζουν ένα διαδίκτυο, μέχρι να φτάσει στον κόμβο προορισμού.

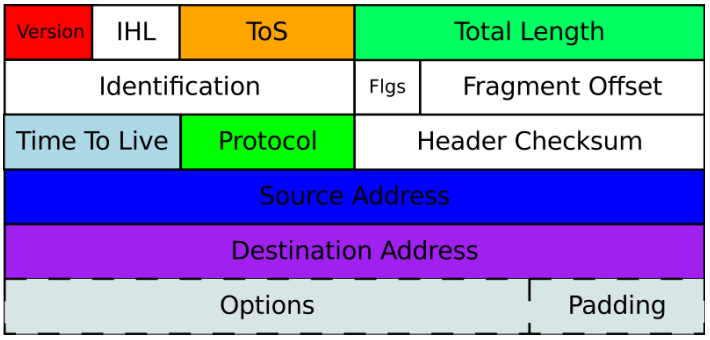
Εικόνα 1.35- Δρομολόγηση πακέτων IP (Πηγή: http://routinglab.blogspot.com)

Η δρομολόγηση βασίζεται στην **ανάθεση διευθύνσεων IP στους κόμβους**. Οι διευθύνσεις IP (v4) είναι 32-bit και απεικονίζονται με ακέραιους αριθμούς. Συνήθως γράφονται με σημειογραφία τελείας δεκαδικού (dot-decimal notation), που αποτελείται από τέσσερις οχτάδες της διεύθυνσης, που εκφράζονται ξεχωριστά σε δεκαδικούς αριθμούς και διαχωρίζονται από τελείες.



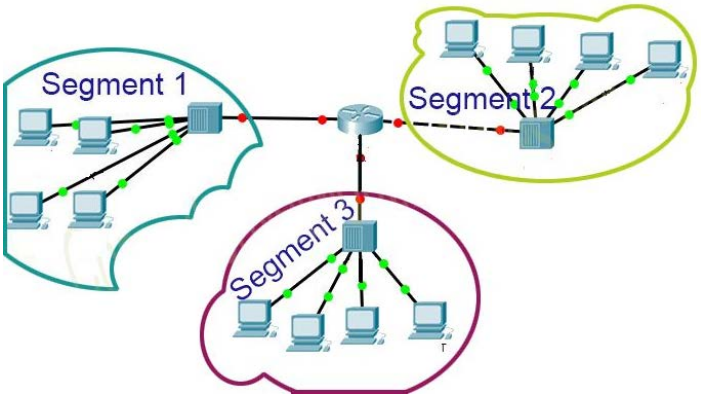
Εικόνα 1.36- Δομή διεύθυνσης IP (Πηγή: Wikimedia)

Οι πληροφορίες στέλνονται από έναν κόμβο μετάδοσης σε έναν κόμβο λήψης υπό τη μορφή πακέτων IP, που συμπεριλαμβάνουν τις διευθύνσεις IP της πηγής και του προορισμού.



Εικόνα 1.37- Δομή πακέτου IP (Πηγή: Wikimedia)

Η κατάτμηση δικτύου στα δίκτυα υπολογιστών είναι ο διαχωρισμός ενός δικτύου σε υποδίκτυα, όπως φαίνεται στην εικόνα 1.38, με το καθένα να αποτελεί ένα τμήμα του δικτύου. Τα πλεονεκτήματα ενός τέτοιου διαχωρισμού είναι η αύξηση των επιδόσεων και η βελτίωση της ασφάλειας.



Εικόνα 1.38- Κατάτμηση δικτύου

Η αύξηση των επιδόσεων επιτυγχάνεται επειδή υπάρχουν λιγότεροι εξυπηρετητές στο κάθε υποδίκτυο, άρα ελαχιστοποιείται η τοπική κίνηση και μειώνεται η συμφόρηση.

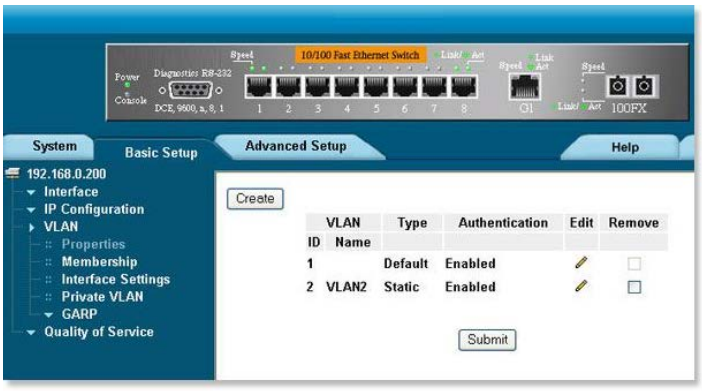
Η αυξημένη ασφάλεια επιτυγχάνεται για τους ακόλουθους λόγους:

- Οι μεταδόσεις θα περιοριστούν στο τοπικό δίκτυο. Η εσωτερική δομή του δικτύου δε θα είναι ορατή απέξω.
- Υπάρχει περιορισμένη επιφάνεια επίθεσης. Οι πιο κοινές επιθέσεις ελαττώνονται μέσω της σωστής κατάτμησης δικτύου, αφού λειτουργούν μόνο στο τοπικό δίκτυο.
- Δημιουργώντας τμήματα δικτύου που εμπεριέχουν μόνο τους πόρους που χρειάζονται οι καταναλωτές που εξουσιοδοτείτε, δημιουργείτε ένα περιβάλλον περιορισμένων δικαιωμάτων.

Ο έλεγχος πρόσβασης επισκεπτών επιτυγχάνεται μέσω της ενσωμάτωσης VLANs για την κατάτμηση του δικτύου.Κατάτμηση δικτύου

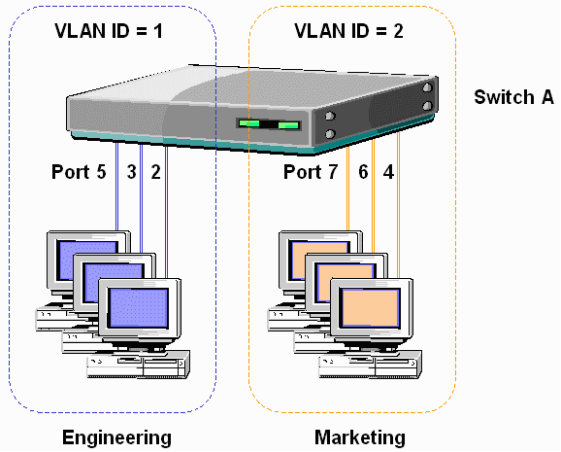
Ένα **εικονικό LAN** (**VLAN**) είναι κάθε τομέας μετάδοσης, που διαχωρίζεται και απομονώνεται σε ένα δίκτυο στο επίπεδο ζεύξης δεδομένων (επίπεδο 2 του OSI).

Για την υποδιαίρεση ενός δικτύου σε VLANs, ο δικτυακός εξοπλισμός (συνήθως switches) πρέπει να ρυθμιστεί μέσω software για να αναθέσει μια ομάδα θυρών στο κάθε VLAN.



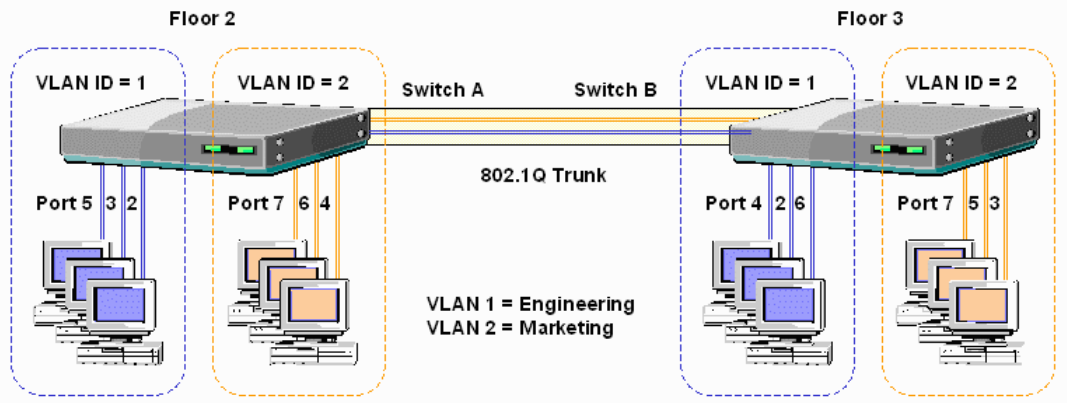
Εικόνα 1.39- Οθόνη ρύθμισης VLAN

Όταν ανατεθούν θύρες στο κάθε VLAN, δεν μπορούν να ανταλλαχθούν δεδομένα ανάμεσα σε κόμβους (υπολογιστές, PLCs...) που είναι συνδεδεμένοι σε διαφορετικές θύρες VLAN.



Εικόνα 1.40- Κατάτμηση VLAN σε switch (Πηγή: http://photos1.blogger.com/blogger/6124/4181/320/vlan-fig1.png)

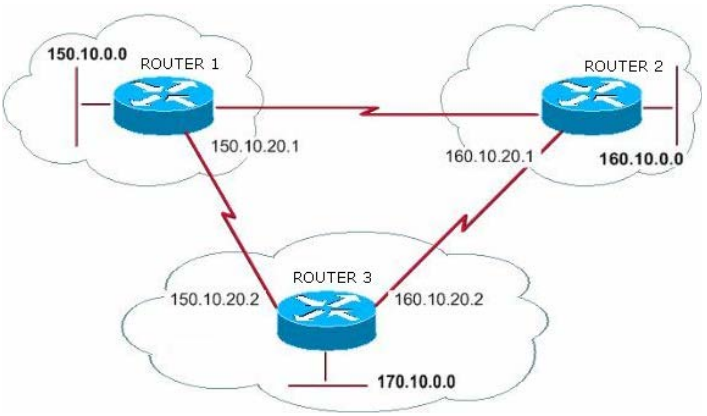
Τα VLANs λειτουργούν θέτοντας **ετικέτες (tags)** (αυτή η μέθοδος αναπτύχθηκε υπό το πρότυπο 802.1Q) σε πλαίσια του 2ου επιπέδου, δημιουργώντας την εμφάνιση και τη λειτουργικότητα κίνησης δικτύου που βρίσκεται φυσικά σε ένα ενιαίο δίκτυο, αλλά φέρεται σαν να είναι διαχωρισμένη σε ξεχωριστά δίκτυα.



Εικόνα 1.41- Ανάθεση ετικετών VLAN (Πηγή: Wikimedia)

Τα VLANs επιτρέπουν στους διαχειριστές δικτύων να ομαδοποιήσουν τους εξυπηρετητές, ακόμα κι αν αυτοί δεν είναι απευθείας συνδεδεμένοι στο ίδιο switch του δικτύου.

Σε τεχνικούς όρους, ένα **router** είναι μια δικτυακή συσκευή πύλης δικτύου (gateway device) του 3ου επιπέδου, άρα επικοινωνεί με δύο ή και περισσότερα δίκτυα και το router λειτουργεί στο επίπεδο δικτύου του μοντέλου OSI. Η εικόνα 1.42 δείχνει πώς τρία router διασυνδέουν διαφορετικά δίκτυα LAN (αναγνωρίζονται από τις διευθύνσεις δικτύου 150.10.0.0, 160.10.0.0 και 170.10.0.0).

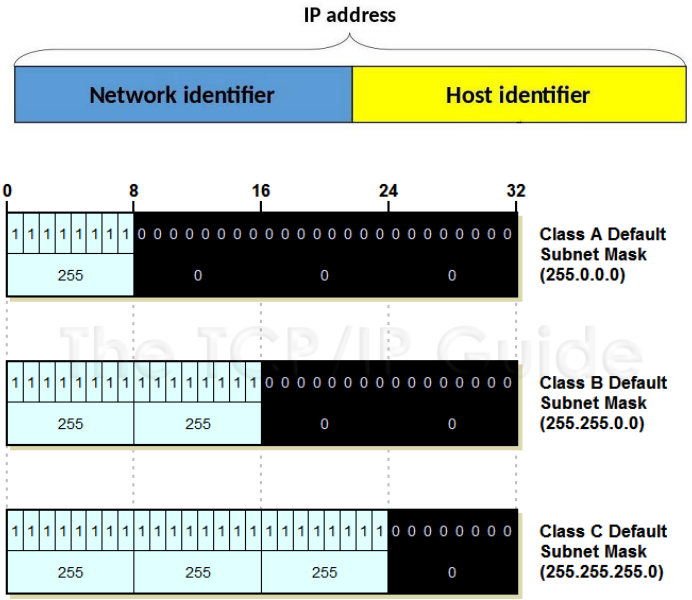


Εικόνα 1.42- Διασύνδεση διαφορετικών δικτύων LAN μέσω router.

Η δρομολόγηση της πληροφορίας από την πηγή στον προορισμό χρειάζεται ένα σύστημα διευθυνσιοδότησης, που συνήθως βασίζεται στις διευθύνσεις του IPv4.

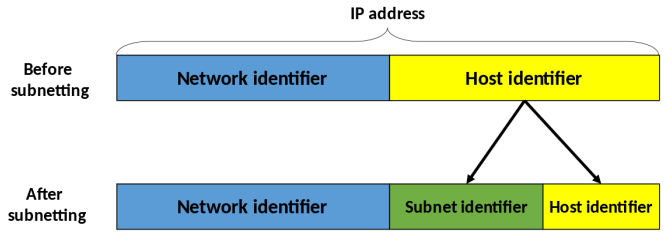
Μια διεύθυνση IP διαχωρίζεται σε δύο πεδία. Στο **αναγνωριστικό του δικτύου (network identifier) (Network ID)** (χρησιμοποιείται από τα routers για να βρουν το δίκτυο προορισμού στο διαδίκτυο) και στο **αναγνωριστικό του εξυπηρετητή** (**host identifier) (Host ID)** (ένα αναγνωριστικό για συγκεκριμένο εξυπηρετητή) (Εικόνα 1.43).

Ο αριθμός των bits στο κάθε πεδίο καθορίζεται από τη **μάσκα δικτύου** (**mask)** της κάθε διεύθυνσης IP, χρησιμοποιώντας λογικά "1" bits για το δικτυακό τμήμα της διεύθυνσης και "0" για το τμήμα του εξυπηρετητή. Ο αριθμός των bits που έχει διανεμηθεί στο τμήμα του δικτύου χρησιμοποιείται για την ταυτοποίηση της διεύθυνσης IP του αντίστοιχου δικτύου (δηλαδή στη διεύθυνση εξυπηρετητή 192.168.1.110/**24** τα πρώτα 24 bits κατανέμονται για τη διευθυνσιοδότηση του δικτύου, οπότε 192.168.1.0**/24** είναι η διεύθυνση IP του δικτύου στο οποίο ανήκει ο εξυπηρετητής).



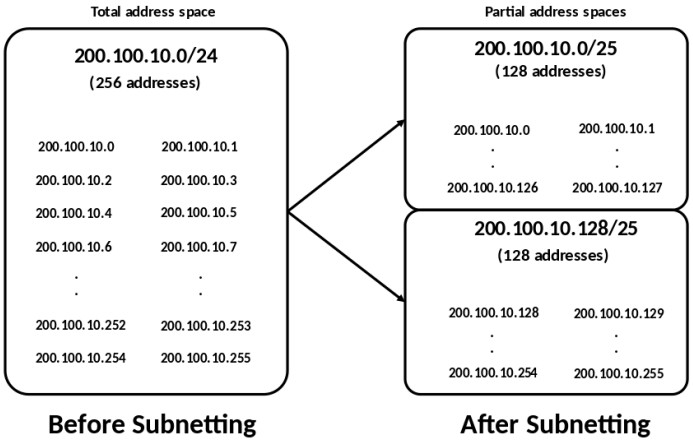
Εικόνα 1.43- Διεύθυνση IP vs μάσκας IP

Ένα **υποδίκτυο (subnetwork** ή **subnet)** είναι λογική υποδιαίρεση (εικόνα 1.44) ενός δικτύου IP. Η πρακτική της διαίρεσης ενός δικτύου σε δύο ή παραπάνω δίκτυα λέγεται **υποδικτύωση (subnetting).**



Εικόνα 1.44- Αναγνωριστικό υποδικτύου IP (Πηγή: Wikipedia)

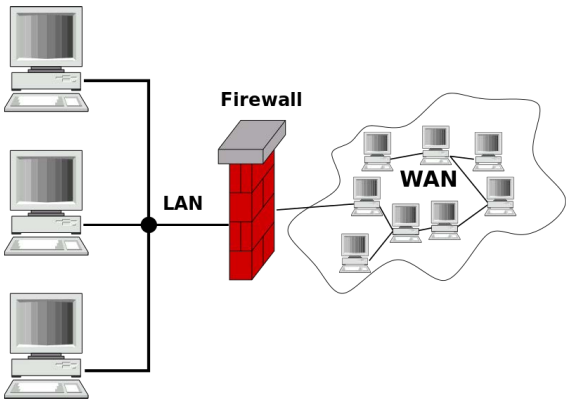
Μερικά bits από το πεδίο αναγνώρισης του εξυπηρετητή κατανέμονται (τροποποιείται η μάσκα του δικτύου IP για την προσθήκη περισσότερων "1" bits στο πεδίο του υποδικτύου) για τη δημιουργία **αναγνωριστικού υποδικτύου** (**subnet identifier)**. Οι υπολογιστές που ανήκουν στο ίδιο υποδίκτυο διευθυνσιοδοτούνται με ολόιδιο αναγνωριστικό υποδικτύου στις διευθύνσεις IP τους.



Εικόνα 1.45- Κατάτμηση υποδικτύωσης IP (Πηγή: Wikimedia)

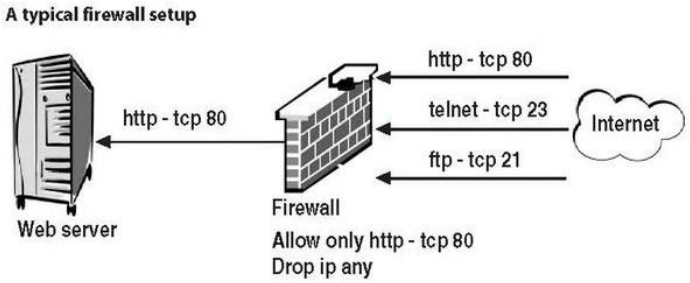
Υπολογιστές που βρίσκονται σε διαφορετικά υποδίκτυα IP χρειάζονται ένα router για να επικοινωνήσουν μεταξύ τους, οπότε η υποδικτύωση είναι μια έγκυρη μέθοδος για την κατάτμηση ενός δικτύου σε απομονωμένα τμήματα.

Το **τείχος προστασίας** (**firewall)** είναι ένα δικτυακό σύστημα ασφάλειας, που επιτηρεί κι ελέγχει την εισερχόμενη κι εξερχόμενη κίνηση του δικτύου, βάσει προκαθορισμένων κανόνων ασφάλειας. Το τείχος προστασίας εγκαθιστά ένα τείχος ανάμεσα σε ένα αξιόπιστο εσωτερικό δίκτυο κι ένα αναξιόπιστο εξωτερικό δίκτυο, όπως είναι το διαδίκτυο λόγου χάρη.



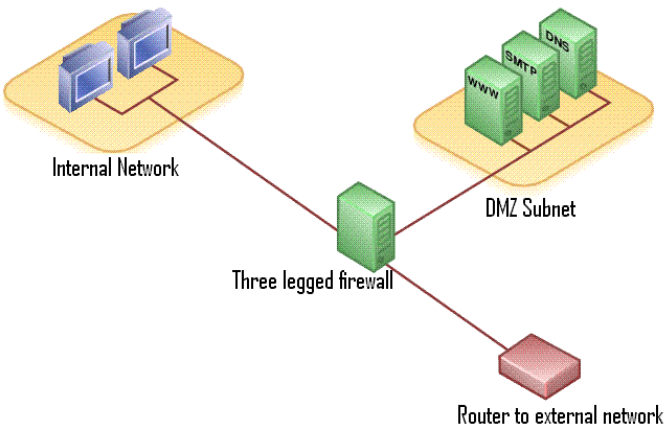
Εικόνα 1.46- Προστασία με Firewall (Πηγή: Wikipedia)

Το Firewall φιλτράρει τα πακέτα που μεταφέρονται ανάμεσα σε υπολογιστές. Όταν ένα πακέτο δεν ταιριάζει στους **κανόνες φιλτραρίσματος** (**filtering rules)**, το firewall απορρίπτει το πακέτο, αλλιώς του επιτρέπει να περάσει. Τα πακέτα μπορούν και να φιλτραριστούν μέσω των διευθύνσεων δικτύου της πηγής και του προορισμού, μέσω του πρωτοκόλλου και μέσω των θυρών της πηγής και του προορισμού.



Εικόνα 1.47- Κανόνες φιλτραρίσματος Firewall (Πηγή: Wikimedia)

DMZ ή demilitarized zone (αποστρατιωτικοποιημένη ζώνη) είναι ένα υποδίκτυο που εμπεριέχει τις υπηρεσίες ενός οργανισμού που βλέπουν προς τα έξω, προς ένα μεγαλύτερο δίκτυο, όπως το διαδίκτυο. Ο σκοπός του DMZ είναι η προσθήκη ενός στρώματος ασφάλειας στο LAN ενός οργανισμού: ένας εξωτερικός κόμβος δικτύου μπορεί να έχει πρόσβαση μόνο σε ότι είναι εκτεθειμένο στο DMZ, ενώ το υπόλοιπο δίκτυο του οργανισμού βρίσκεται πίσω από το τείχος προστασίας.

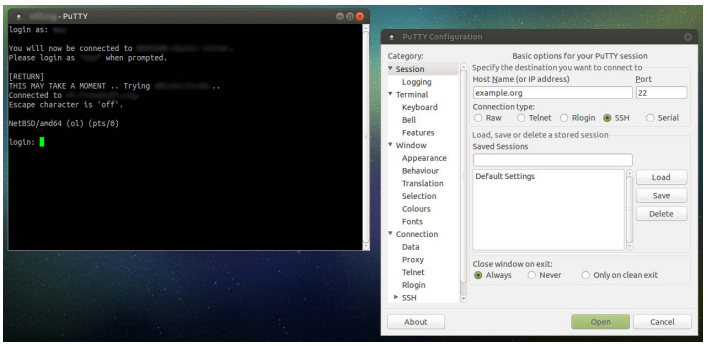


Εικόνα 1.48- DMZ που βασίζεται σε Firewall (Πηγή: Wikimedia)

Η **υπηρεσία απομακρυσμένης πρόσβασης** (**remote access service)** (**RAS**) είναι ο οποιοσδήποτε συνδυασμός hardware και software που επιτρέπει τη σύνδεση ανάμεσα σε έναν πελάτη κι έναν εξυπηρετητή, που είναι γνωστός ως απομακρυσμένος σέρβερ πρόσβασης.

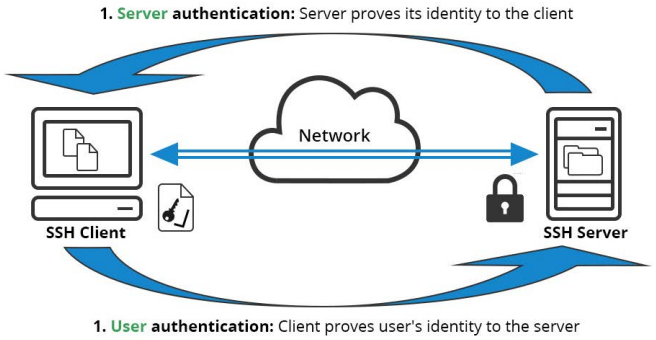
Πολλά γραφεία πληροφοριών κατασκευαστών χρησιμοποιούν αυτή την υπηρεσία **για την τεχνική επίλυση των προβλημάτων των πελατών τους**. Υπάρχουν διαθέσιμες πολλές επαγγελματικές εφαρμογές, εφαρμογές τρίτων, εφαρμογές ανοιχτού κώδικα (open source) και δωρεάν εφαρμογές **απομακρυσμένης επιφάνειας εργασίας** (**remote desktop).**

Το **Telnet και το SSH** (Secure Shell) είναι δύο πρωτόκολλα δικτύου που χρησιμοποιούνται για τη σύνδεση σε **απομακρυσμένους σέρβερ (remote servers)** για να διευκολύνουν την επικοινωνία. Επιτρέπουν στους διαχειριστές του δικτύου να έχουν απομακρυσμένη πρόσβαση σε μια συσκευή και να τη χειριστούν μέσω **εξομοιωτή τερματικού (terminal emulator)**.



Εικόνα 1.50- Απομακρυσμένη πρόσβαση με το putty

Η κεντρική διαφορά ανάμεσα στο Telnet και το SSH είναι ότι το SSH παρέχει μηχανισμούς ασφάλειας (κρυπτογραφεί τα δεδομένα που ανταλλάσσονται χρησιμοποιώντας **κρυπτογράφηση δημοσίου κλειδιού**) που προστατεύουν τους χρήστες εγκαθιστώντας μια ασφαλή σύνδεση ανάμεσα σε δύο απομακρυσμένους εξυπηρετητές μέσω διαδικτύου, ενώ το Telnet δεν έχει μέτρα ασφάλειας, αφού τα δεδομένα ταυτοποίησης (username/password) είναι χωρίς κρυπτογράφηση.



Εικόνα 1.51- Κρυπτογραφημένη σύνδεση με βάση το SSH

Ο όρος **απομακρυσμένη επιφάνεια εργασίας (Remote desktop)** αναφέρεται σε λογισμικό που επιτρέπει στην επιφάνεια εργασίας ενός υπολογιστή να λειτουργήσει απομακρυσμένα, ενώ εμφανίζεται στη συσκευή ενός άλλου πελάτη. Η απομακρυσμένη ανάληψη ελέγχου μιας επιφάνειας εργασίας είναι μια μορφή απομακρυσμένης διαχείρισης.

Εικόνα 1.52- Έλεγχος απομακρυσμένης επιφάνειας (Πηγή: http://www.itarian.com)

Το πρωτόκολλο απομακρυσμένης επιφάνειας εργασίας (Remote Desktop Protocol) (**RDP**) είναι ένα ιδιωτικό πρωτόκολλο που αναπτύχθηκε από τη Microsoft, που δίνει στον χρήστη ένα γραφικό περιβάλλον για να συνδεθεί σε έναν άλλον υπολογιστή μέσω μιας σύνδεσης δικτύου. Ο χρήστης χρησιμοποιεί λογισμικό RDP client (είναι ενσωματωμένο σε πολλά λειτουργικά συστήματα) γι' αυτό τον σκοπό, ενώ ο άλλος υπολογιστής πρέπει να τρέξει λογισμικό RDP server (είναι ενσωματωμένο μόνο σε λειτουργικό σύστημα Windows).

Η Microsoft αναφέρεται στο επίσημο λογισμικό της RDP client ως Remote Desktop Connection, ενώ παλαιότερα λεγόταν "Terminal Services Client".

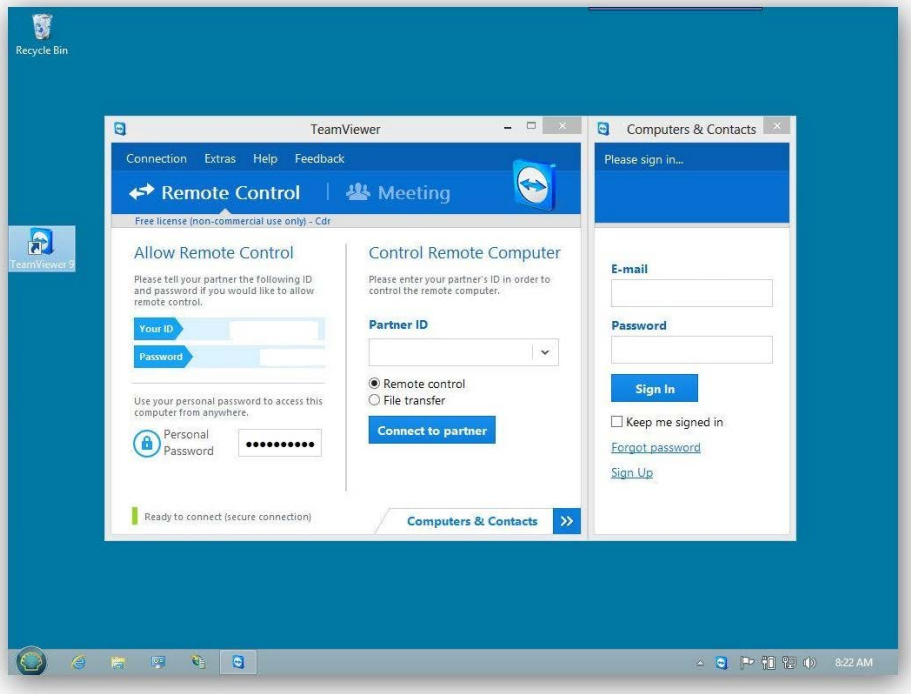
Λογισμικό RDP που δεν είναι ενημερωμένο στην τελευταία έκδοση είναι αυτές τις μέρες ένα από τα κύρια σημεία εισόδου για **ransomware**. Είναι πολύ σημαντικό να κρατάμε ενημερωμένα τα Windows για ν' αποφύγουμε τέτοιες επιθέσεις. Υπάρχουν μερικές επιλογές για να το ασφαλίσουμε. Follow the link for further information

Η χρήση εικονικού δικτύου (Virtual Network Computing) (**VNC**) είναι ένα γραφικό σύστημα ανοιχτού κώδικα για την κοινοχρησία της επιφάνειας εργασίας, που χρησιμοποιεί το πρωτόκολλο Remote Framebuffer (RFB) για τον απομακρυσμένο έλεγχο ενός άλλου υπολογιστή. Μεταδίδει μέσω δικτύου τη χρήση πληκτρολογίου και ποντικιού από έναν υπολογιστή σε έναν άλλο, και μεταφέρει τις ενημερώσεις του γραφικού περιβάλλοντος πίσω προς την άλλη κατεύθυνση.

Μπορούν να συνδεθούν ταυτόχρονα πολλοί πελάτες σε έναν σέρβερ VNC. Δημοφιλείς χρήσεις αυτής της τεχνολογίας συμπεριλαμβάνουν την απομακρυσμένη τεχνική υποστήριξη και την πρόσβαση στα αρχεία του υπολογιστή μας στο γραφείο από το σπίτι μας, ή και το ανάποδο.

Εικόνα 1.53- Παράθυρο εισαγωγής στοιχείων ταυτοποίησης για απομακρυσμένη επιφάνεια εργασίας (Πηγή: flickr VNC)

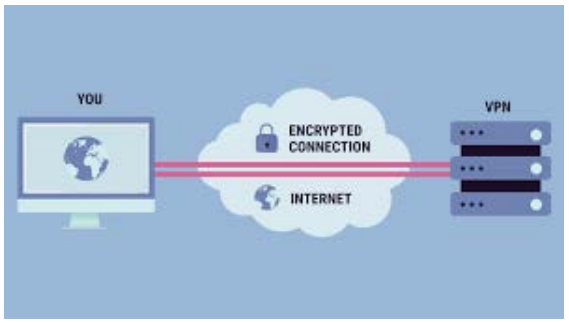
Το TeamViewer είναι ιδιωτικό λογισμικό για απομακρυσμένο έλεγχο, για κοινοχρησία της επιφάνειας εργασίας, για online συναντήσεις, για συσκέψεις μέσω web και για τη μεταφορά αρχείων ανάμεσα σε υπολογιστές. Όταν εγκατασταθεί σε έναν υπολογιστή, επιτρέπει την απομακρυσμένη σύνδεση χρηστών με την ανάλογη άδεια.



Εικόνα 1.54- Αρχική οθόνη σύνδεσης και ρύθμισης teamviewer

Ένα **εικονικό ιδιωτικό δίκτυο** (**virtual private network)** (**VPN**) επεκτείνει ένα ιδιωτικό δίκτυο σε ένα δημόσιο δίκτυο κι επιτρέπει στους χρήστες να στείλουν και να λάβουν δεδομένα σε κοινόχρηστα ή δημόσια δίκτυα, λες κι οι συσκευές τους ήταν απευθείας συνδεδεμένες στο ιδιωτικό δίκτυο.

Για να διασφαλιστεί η ασφάλεια, η σύνδεση του ιδιωτικού δικτύου γίνεται μέσω της χρήσης ενός κρυπτογραφημένου πρωτοκόλλου σήραγγας με επίπεδα κι οι χρήστες του VPN χρησιμοποιούν μεθόδους ταυτοποίησης, όπως κωδικούς ή πιστοποιητικά.



Εικόνα 1.55- VPN connection (Πηγή: http://hardzone.es)

1.3 Πρωτόκολλα Βιομηχανικού Δικτύου

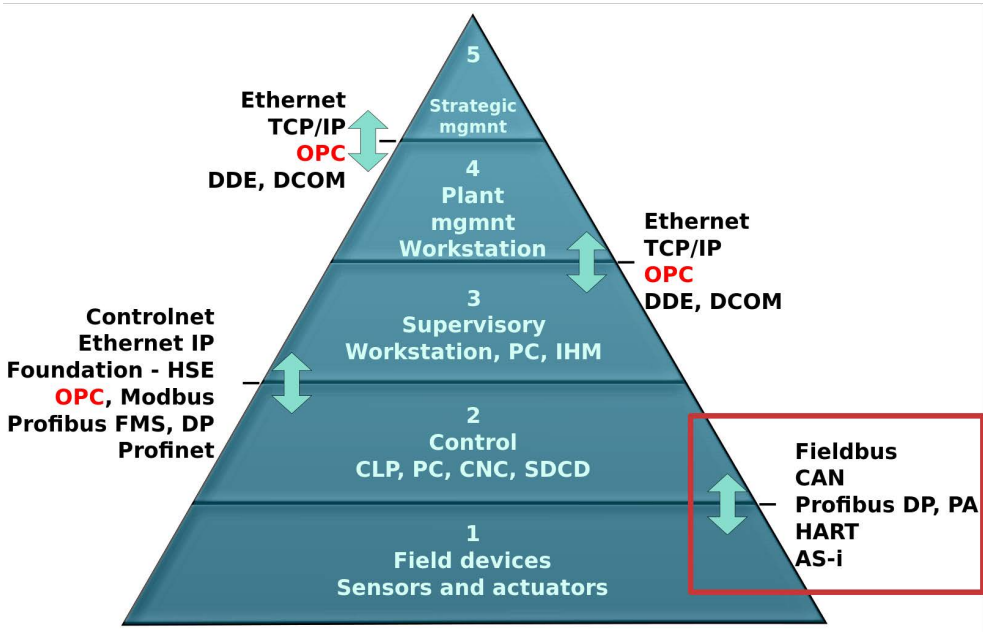
Description

1.3 Πρωτόκολλα Βιομηχανικού Δικτύου

Table of contents

Fieldbus είναι το όνομα μιας οικογένειας βιομηχανικών πρωτοκόλλων δικτύου, που χρησιμοποιούνται για κατανεμημένο έλεγχο σε ζωντανό χρόνο.

Σε ένα βιομηχανικό σύστημα ελέγχου συνήθως υπάρχει μια Διεπαφή Ανθρώπου Μηχανής (Human Machine Interface) (HMI) στην κορυφή της ιεραρχίας, που συνδέεται στο μεσαίο επίπεδο των προγραμματιζόμενων λογικών ελεγκτών (PLC) μέσω ενός συστήματος επικοινωνίας χωρίς χρονικούς περιορισμούς (όπως το Ethernet π.χ.). Στη βάση του συστήματος ελέγχου είναι το fieldbus, που συνδέει τα PLCs (Επίπεδο 1) με τα εξαρτήματα που κάνουν τη δουλειά (Επίπεδο 0), όπως αισθητήρες, ενεργοποιητές, ηλεκτρικά μοτέρ, φώτα κονσόλας, διακόπτες, βαλβίδες και επαφείς (contactors).



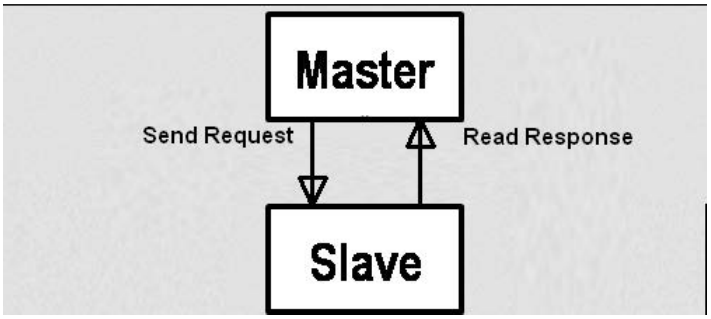
Εικόνα 1.56- Διάταξη επιπέδων Fieldbus (Πηγή: Wikimedia)

Το Fieldbus είναι ένα βιομηχανικό σύστημα δικτύου για κατανεμημένο έλεγχο σε **ζωντανό χρόνο** και είναι αντίστοιχο με τις συνδέσεις τύπου LAN, που απαιτούν μόνο ένα σημείο επικοινωνίας στο επίπεδο του ελεγκτή κι επιτρέπουν την ταυτόχρονη σύνδεση πολλαπλών συσκευών.

Το Modbus είναι ένα σειριακό (συνήθως τύπου RS-232 ή RS-485) πρωτόκολλο επικοινωνίας, που χρησιμοποιείται για την επικοινωνία με τα PLCs. Έχει γίνει πρότυπο πρωτόκολλο επικοινωνίας και αποτελεί πια ένα κοινό μέσο σύνδεσης ηλεκτρονικών βιομηχανικών συσκευών για τους ακόλουθους λόγους:

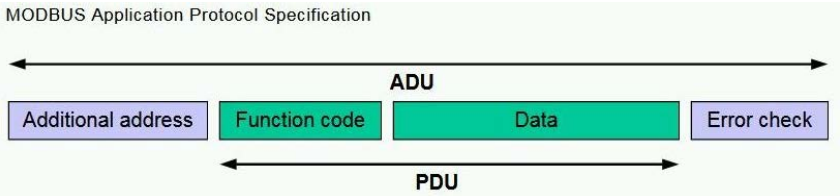
- Έχει δημοσιευθεί ανοιχτά και δεν απαιτεί καταβολή δικαιωμάτων πνευματικής ιδιοκτησίας.
- Μεταφέρει ανεπεξέργαστα bits ή λέξεις χωρίς να θέσει πολλούς περιορισμούς στους παρόχους.

Το Modbus χρησιμοποιείται συχνά για τη σύνδεση ενός υπολογιστή επιτήρησης (**master**) με ένα απομακρυσμένο RTU (**slave**) σε συστήματα SCADA. Χαρακτηρίζεται σαν πρωτόκολλο master/slave (εικόνα 1.57), δηλαδή η συσκευή που λειτουργεί σαν master θα ρωτήσει μία ή περισσότερες συσκευές που λειτουργούν σαν slave. Άρα η συσκευή slave δεν μπορεί να προσφέρει πληροφορίες εθελοντικά. Πρέπει να περιμένει να της ζητηθούν. Η συσκευή master θα γράψει δεδομένα στους καταχωρητές (registers) μιας συσκευής slave και θα διαβάσει δεδομένα πάλι από τους ίδιους καταχωρητές.



Εικόνα 1.57- Διαδικασίας επικοινωνίας Master Slave

Κάθε ανταλλαγή δεδομένων αποτελείται από ένα αίτημα από τον master κι ακολουθείται από την απάντηση του slave. Όπως φαίνεται στην εικόνα 1.58, κάθε πακέτο δεδομένων, είτε αυτό είναι αίτημα είτε απάντηση, ξεκινά με τη διεύθυνση συσκευής ή slave address, ενώ μετά ακολουθείται από τον κώδικα λειτουργίας και τις παραμέτρους που καθορίζουν τι ακριβώς ζητιέται ή παρέχεται. Η ακριβής μορφολογία του αιτήματος και της απάντησης παρουσιάζεται αναλυτικά στις προδιαγραφές του πρωτοκόλλου Modbus.

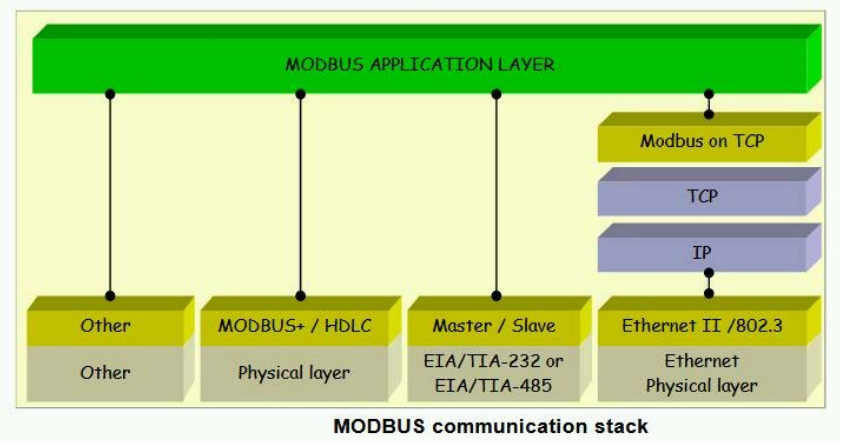


Εικόνα 1.58- Δομή πακέτου δεδομένων Modbus (Πηγή: Modbus Organization)

Όπως δείχνει η εικόνα 1.59, το πρωτόκολλο **Modbus TCP** ενθυλακώνει τα δεδομένα αιτημάτων κι απαντήσεων του Modbus RTU σε ένα πακέτο TCP, που μεταδίδεται μέσω κλασικών δικτύων Ethernet. Η πιο σημαντική διεύθυνση εδώ είναι η διεύθυνση IP. Η κλασική θύρα του Modbus TCP είναι η 502, αλλά ο αριθμός θύρας μπορεί και ν' αλλάξει αν αυτό είναι επιθυμητό.

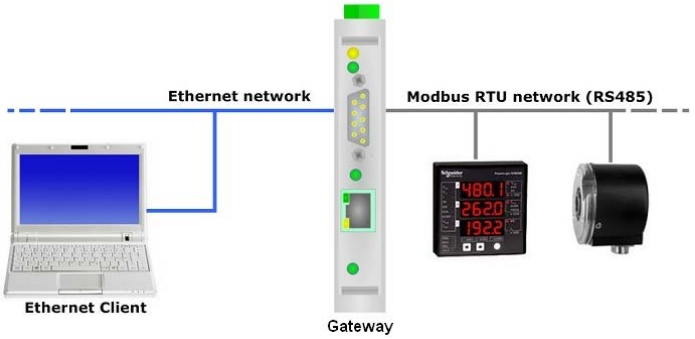
Το άθροισμα ελέγχου (checksum) κι η διαχείριση σφαλμάτων (error handling) αναλαμβάνονται από το Ethernet στην περίπτωση του Modbus TCP.

Η TCP έκδοση του Modbus ακολουθεί το μοντέλο αναφοράς OSI. Το Modbus TCP καθορίζει τα επίπεδα παρουσίασης και εφαρμογών του μοντέλου OSI.



Εικόνα 1.59- Στοίβα πρωτοκόλλου Modbus (Πηγή: Modbus Organization)

Το Modbus TCP τρέχει στο Ethernet (επίπεδο ζεύξης δεδομένων και φυσικό επίπεδο) και το Modbus RTU είναι ένα πρωτόκολλο σειριακού επιπέδου (φυσικό επίπεδο). Για να επικοινωνήσουν τα δύο δίκτυα απαιτείται η ύπαρξη μιας **πύλης δικτύου** (**gateway)** (εικόνα 1.60) για τη μετατροπή του ενός πρωτοκόλλου στο άλλο, μέσω της προσθήκης ή της αφαίρεσης μιας κεφαλίδας των 6-byte, που επιτρέπει τη δρομολόγηση στο Modbus TCP.



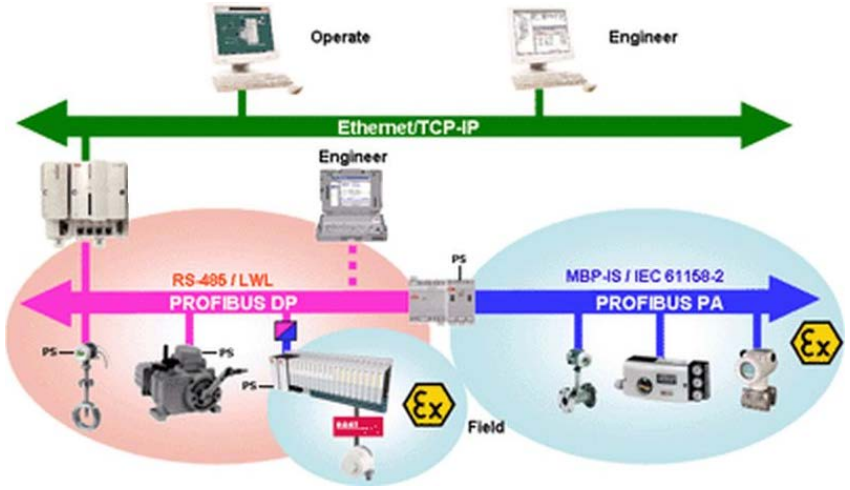
Εικόνα 1.60 – Πύλη δικτύου για την επικοινωνία ανάμεσα σε TCP-RTU

Το Modbus TCP είναι το κοινό πρωτόκολλο που συνδέει τις υπόλοιπες επιλογές Modbus μέσω πυλών δικτύου.

Το Profibus (Process Field Bus) είναι ένα πρότυπο για την επικοινωνία του fieldbus στην αυτοματοποιημένη τεχνολογία. Μην το μπερδέψετε με το πρότυπο Profinet για το βιομηχανικό Ethernet.

Σήμερα χρησιμοποιούνται δύο εκδοχές του Profibus (εικόνα 1.62). Η πιο κοινή είναι το Profibus DP:

- **Το PROFIBUS DP** (Decentralised Peripherals) (αποκεντρωμένα περιφερειακά) χρησιμοποιείται για τη λειτουργία αισθητήρων κι ενεργοποιητών μέσω ενός κεντρικού ελεγκτή σε ένα αυτοματοποιημένο σύστημα παραγωγής.
- **Το PROFIBUS PA** (Process Automation) (αυτοματοποίηση διεργασιών) χρησιμοποιείται για την παρακολούθηση οργάνων μέτρησης σε εφαρμογές αυτοματοποίησης διεργασιών. Αυτή η εκδοχή είναι σχεδιασμένη για χρήση σε επικίνδυνες περιοχές με κίνδυνο έκρηξης (Ex-zone 0 και 1). Το Φυσικό Επίπεδο ακολουθεί το IEC 61158-2, που επιτρέπει την παροχή ενέργειας στα όργανα μέσω διαύλου, ενώ παράλληλα περιορίζει τη ροή του ρεύματος για να μη δημιουργηθούν εκρηκτικές συνθήκες, ακόμα κι αν προκύψει κάποια βλάβη.



Εικόνα 1.62- Profibus DP/PA

Το Profibus αναπτύχθηκε στα επίπεδα 1, 2 και 7 του OSI (εικόνα 1.63):

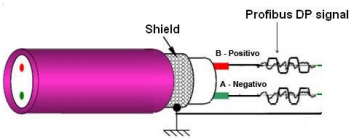
OSI-Layer		PROFIBUS		
7	Application	DPV0	DPV1	DPV2
6	Presentation	--		
5	Session			
4	Transport			
3	Network			
2	Data Link	FDL		
1	Physical	EIA-485	Optical	MBP

Εικόνα 1.63- Μοντέλο OSI – Σύγκριση επιπέδων Profibus

Επίπεδο 1:

Διευκρινίζονται τρεις μέθοδοι για το επίπεδο μετάδοσης bit:

- Στην ηλεκτρική μετάδοση, που γίνεται σύμφωνα με το EIA-485, μπορούν να χρησιμοποιηθούν bit rates από 9.6 kbit/s μέχρι και 12 Mbit/s. Το μήκος καλωδίου ανάμεσα σε δύο αναμεταδότες περιορίζεται από τα 100 μέχρι και τα 1200 μέτρα, ανάλογα με τον ρυθμό μετάδοσης που χρησιμοποιείται. Αυτή η μέθοδος μετάδοσης χρησιμοποιείται κυρίως με το PROFIBUS DP.



Εικόνα 1.64- Καλώδιο RS-485 του Profibus

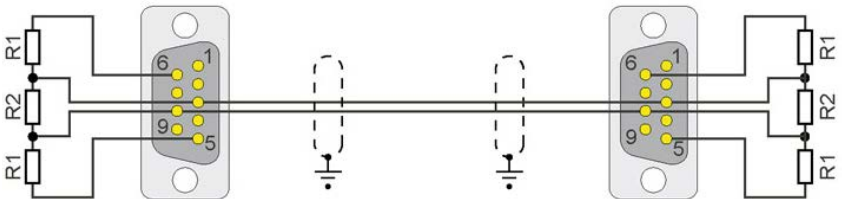
- Στην οπτική μετάδοση, που γίνεται μέσω οπτικών ινών, χρησιμοποιούνται τοπολογίες αστεριού, διαύλου και δακτυλίου. Η απόσταση

ανάμεσα στους αναμεταδότες φτάνει μέχρι και τα 15 χιλιόμετρα. Απαιτούνται μετατροπείς οπτικής ίνας σε RS485 (εικόνα 1.65).

Εικόνα 1.65- Μετατροπέας οπτικής ίνας σε RS485

- Με την τεχνολογία μετάδοσης MBP (Manchester Bus Powered), τα δεδομένα και το ρεύμα περνάνε από το ίδιο καλώδιο. Αυτή η τεχνολογία χρησιμοποιείται στο Profibus PA.

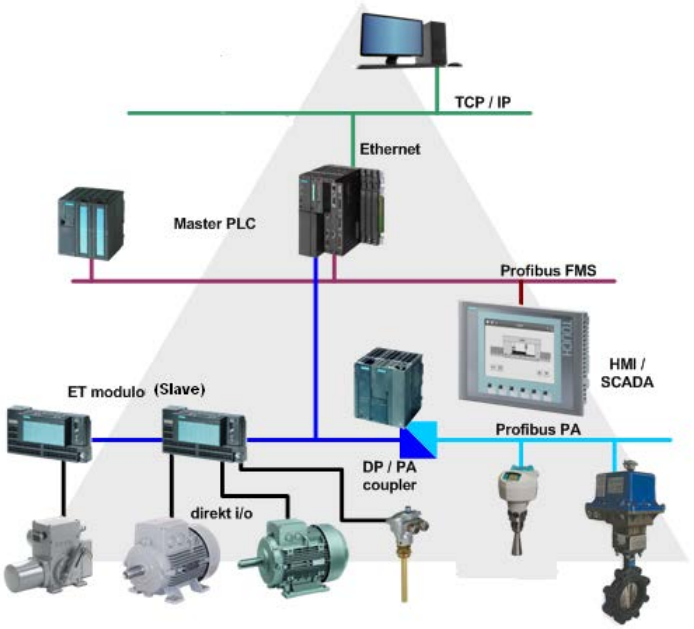
Στα δίκτυα Profibus συνήθως χρησιμοποιούνται βύσματα τύπου Sub-D με 9 pins.



Εικόνα 1.67- Βύσμα RS485 τύπου D με 9 pins για Profibus (Πηγή: Wikimedia)

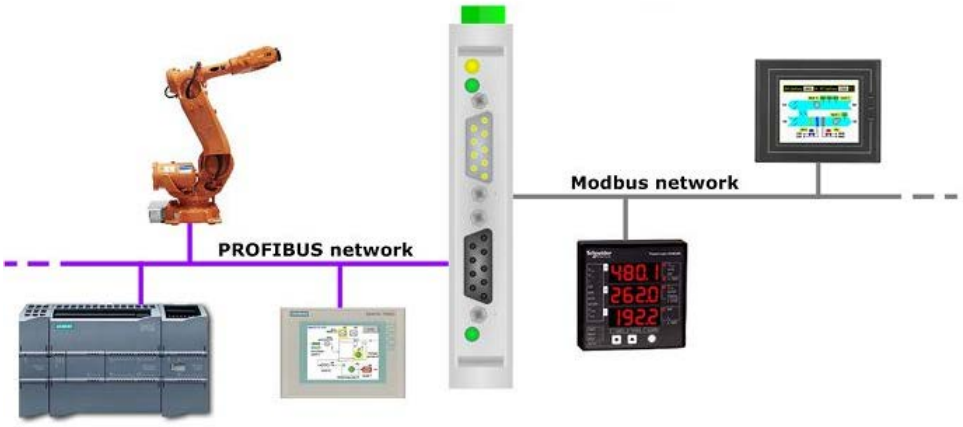
Επίπεδο 2:

Το επίπεδο ζεύξης δεδομένων λέγεται **FDL** (Field bus Data Link) και λειτουργεί με υβριδική μέθοδο πρόσβασης, που συνδυάζει αδειοδοτικό (token) με τη μέθοδο master-slave. Σε ένα δίκτυο PROFIBUS DP, οι ελεγκτές ή τα συστήματα ελέγχου διεργασιών είναι οι **masters** κι οι αισθητήρες κι οι ενεργοποιητές είναι οι **slaves** (εικόνα 1.68).



Εικόνα 1.68- Αρχιτεκτονική master-slave στο Profibus (Πηγή: Wikimedia)

Το Profibus μπορεί να συνδεθεί σε άλλα δίκτυα fieldbus χρησιμοποιώντας την απαιτούμενη πύλη δικτύου (εικόνα 1.69).

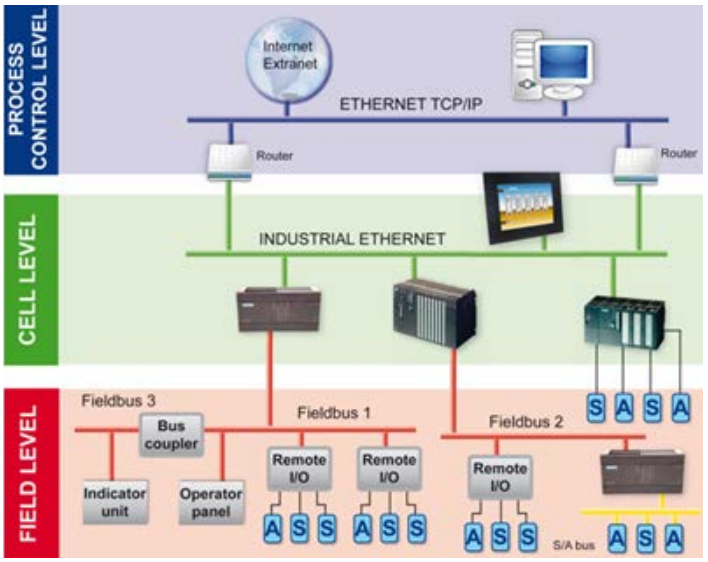


Εικόνα 1.69- Διασύνδεση Profibus και Modbus μέσω πύλης δικτύου

Σήμερα χρησιμοποιούνται δύο εκδοχές του Profibus (εικόνα 1.62). Η πιο κοινή είναι το Profibus DP:

Το Βιομηχανικό Ethernet χρησιμοποιεί τα πρότυπα που αναπτύχθηκαν για το Ethernet και τα ενσωματώνει για την επικοινωνία του κατασκευαστικού δικτύου (εικόνα 1.70). Με την τροποποίηση του επιπέδου ζεύξης δεδομένων (Media Access Control) το Βιομηχανικό Ethernet προσφέρει **ντετερμινισμό** (**determinism)** και **έλεγχο σε ζωντανό χρόνο** (low latency), που μπορεί να μην είναι κρίσιμα σε ένα περιβάλλον IT (Information Technology) (πληροφορικής), αλλά είναι απαραίτητα στο λειτουργικό κομμάτι (Operation Technology) (βιομηχανική αυτοματοποίηση).

Επιπροσθέτως, πρέπει να προσφέρει **διαλειτουργικότητα** στα υψηλότερα επίπεδα του μοντέλου OSI, καθώς και **ασφάλεια** απέναντι στις εισβολές που γίνονται έξω από το εργοστάσιο, αλλά και στη μη εξουσιοδοτημένη χρήση μέσα σε αυτό.



Εικόνα 1.70 Αρχιτεκτονική βιομηχανικού δικτύου Ethernet (Πηγή: Industrial Ethernet Book)

Ο βιομηχανικός εξοπλισμός Ethernet σχεδιάζεται για **σκληρά περιβάλλοντα**, οπότε χρειάζεται ειδικές δυνατότητες, όπως ανθεκτικά βύσματα και switches υψηλών θερμοκρασιών, όπως απαιτούνται σε ένα βιομηχανικό περιβάλλον. Τα εξαρτήματα που χρησιμοποιούνται στα σημεία επεξεργασίας του εργοστασίου πρέπει να σχεδιαστούν για να λειτουργήσουν σε ακραίες θερμοκρασίες, με υγρασία και δονήσεις που ξεπερνούν το εύρος του εξοπλισμού IT.

Η χρήση Ethernet οπτικών ινών (θύρες **SFP**) ελαττώνει τα προβλήματα του ηλεκτρικού θορύβου και προσφέρει ηλεκτρική απομόνωση.

Εικόνα 1.71- Switch βιομηχανικού Ethernet (Πηγή: Wikipedia)

Το Profinet είναι το ανοιχτό πρότυπο βιομηχανικού Ethernet του διεθνή οργανισμού Profibus, και ένα από τα πιο κοινά πρότυπα επικοινωνίας στα δίκτυα αυτοματοποίησης.

Το Profinet επιτρέπει τη συμβατότητα στις επικοινωνίες μέσω Ethernet (που συνηθίζονται στα περιβάλλοντα IT), αλλά πρέπει να έχουμε υπόψη τη διαφορά ταχύτητας στην επικοινωνία μέσω Ethernet ενός εταιρικού δικτύου με την απόδοση σε ζωντανό χρόνο που απαιτείται σε ένα βιομηχανικό δίκτυο.

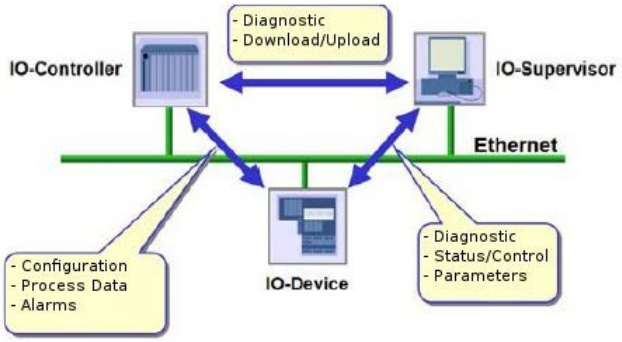
Η χρήση του Profinet προσφέρει τα ακόλουθα πλεονεκτήματα:

- Βελτιώνει τη δυνατότητα επέκτασης στις υποδομές.
- Διευκολύνει την πρόσβαση στις συσκευές από άλλα δίκτυα.
- Οι εργασίες συντήρησης μπορούν να γίνουν απ' οπουδήποτε μέσω ασφαλών συνδέσεων (VPN) για απομακρυσμένη συντήρηση.

Το πρωτόκολλο PROFINET αποτελείται από τρεις συσκευές (εικόνα 1.72).

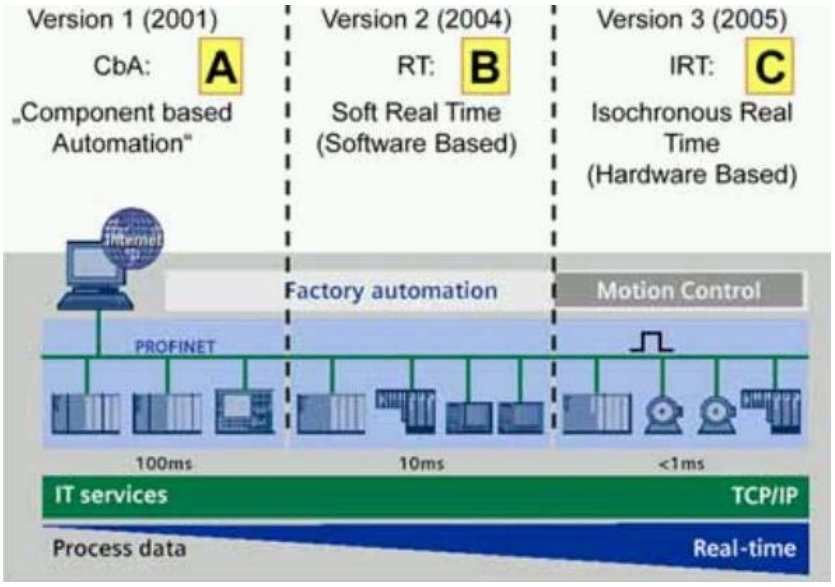
- **Ελεγκτής IO (IO Controller)**: Master, εκεί που εκτελείται το πρόγραμμα ελέγχου.
- **Συσκευή IO (IO Device)**: Απομακρυσμένη συσκευή που διατηρεί επικοινωνία με έναν ελεγκτή
- **Επιτηρητής IO (IO Supervisor)**: προγραμματιζόμενη συσκευή γραφικών, όπου πραγματοποιείται η ανάλυση δικτύου.

Δεν υπάρχει ιεραρχία ανάμεσα σε αυτές τις συσκευές, οπότε κάθε IO έχει την ίδια σημασία σε ένα δίκτυο PROFINET.



Εικόνα 1.72- Τύποι συσκευών Profinet (Πηγή: www.semanticscholar.org)

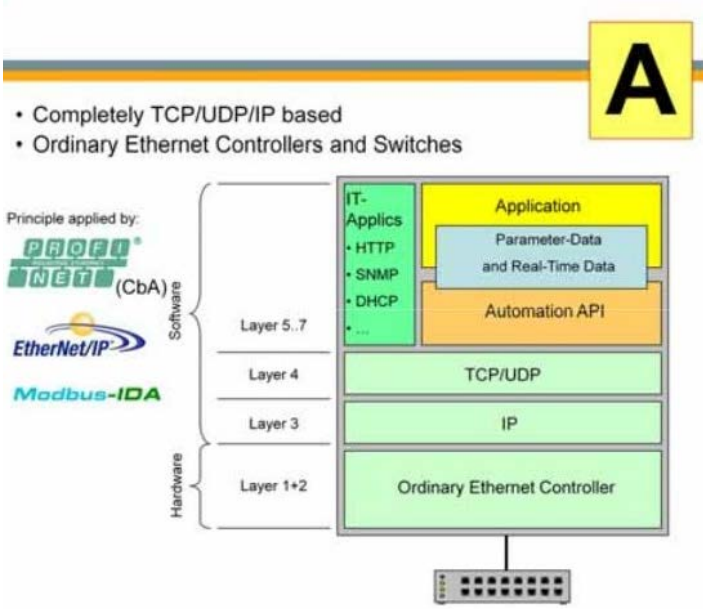
Το Profinet ενσωματώνει διαφορετικά **προφίλ,** αφού ερμηνεύει με συγκεκριμένο τρόπο την κάθε περίπτωση μετάδοσης δεδομένων, οπότε και τροποποιεί το 7^{ο} επίπεδο του OSI (εφαρμογών). Υπάρχουν τρεις εκδόσεις του Profinet:



Εικόνα 1.73- Προφίλ του Profinet (Πηγή: www.semanticscholar.org)

- Έκδοση 1 (Class A): **Αυτοματοποίηση βάσει εξαρτημάτων (Component Based Automation) (CBA)**

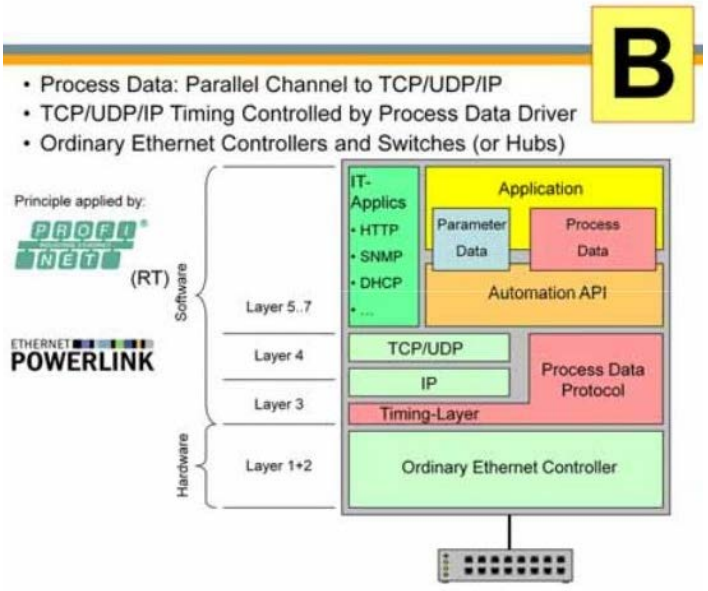
Έχει τυπικό χρονικό κύκλο 100ms και χρησιμοποιείται για παραμετροποίηση, κι όχι για τη μεταφορά δεδομένων επεξεργασίας. Δεν υποστηρίζεται πια από το Profibus.



Εικόνα 1.74- Αρχιτεκτονική CBA του Profinet (Πηγή: www.ethercat.org)

- Έκδοση 2 (Class B): **Πραγματικού χρόνου (Real-Time) (RT)**

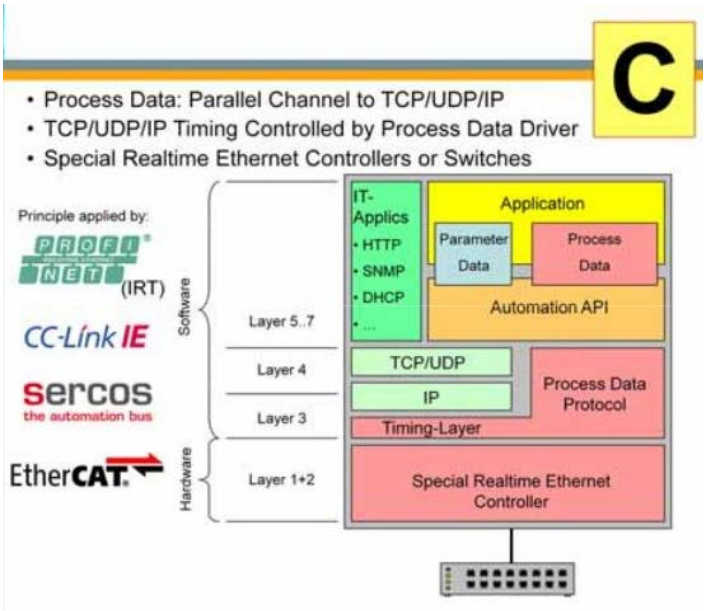
Έχει τυπικό χρονικό κύκλο 10ms, παρόμοιο με του Profibus, και χρησιμοποιείται για τη μετάδοση δεδομένων επεξεργασίας.



Εικόνα 1.75- Αρχιτεκτονική RT του Profinet (Πηγή: www.ethercat.org)

- Έκδοση 3 (Class C) : **Ισόχρονου Πραγματικού χρόνου (Isochronous Real Time) (IRT)**

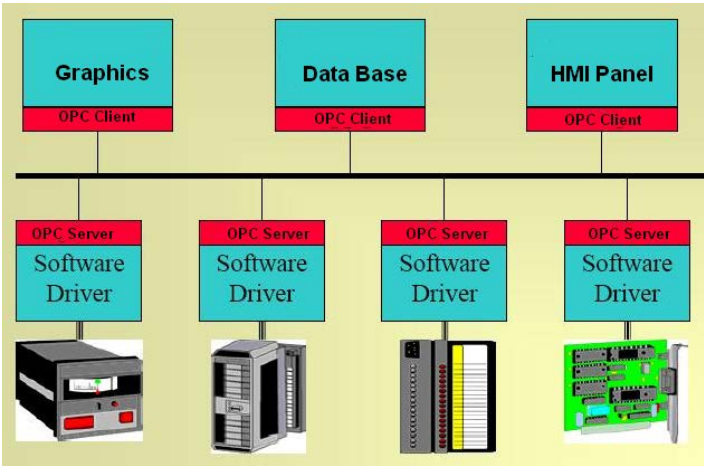
Έχει τυπικό χρονικό κύκλο 1 ms. Η διαφορά με την επικοινωνία ζωντανού χρόνου είναι ο υψηλός βαθμός ντετερμινισμού, οπότε και διατηρείται με υψηλή ακρίβεια η αρχή του δικτυακού κύκλου.



Εικόνα 1.76- Αρχιτεκτονική IRT του Profinet (Πηγή: www.ethercat.org)

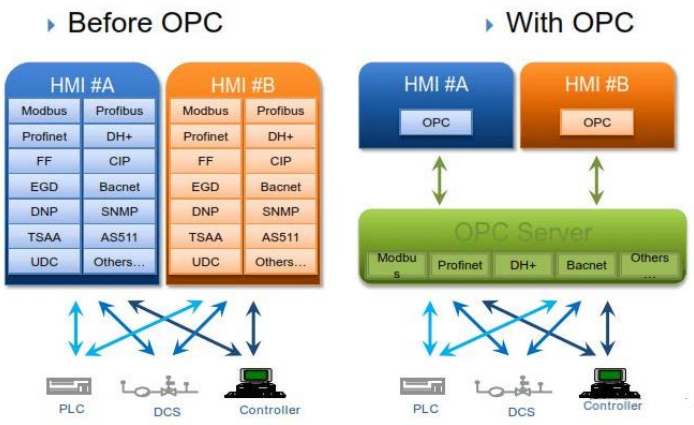
Το OPC (Open Platform Communications) (ανοιχτή πλατφόρμα επικοινωνιών) είναι πρότυπο διαλειτουργικότητας για την ασφαλή κι αξιόπιστη ανταλλαγή δεδομένων στη βιομηχανική αυτοματοποίηση. Είναι ανεξάρτητο από πλατφόρμες και διασφαλίζει την απρόσκοπτη ροή πληροφοριών ανάμεσα σε συσκευές από πολλαπλούς προμηθευτές.

Αυτές οι προδιαγραφές καθορίζουν τη διασύνδεση ανάμεσα σε **clients και servers**, καθώς και των servers σε servers, συμπεριλαμβάνοντας την πρόσβαση σε δεδομένα ζωντανού χρόνου, την παρακολούθηση συναγερμών και συμβάντων, την πρόσβαση σε δεδομένα ιστορικού κι άλλες εφαρμογές.



Εικόνα 1.77- Αρχιτεκτονική server/client του OPC (Πηγή: Wikipedia)

Το OPC σχεδιάστηκε για να παρέχει **κοινή γέφυρα** στις διάφορες εφαρμογές και στον εξοπλισμό ελέγχου διεργασιών, για την πρόσβαση στα δεδομένα των συσκευών που βρίσκονται στο πεδίο (εικόνα 1.78).



Εικόνα 1.78- Αρχιτεκτονική OPC (Πηγή: www.theautomization.com)

Ένας server OPC για μια συσκευή hardware προσφέρει τις ίδιες μεθόδους πρόσβασης στα δεδομένα του όπως κι ένας OPC Client. Όταν ένας κατασκευαστής hardware είχε αναπτύξει τον **OPC Server** του για τη νέα συσκευή, η δουλειά του είχε τελειώσει κι επέτρεπε 'top end' πρόσβαση στη συσκευή του. Όταν ένας παραγωγός SCADA είχε αναπτύξει τον δικό του **OPC Client,** η δουλειά του είχε τελειώσει κι επέτρεπε την πρόσβαση σε κάθε κομμάτι hardware ενός server συμβατού με το OPC.

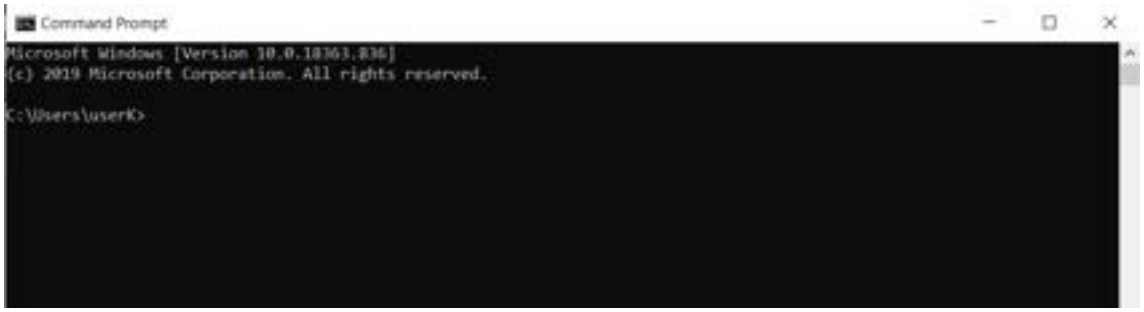
Η **ενοποιημένη αρχιτεκτονική (Unified Architecture) (UA**) του OPC είναι μια αρχιτεκτονική ανεξάρτητη από πλατφόρμες και με προσανατολισμό προς τις υπηρεσίες, που ενσωματώνει όλη τη λειτουργικότητα των μεμονωμένων προδιαγραφών του OPC Classic σε ένα επεκτάσιμο πλαίσιο.

Πρωτοποριακές τεχνολογίες και μεθοδολογίες, όπως νέα πρωτόκολλα μεταφορών, αλγόριθμοι ασφάλειας, πρότυπα κωδικοποίησης ή υπηρεσίες εφαρμογών, μπορούν να ενσωματωθούν στο OPC UA διατηρώντας την προς τα πίσω συμβατότητα.

Εργασία 1. Ρυθμίσεις υπολογιστή

Σε αυτήν την πρώτη εργασία θα μάθετε πώς να ρυθμίζετε το δίκτυο του υπολογιστή σας.

Ανοίξτε ένα παράθυρο διεπαφής εντολών (Εκκίνηση > cmd). Ισοδύναμα μπορεί να γίνει πατώντας το κουμπί Windows + R και γράφοντας cmd. 'Επειτα θα ανοίξει το ακόλουθο παράθυρο:



Θυμηθείτε πώς το ανοίξατε, γιατί μπορεί να το χρειαστείτε αργότερα.

Πληκτρολογήστε "ipconfig" (χωρίς εισαγωγικά) και πατήστε το κουμπί Enter. Η εντολή θα επιστρέψει τις ρυθμίσεις του δικτύου του υπολογιστή σας. Συμπληρώστε τον παρακάτω πίνακα με τις απαντήσεις που βλέπετε:

Διεύθυνση IP / IP address	
Μάσκα υποδικτύου / Subnet mask	
Προεπιλεγμένη πύλη (δρομολογητής) / Default Gateway (router)	

Πληκτρολογήστε "ipconfig /?" για να δείτε περισσότερες επιλογές αυτής της εντολής.

Πληκτρολογήστε "ipconfig /all" και θα σας επιστρέψει τις ρυθμίσεις για προχωρημένους. Αυτές οι πληροφορίες είναι επίσης ορατές με την εκκίνηση του winipcfg (Home / launch / winipcfg). Συμπληρώστε τον παρακάτω πίνακα.

Ρυθμίσεις IP των Windows / Windows IP settings	
Όνομα κεντρικού υπολογιστή / Host name	
Κύριο DNS / Main DNS suffix	
Ενεργοποίηση δρομολόγησης / Enabled routing	
Προσαρμογέας Ethernet / Ethernet adapter	
Φυσική Διεύθυνση / Physical address	
Ενεργοποίηση DHCP / Enabled DHCP	

Συμπληρώστε τον πίνακα με τα δεδομένα των συναδέλφων σας που βρίσκονται αριστερά και δεξιά σας (αν είστε τελευταίος στη σειρά, ρωτήστε έναν άλλο συνάδελφο). Συγκρίνετε όμοιες και διαφορετικές τιμές.

Συνάδελφος στα αριστερά

Ρυθμίσεις IP των Windows / Windows IP settings	
Όνομα κεντρικού υπολογιστή / Host name	
Κύριο DNS / Main DNS suffix	

Ενεργοποίηση δρομολόγησης / Enabled routing	
Προσαρμογέας Ethernet / Ethernet adapter	
Φυσική Διεύθυνση / Physical address	
Ενεργοποίηση DHCP / Enabled DHCP	
Διεύθυνση IP / IP address	
Μάσκα υποδικτύου / Subnet mask	
Προεπιλεγμένη πύλη (δρομολογητής) / Default Gateway (router)	
Διακομιστής DNS / DNS server	

Συνάδελφος στα δεξιά

Ρυθμίσεις IP των Windows / Windows IP settings	
Όνομα κεντρικού υπολογιστή / Host name	
Κύριο DNS / Main DNS suffix	
Ενεργοποίηση δρομολόγησης / Enabled routing	
Προσαρμογέας Ethernet / Ethernet adapter	
Φυσική Διεύθυνση / Physical address	
Ενεργοποίηση DHCP / Enabled DHCP	
Διεύθυνση IP / IP address	
Μάσκα υποδικτύου / Subnet mask	
Προεπιλεγμένη πύλη (δρομολογητής) / Default Gateway (router)	
Διακομιστής DNS / DNS server	

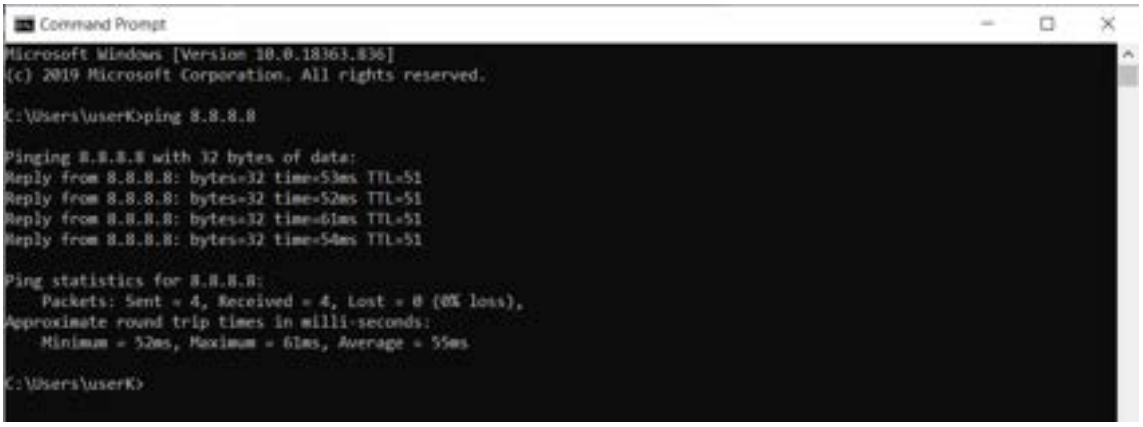
Εργασία 2. Διεύθυνση IP

Στο Internet, οι υπολογιστές αναγνωρίζονται από τη διεύθυνση IP τους (Internet Protocol). Η διεύθυνση IP αποτελείται από 4 αριθμούς, χωρισμένοι με 3 κουκίδες. Κάθε ένας από τους 4 αριθμούς έχει τιμή μεταξύ 0 και 255 (δηλ. 192.168.2.3 ή 158.42.4.2).

Υπάρχει επίσης ένας άλλος τύπος αναγνώρισης, χρησιμοποιώντας ονόματα τομέα (π.χ. www.google.com). Χάρη στο πρωτόκολλο DNS, ο υπολογιστής γνωρίζει ποια διεύθυνση IP ταιριάζει με αυτό το όνομα, στην περίπτωση αυτή η διεύθυνση με IP 216.58.201.164 .

Ανοίξτε ένα παράθυρο διεπαφής εντολών (Εκκίνηση> cmd). 'Επειτα θα ανοίξει το ακόλουθο παράθυρο :

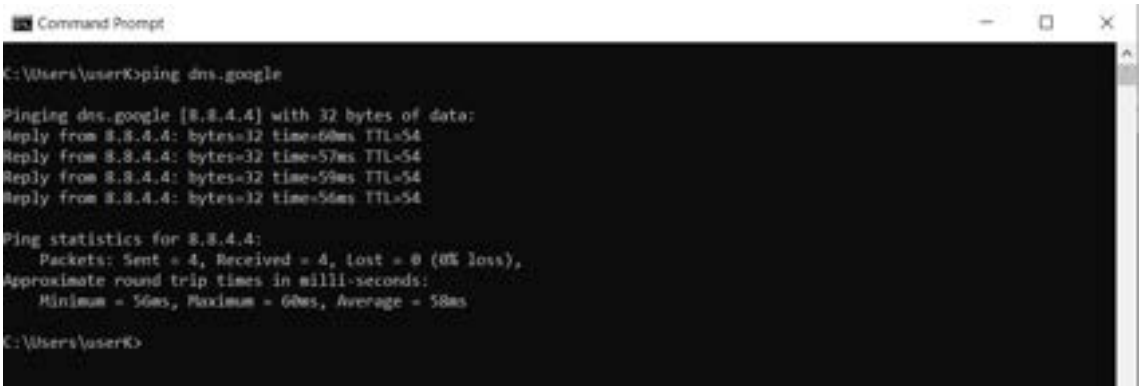
Εκτελέστε την εντολή "ping 8.8.8.8" και δείτε αν το αποτέλεσμα είναι παρόμοιο με αυτό:



Η παράμετρος "Time" δείχνει το χρονικό διάστημα (συνήθως σε χιλιοστά του δευτερολέπτου) όπου ένα ICMP πακέτο χρειάζεται (αυτό αντιστοιχεί στην εντολή *ping*) για να φτάσει στον προορισμό (σε αυτή την περίπτωση στον υπολογιστή με διεύθυνση IP 8.8.8.8) και να επιστρέψει στον αποστολέα (τον υπολογιστή μας).

Εάν δεν υπάρχει σύνδεση μεταξύ του αποστολέα και του προορισμού, το μήνυμα σφάλματος θα είναι παρόμοιο με το παρακάτω:

Δείτε τώρατι συμβαίνει κατά την εκκίνηση της εντολής "ping dns.google ". *Το Dns google* πρέπει να μεταφραστεί στην αντίστοιχη διεύθυνση IP του. Ποια είναι αυτή η IP;



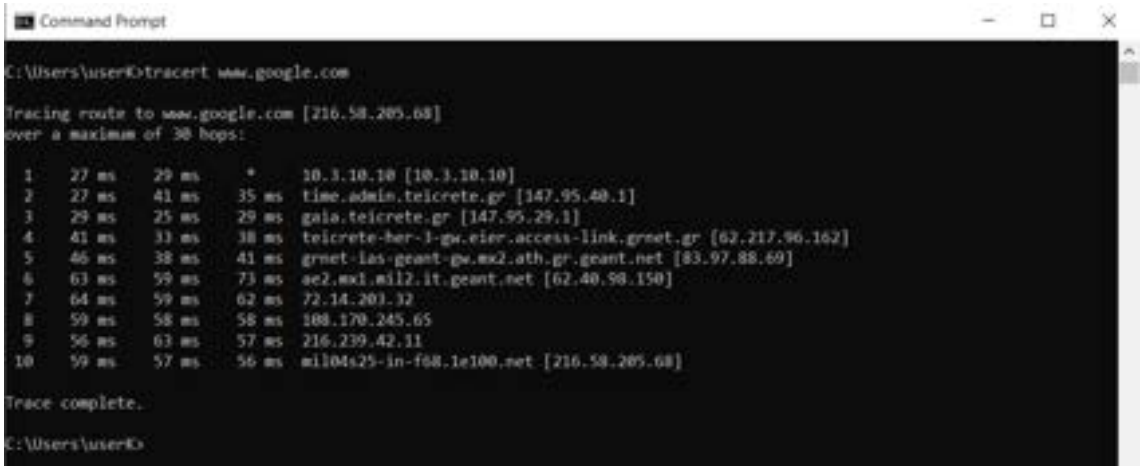
Τώρα τρέξτε την εντολή "ping google.com ". Ποια είναι η IP;

Εργασία 3. Εντολή Tracert

Το Διαδίκτυο αποτελείται από πολλά δίκτυα, που συνδεδεμένα μεταξύ τους με συσκευές επικοινωνίας που ονομάζονται δρομολογητές. Όταν οι πληροφορίες αποστέλλονται μέσω του Διαδικτύου, τα δεδομένα περνούν από κάθε δρομολογητή έως ότου φτάσουν στον προορισμό τους. Κάθε φορά που ένα δίκτυο αλλάζει μέσω ενός δρομολογητή, λέμε ότι τα δεδομένα έχουν γίνει "jumped".

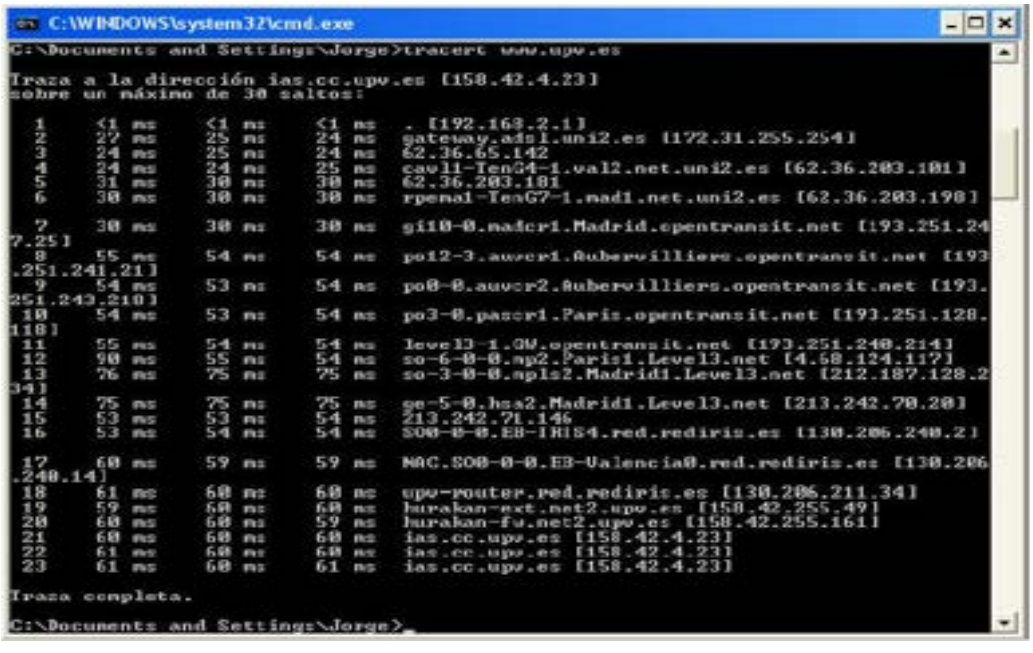
Η εντολή tracert μπορεί να χρησιμοποιηθεί για να γνωρίζουμε ποιες συσκευές έχουν περάσει τα δεδομένα για να φτάσουν στον προορισμό τους. Αυτή η εντολή λειτουργεί όπως η εντολή ping. Σε ένα παράθυρο διεπαφής εντολών, πρέπει να πληκτρολογήσουμε την εντολή tracert ακολουθούμενη από τη διεύθυνση IP ή το όνομα τομέα (domain) από το οποίο χρειαζόμαστε τις πληροφορίες. Εάν ζητάμε έναν τομέα, δίνει επίσης πληροφορίες για μια διεύθυνση IP.

Για παράδειγμα, εάν πρέπει να μάθουμε πώς να φτάσουμε στον διακομιστή ιστού της Google, πρέπει να εκτελέσουμε την εντολή "tracert www.google.com " :



Η απάντηση δείχνει τις διευθύνσεις IP των δρομολογητών που έχει περάσει το αίτημα απόκρισης έως ότου φτάσει στον προορισμό του, καθώς και τον χρόνο απόκρισης τους.

Χρησιμοποιώντας την εντολή tracert μπορεί να παρατηρήσουμε κάποιες ιδιαιτερότητες, όπως το ότι δεν ακολουθείται πάντα η συντομότερη διαδρομή για να φτάσει στον προορισμό. Στο παρακάτω παράδειγμα μπορείτε να δείτε ότι για να φτάσετε στον διακομιστή UPV απο το Μπιλμπάο (ο οποίος βρίσκεται στη Βαλένθια), επιλέχτηκε διαδρομή μέσω διάφορων δρομολογητών που βρίσκονται στο Παρίσι.



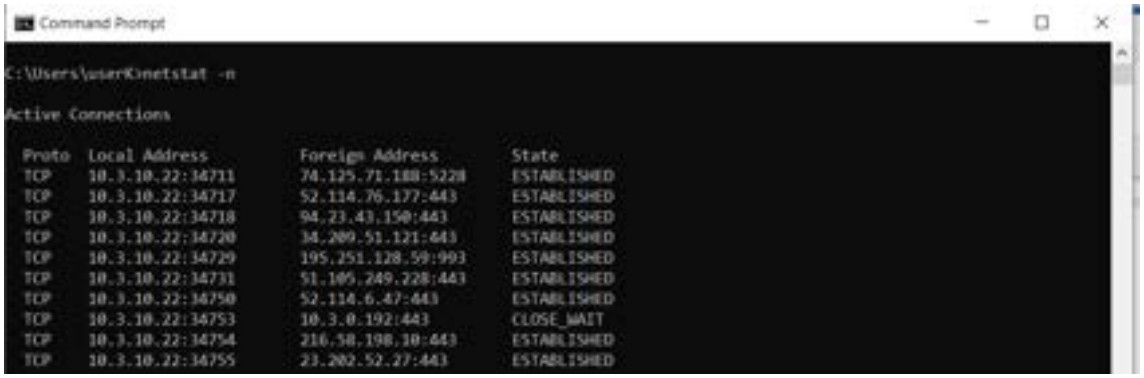
Συμπληρώστε τον παρακάτω πίνακα με τα αποτελέσματα της εντολής tracert στους ακόλουθους τομείς:

Όνομα	**Αριθμός από άλματα “jumps”**
www.elpais.com	
www.upv.es	
www.marca.com	
Smtp.correo.yahoo.es	
www.google.com	

Εργασία 4. Εντολή Netstat

Η εντολή netstat εμφανίζει τις συνδέσεις που είναι ανοιχτές μεταξύ διαφόρων υπολογιστών, για παράδειγμα, όταν συνδέεστε σε έναν ιστότοπο ή κάνετε λήψη του email.

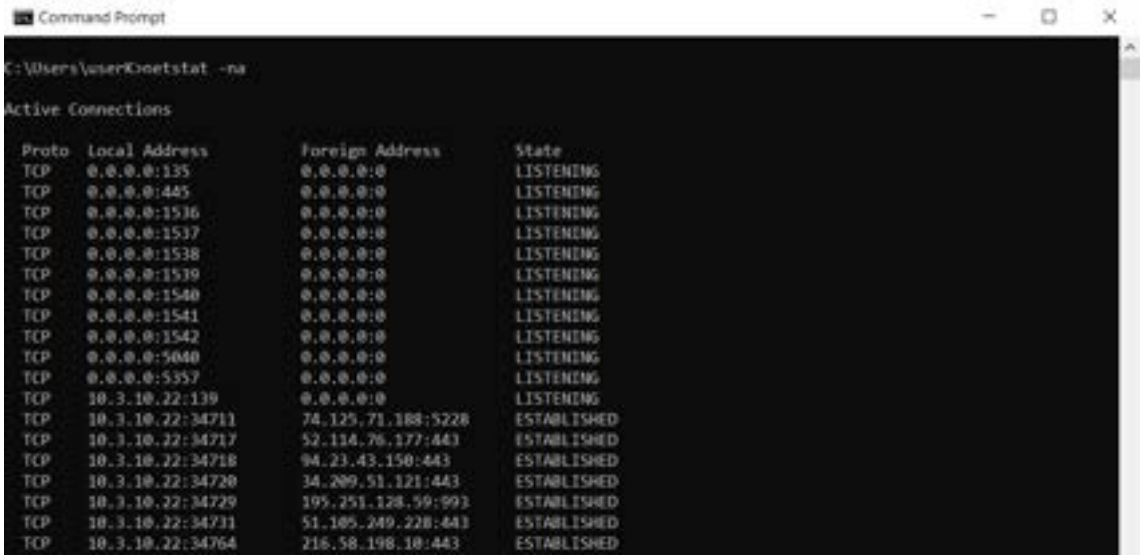
Εκτελέστε την εντολή "netstat -n" και δείτε ποιες συνδέσεις είναι ανοιχτές αυτήν τη στιγμή στον υπολογιστή σας:



Στην απάντηση της εντολής Netstat, τόσο οι τοπικές όσο και οι απομακρυσμένες διευθύνσεις υποδεικνύονται από το όνομα IP ή το όνομα υπολογιστή, ακολουθούμενο από δύο κουκίδες και τον αριθμό της θύρας. Η θύρα είναι ένας αριθμός που δείχνει την εφαρμογή ή το πρωτόκολλο που χρησιμοποιείται.

Για παράδειγμα, η θύρα 80 προέρχεται από το πρωτόκολλο http, για ιστότοπους ενώ η θύρα 1863 είναι η θύρα Messenger (εφαρμογή ανταλλαγής μηνυμάτων).

Μια άλλη επιλογή για την εντολή netstat είναι η παράμετρος -a. Αυτό δείχνει ποιες θύρες έχετε ανοίξει αυτήν τη στιγμή στον υπολογιστή σας. Πρόκειται για εφαρμογές που ακούνε ως διακομιστές στον υπολογιστή σας και επιτρέπουν σε άλλα άτομα να συνδεθούν στον υπολογιστή σας (για παράδειγμα, εάν έχετε ένα κοινόχρηστο φάκελο). Αυτό μπορείτε να το αναγνωρίσετε επειδή η κατάσταση (State) δείχνει *Listening*.



Εκκινήστε την εντολή netstat -a στη γραμμή εντολών σας. Πόσες συνδέσεις υπάρχουν; Ποιες είναι οι διευθύνσεις IP και οι θύρες τους;

Εργασία 5. Πώς να συνδεθείτε μέσω SSH / Telnet σε δρομολογητή για προηγμένες ρυθμίσεις με το PuTTY

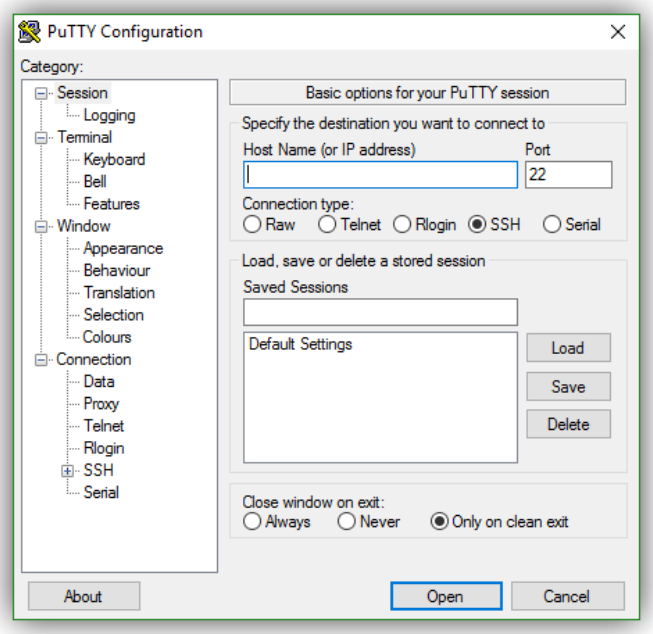
Σήμερα, σχεδόν όλοι οι δρομολογητές στην αγορά έχουν ένα web interface από το οποίο μπορούμε να κάνουμε όλες τις ρυθμίσεις τους: Αλλαγή του ονόματος χρήστη / κωδικού πρόσβασης, τις ρυθμίσεις Wi-Fi, άνοιγμα θυρών και ούτω καθεξής. Αυτή η διεπαφή έχει δημιουργηθεί κυρίως για οικιακούς χρήστες, οι οποίοι έχουν έλλειψη προηγμένων γνώσεων. Εκτός από το ότι είναι φιλικό προς το χρήστη, δείχνει μόνο τις κύριες και τις πιο χρησιμοποιούμενες επιλογές των δρομολογητών και επομένως οι περισσότερες από τις λειτουργίες είναι κρυφές και χωρίς πρόσβαση , τουλάχιστον μέσω αυτής της διεπαφής.

Πρακτικά κάθε δρομολογητής διαθέτει ένα διακομιστή Telnet ο οποίος είναι ιδανικός για έμπειρους χρήστες με προηγμένες γνώσεις και επιτρέπει την επικοινωνία με τον δρομολογητή από τη γραμμή εντολών,. Μας επιτρέπει να ελέγξουμε σχεδόν κάθε δυνατή εσωτερική ρύθμιση από το δρομολογητή, σε περίπτωση που χρειαζόμαστε πρόσβαση σε αυτούς. Οι πιο προηγμένοι δρομολογητές διαθέτουν υποστήριξη πρωτοκόλλου SSH, που μας επιτρέπει να συνδεθούμε με παρόμοιο τρόπο όπως και μέσω του Telnet, αλλά κρυπτογραφώντας όλες τις συνδέσεις.

Παρόλο που το λειτουργικό σύστημα Windows μπορεί να ενεργοποιήσει Telnet και SSH συνεδρίες στο σύστημα, υπάρχουν ορισμένες εφαρμογές τρίτων που είναι ευκολότερες στη χρήση, όπως το PuTTY, που θα μας επιτρέψουν να διαχειριστούμε όλες αυτές τις συνδέσεις με σωστό τρόπο .

Το PuTTY είναι μια δωρεάν εφαρμογή, φορητή (portable) και ανοιχτού κώδικα, η οποία έχει αναπτυχθεί για να διευκολύνει τις συνδέσεις μέσω των πρωτοκόλλων SSH / Telnet στο λειτουργικό σύστημα Windows (υπάρχει και σε Linux,Mac). Ας δούμε πώς μπορούμε να συνδεθούμε εξ αποστάσεως με έναν δρομολογητή χρησιμοποιώντας αυτά τα πρωτόκολλα.

Πρώτον, πρέπει να κατεβάσετε την τελευταία έκδοση του PuTTY από τον κύριο ιστότοπό τους. Είναι φορητό (portable) και δεν χρειάζεται εγκατάσταση, οπότε μόλις το κατεβάσετε, χρειάζεται μόνο να το εκτελέσετε. Θα ανοίξει ένα παράθυρο παρόμοιο με αυτό:

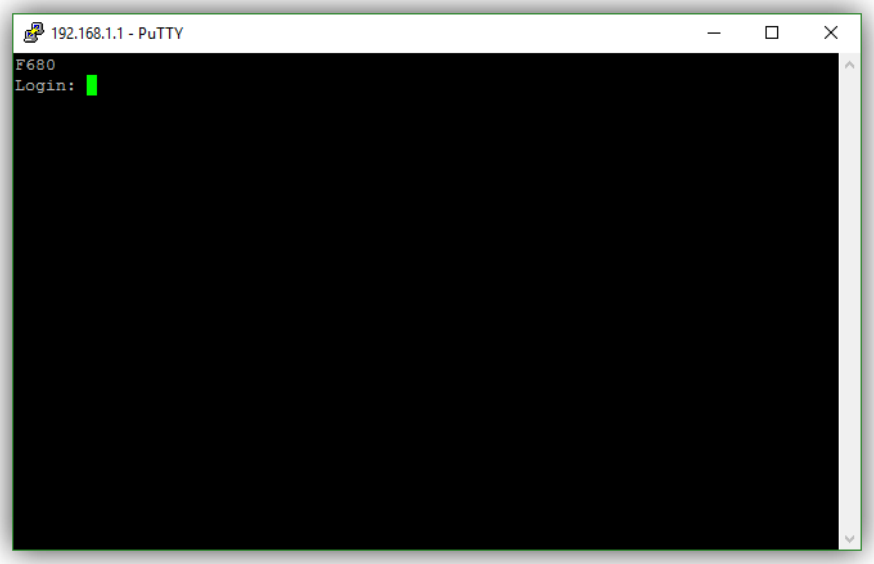


Πρώτα, πρέπει να εισαγάγουμε τη διεύθυνση IP του δρομολογητή μας. Συνήθως είναι η 192.168 .1.1 ή η 192.168.0.1, ανάλογα με το μοντέλο και τις ρυθμίσεις που έχουμε.

Ακριβώς κάτω από το κενό που εισάγαμε την IP μας, βρίσκουμε το "**Τύπος σύνδεσης/Connection type"**, στο οποίο πρέπει να καθορίσουμε το πρωτόκολλο που πρόκειται να χρησιμοποιήσουμε. Τα πιο συνηθισμένα, όπως είπαμε, είναι το SSH και το Telnet. Εάν ο δρομολογητής μας συνδέεται μέσω της σειριακής θύρας, το PuTTY θα μας επιτρέψει επίσης να ορίσουμε μια σύνδεση με τη σειριακή θύρα για να τη ρυθμίσουμε μέσω των εντολών.

Αφού εισαγάγετε την IP και επιλέξετε το πρωτόκολλο σύνδεσης, πατήστε "Άνοιγμα" και το πρόγραμμα θα συνδεθεί στο δρομολογητή.

Εάν η σύνδεση επιτρέπεται και έχει ρυθμιστεί, το PuTTY θα εμφανίσει το ακόλουθο παράθυρο:



Τέλος, πρέπει να συνδεθούμε με το όνομα χρήστη και τον κωδικό πρόσβασης για να ξεκινήσουμε τον έλεγχο της συσκευής.

Σημειώστε ότι το όνομα χρήστη και ο κωδικός πρόσβασης του Telnet / SSH δεν αντιστοιχούν απαραίτητα σε αυτά της διεπαφής ιστού (ειδικά σε δρομολογητές παρόχων) που θέλουμε να συνδεθούμε.

Co-funded by the
Erasmus+ Programme
of the European Union

ΕΝΟΤΗΤΑ 2

Αρχές ασφάλειας σε βιομηχανικά περιβάλλοντα, ενσωμάτωση IT/OT

2.1 Ασφάλεια σε Κρίσιμες Υποδομές

Description

2.1 Ασφάλεια σε Κρίσιμες Υποδομές

Table of contents

Η ασφάλεια εργοστασίου διασφαλίζει ότι τα κτίρια που εμπλέκονται στην κατασκευαστική διαδικασία είναι καλά προστατευμένα ενάντια στην απαγορευμένη πρόσβαση. Ορισμένα αντίμετρα που μπορούν να παρθούν είναι:

Ø **Φράχτες**

Η περικύκλωση ενός εργοστασίου με φράχτες είναι κοινή πρακτική (εικόνα 2.1)

Εικόνα 2.1 Βιομηχανική περιοχή με φράχτη πηγή

Τυπικά, ο φράχτης θέτει τα όρια του εργοστασιακού χώρου, αλλά η κύρια χρήση του είναι να λειτουργήσει ως πρώτο μέτρο ασφάλειας απέναντι σε πιθανούς εισβολείς. Αν κι ο φράχτης από μόνος του δε θα εμποδίσει έναν εισβολέα, μπορεί να χρησιμοποιηθεί παράλληλα με άλλα μέτρα ασφάλειας κι έτσι να αποτελέσει μια καλή προστατευτική λύση. Τη σήμερον ημέρα οι φράχτες γίνονται «έξυπνοι». Αυτό σημαίνει ότι οι αισθητήρες του φράχτη μπορούν να αναγνωρίσουν αν έχει μπει κάποιος εισβολέας στην απαγορευμένη περιοχή. Αυτή η νέα γενιά φραχτών μπορεί να συνδεθεί σε δίκτυο.

G

G **Φρουροί.**

Η παρουσία φρουρών εξαρτάται από τον τύπο και το μέγεθος της εγκατάστασης. Ανάλογα με τη νομοθεσία, ίσως μπορούν και να είναι οπλισμένοι. Συνήθως υπάρχει φυλάκιο στην κεντρική πύλη του εργοστασίου κι οι φρουροί επιτρέπουν ή εμποδίζουν την είσοδο του προσωπικού και των επισκεπτών. Μέρος των καθηκόντων τους μπορεί να είναι κι η περιπολία του εργοστασίου, ειδικά όταν αυτό είναι κλειστό.

Περιστρεφόμενες θύρες.

Μια περιστρεφόμενη θύρα (εικόνα 2.2) μπορεί να υπάρχει στην κεντρική πύλη του εργοστασίου. Εμποδίζει την ανεξέλεγκτη είσοδο επισκεπτών και καθυστερεί τους εισβολείς. Οι πιο πρόσφατες υλοποιήσεις δίνουν δυνατότητες δικτύου στις περιστρεφόμενες θύρες.

Εικόνα 2.2: Μια περιστρεφόμενη θύρα από τη Fabtron – CC BY-SA 4.0 πηγή

Ø **Κάμερες CCTV**

CCTV σημαίνει closed circuit television (τηλεόραση κλειστού κυκλώματος). Οι κάμερες ασφάλειας (εικόνα 2.3) τοποθετούνται στην εξωτερική περίμετρο του εργοστασίου – συνήθως στις κολόνες του εξωτερικού φράχτη – για να καταγράφουν κάθε δραστηριότητα 24/7. Κάμερες ασφάλειας τοποθετούνται και στο κτίριο, στην κεντρική είσοδο και πολλές φορές ακόμα και στους εργασιακούς χώρους. Σε μεγάλες εγκαταστάσεις (με μεγάλο αριθμό καμερών ασφάλειας) υπάρχει δωμάτιο ελέγχου, όπου το εξουσιοδοτημένο κι εκπαιδευμένο προσωπικό παρακολουθεί τις κάμερες για να εντοπίσει τυχόν παραβατική συμπεριφορά. Όλα τα δεδομένα που καταγράφουν οι κάμερες αποθηκεύονται σε σκληρούς δίσκους, σε ψηφιακό καταγραφέα βίντεο (Digital Video Recorder) (DVR) ή σε δικτυακό καταγραφέα βίντεο (network video recorder) (NVR). Στην τελευταία περίπτωση, ο τεχνικός εγκατάστασης και το προσωπικό παρακολούθησης πρέπει να είναι πολύ προσεκτικοί, διότι το NVR μπορεί να γίνει στόχος ψηφιακής επίθεσης (cyberattack).

Εικόνα 2.3 Κάμερες ασφαλείας

Βιομετρικοί αισθητήρες

Τοποθετούνται έξω από πόρτες, κεντρικές πύλες κλπ. Τα τυπικά βιομετρικά δεδομένα για την ταυτοποίηση ενός ατόμου συμπεριλαμβάνουν: δαχτυλικά αποτυπώματα, ίριδα ματιού και σχήμα προσώπου. Αφού όλα τα προαναφερόμενα βιομετρικά χαρακτηριστικά είναι μοναδικά για κάθε άτομο, οι βιομετρικοί αισθητήρες υποτίθεται ότι προσφέρουν ένα πολύ καλό επίπεδο ασφάλειας. Ωστόσο, υπάρχει πάντα το ρίσκο της δολιοφθοράς, ειδικά όταν είναι συνδεδεμένοι σε δίκτυο. Οι βιομετρικοί αισθητήρες μπορούν και να χρησιμοποιηθούν συνδυαστικά με κάρτες RFID ή και με κάποιον κωδικό για ακόμα καλύτερη ασφάλεια (εικόνα 2.4). Οι πιο σύγχρονοι βιομετρικοί αισθητήρες έχουν δυνατότητες δικτύου, οπότε είναι αρκετά μεγάλο το ρίσκο να γίνουν στόχοι ψηφιακής επίθεσης.

Ø 

Εικόνα 2.4 – Βιομετρικός αισθητήρας - Πηγή

Ø

Ελεγκτές Πρόσβασης

Αυτά τα συστήματα ασφάλειας χρησιμοποιούνται για να παράσχουν πρόσβαση σε εξουσιοδοτημένο προσωπικό ή επισκέπτες. Είναι προγραμματιζόμενοι και μπορούν να καθορίσουν διαφορετικά δικαιώματα πρόσβασης, ανάλογα με το πλάνο ασφάλειας της βιομηχανίας. Διαφορετικοί υπάλληλοι μπορούν να έχουν διαφορετικά δικαιώματα πρόσβασης ως προς τις περιοχές που μπορούν να επισκεφτούν, τις ώρες επίσκεψης κλπ. Όπως όλες οι προαναφερόμενες μέθοδοι, έτσι κι οι ελεγκτές πρόσβασης έχουν δυνατότητες δικτύωσης. Μπορούν να χρησιμοποιηθούν συσκευές RFID, έξυπνες μαγνητικές κάρτες ή ακόμα και βιομετρικοί αισθητήρες.

Ασφάλεια Δικτύου

- Αφορά σε hardware και σε software
- Εστιάζει σε ποικίλες απειλές
- Εμποδίζει τη μη εξουσιοδοτημένη πρόσβαση σε δίκτυα
- Επιβλέπει την πρόσβαση στο δίκτυο

Κοινοί τύποι ασφάλειας δικτύου είναι:

- Λογισμικό Internet security (antivirus, anti-malware, προστασία από ransomware κλπ.)
- Ασφάλεια εφαρμογών
- Αποφυγή απώλειας δεδομένων
- Ασφάλεια Email
- Firewalls – Διαχωρισμός Δικτύου - Virtual Private Network (VPN)
- Ασφάλεια web
- Ασύρματη ασφάλεια
- Έλεγχος πρόσβασης

Η ακεραιότητα του συστήματος αφορά σε όλα τα μέτρα/πολιτικές που έχουν παρθεί για την προστασία των αυτοματοποιημένων συστημάτων και εξαρτημάτων από τη μη εξουσιοδοτημένη πρόσβαση (φυσική ή απομακρυσμένη). Ορισμένα μέτρα μπορεί να είναι:

- Λογισμικό Antivirus και λογισμικό εξουσιοδότησης
- Συντήρηση και διεργασίες ενημέρωσης λογισμικού
- Ταυτοποίηση χρηστών για χειριστές εργοστασίου ή μηχανημάτων
- Ενσωματωμένοι μηχανισμοί προστασίας για την πρόσβαση σε αυτοματοποιημένα εξαρτήματα

2.2. Ενσωμάτωση OT/IT

Description

2.2. Ενσωμάτωση OT/IT

Table of contents

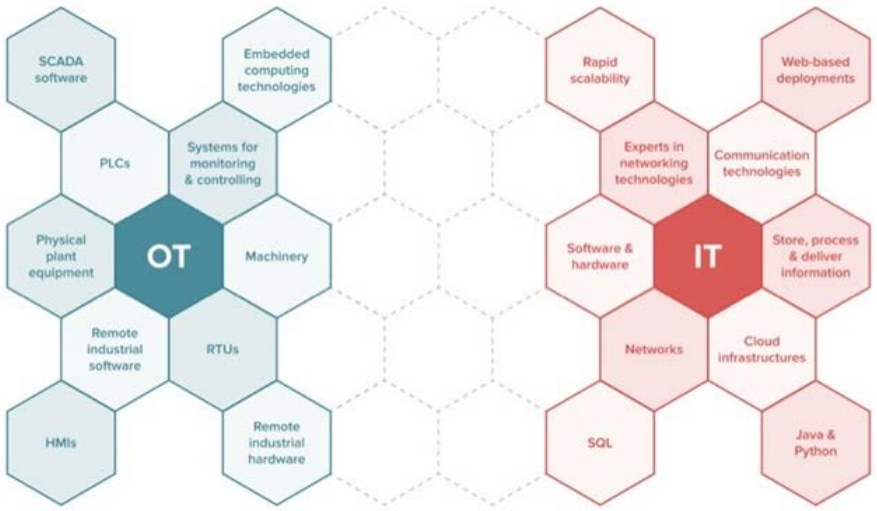
Η Τεχνολογία λειτουργίας (operational technology) (OT) σε οποιοδήποτε βιομηχανικό περιβάλλον είναι το hardware και το software που εντοπίζει ή προκαλεί μια αλλαγή μέσω της απευθείας παρακολούθησης και/ή τον έλεγχο των φυσικών συσκευών, διεργασιών και συμβάντων στην επιχείρηση.

Βασικά, το OT είναι η χρήση υπολογιστών (PCs) για την παρακολούθηση ή την αλλαγή της φυσικής κατάστασης ενός συστήματος.

Ορισμένα παραδείγματα είναι:

- SCADA
- PLCs
- Επιστημονικός εξοπλισμός
- DCS

Η τεχνολογία πληροφορίας (Information Technology) (IT) αφορά σε ό,τι ταυτίζεται με την εισαγωγή καινοτομίας στην τεχνολογία υπολογιστών, στον εξοπλισμό υπολογιστών, στον προγραμματισμό λογισμικού, και στη διαχείριση hardware και συστημάτων. Ο προγραμματισμός λογισμικού αφορά όλα τα προγράμματα – κώδικες και οδηγίες – μέσα σε ένα PC. Τα PCs δε λειτουργούν χωρίς προγραμματισμό. Το hardware του υπολογιστή, όπως αναφέρεται σε αυτήν την περίπτωση, αφορά στα φυσικά κομμάτια ενός PC. Η οθόνη, το ποντίκι, η μητρική κι ένα σωρό άλλες συσκευές, είναι όλες τους συσκευές hardware.



Εικόνα 2.5 – Τεχνολογία λειτουργίας (OT) και τεχνολογία πληροφορίας (IT) Πηγή

Μπορεί να έρθει στο μυαλό σας ότι το IT είναι οι επικοινωνίες, το hardware και το software ενός συστήματος, που αποθηκεύει, επεξεργάζεται και μεταβιβάζει δεδομένα σε όλα τα τμήματα ενός οργανισμού. Οι ειδικοί των τμημάτων IT είναι πολύ οικείοι με αυτές τις διαδικασίες και περνούν πολύ χρόνο σε αυτές. Ασχολούνται με το cloud, με διαδικτυακές εφαρμογές, τεχνολογίες προγραμματισμού (Python, SQL, java, c++) κλπ.

Το OT συμπεριλαμβάνει συσκευές, φυσικό εξοπλισμό, hardware κι απομακρυσμένο βιομηχανικό λογισμικό. Οι ειδικοί των τμημάτων OT επικεντρώνονται σε συστήματα που αφορούν στην παρακολούθηση και στον έλεγχο. Αυτές οι υλοποιήσεις αφορούν σε PLCs, σε διεπαφές ανθρώπου μηχανής (HMIs), σε ενσωματωμένες τεχνολογίες υπολογισμών, σε RTUs και σε πλαίσια SCADA.

Τα συστήματα SCADA συγκεντρώνουν πληροφορίες από διάφορες διαδικασίες στον εργοστασιακό χώρο. Οι επαγγελματίες του OT πρέπει να αντιληφθούν πώς να ενσωματώσουν όλα τα συστήματα για να συνεργαστούν μεταξύ τους. Δεδομένου ότι οι περισσότερες καινοτομίες στον χώρο του OT είναι πατενταρισμένες, είναι δύσκολη η ενσωμάτωση πολλών διατάξεων SCADA.

Το PROFINET (δίκτυο OT) και το Ethernet (δίκτυο IT) είναι δύο διαδεδομένα πρωτόκολλα που μπορούν να διασυνδεθούν (περισσότερες πληροφορίες στο Module 1). Το μόνο πρόβλημα με τη διασύνδεσή τους είναι ότι ίσως μειωθεί η availability.

Για περισσότερες πληροφορίες στα αντίμετρα ασφάλειας, επισκεφτείτε: https://www.iso.org/isoiec-27001-information-security.html

Η ενσωμάτωση OT/IT έχει πολλά πλεονεκτήματα:

Αυξάνει την παραγωγή και γλιτώνει χρόνο

Η τεχνολογία πληροφορίας έχει βοηθήσει την παραγωγική διαδικασία και την έχει κάνει απίστευτα αποδοτική από οικονομική άποψη. Έτσι αυξάνεται η αποδοτικότητα κι αυτό μεταφράζεται σε μεγαλύτερα κέρδη, άρα και καλύτερους μισθούς και λιγότερο κουραστικές συνθήκες εργασίας.

Βελτιώνει την επικοινωνία

Τα εργαλεία της τεχνολογίας πληροφοριών κι επικοινωνίας (information communication technology) (ICT), όπως το email, η τηλεδιάσκεψη, τα κινητά τηλέφωνα, τα laptops κλπ., επιτρέπουν την άμεση επικοινωνία μέσα σε μια επιχείρηση. Αυτό επιτρέπει την ύπαρξη ακόμα περισσότερης συνδεσιμότητας στις εσωτερικές κι εξωτερικές δομές.

Βελτιώνει την αποθήκευση δεδομένων, τη διαχείριση αρχείων και την ανάλυση/αναφορά δεδομένων

Οι επιχειρήσεις χρησιμοποιούν υπηρεσίες cloud για την αποθήκευση και τη δημιουργία αντιγράφων ασφάλειας των δεδομένων τους. Επιπροσθέτως, γλυτώνουν χρόνο έτσι και κάνουν ευκολότερη την πρόσβαση και μεταφορά δεδομένων απ' οπουδήποτε και σε οποιαδήποτε στιγμή. Με υπηρεσίες όπως το Dropbox, οι επαγγελματίες παίρνουν τις πληροφορίες τους οποτεδήποτε θελήσουν. Επιπλέον, οι σημερινές βάσεις δεδομένων προσφέρουν καλύτερη ανάλυση πολλών δεδομένων και διευκολύνουν τη λήψη αποφάσεων με απώτερο στόχο την ανάπτυξη.

Μειώνει τα λειτουργικά κόστη

Η τεχνολογία επικοινωνίας κι η κοινωνική τεχνολογία έχουν κάνει πιο οικονομική την ανάπτυξη των επιχειρήσεων και την κυκλοφορία των προϊόντων. Πολλές ανεξάρτητες εταιρείες έχουν ανακαλύψει προσεγγίσεις για την υλοποίηση της κοινωνικής τεχνολογίας, ώστε να γίνουν πιο αναγνωρίσιμες και να κερδίσουν περισσότερους πελάτες, με αμελητέο κόστος. Στοιχεία όπως το κόστος παίζουν αποφασιστικό ρόλο στην εξέλιξη κι ανάπτυξη μιας επιχείρησης. Με βάση αυτό το σκεπτικό, η χρήση των καινοτομιών της τεχνολογίας πληροφορίας στον τομέα των δεδομένων, μπορεί να μειώσει τα λειτουργικά κόστη και να φέρει την ανάπτυξη για την επιχείρηση.

Βελτιώνει την ανταγωνιστικότητα της επιχείρησης

Μια επιχείρηση χρησιμοποιεί την τεχνολογία για να αποκτήσει ανταγωνιστικά πλεονεκτήματα. Εξελίσσεται κι ασπάζεται την καινοτομία για να παραμείνει παραγωγική και για να βελτιώσει τις διεργασίες της. Τέτοιες επιχειρήσεις συνήθως έχουν υψηλό ποσοστό εμπιστοσύνης από τους πελάτες τους, αφού μπορούν να καλύψουν τις ανάγκες τους με αξιοπιστία.

Ωστόσο, η ενσωμάτωση OT/IT έχει και μειονεκτήματα:

Κόστος υλοποίησης

Μερικές φορές, οι μικρές επιχειρήσεις έχουν βασική τεχνολογία ακρίβειας και προσπαθούν να διατηρήσουν αυτή την τεχνολογία, οπότε χάνουν τους πελάτες τους για ν' ανταγωνιστούν τις άλλες εταιρείες της αγοράς τους, ενώ έχουν τα χρήματα και τους πόρους.

Χαμένες θέσεις εργασίας

Είναι ευρύτερα γνωστό ότι η τεχνολογική ανάπτυξη έχει αντικαταστήσει το ανθρώπινο δυναμικό σε πολλές δουλειές.

Παραβιάσεις ασφάλειας

Δεδομένου ότι οι επιχειρήσεις αποθηκεύουν τις πληροφορίες τους σε απομακρυσμένους cloud servers, στους οποίους μπορούμε να συνδεθούμε μέσω διαδικτύου με ένα username κι ένα μυστικό password, υπάρχει η πιθανότητα να χαθούν αυτές οι πληροφορίες εξαιτίας σφαλμάτων ή κακόβουλων hackers.

Για τη διασφάλιση της ασφάλειας και της αξιοπιστίας, είναι σημαντικό να υπάρχουν σαφείς γραμμένες οδηγίες για την τακτική εγκατάσταση όλων των ενημερώσεων του λογισμικού. Ο παρακάτω πίνακας προσφέρει κανόνες για τα αντίγραφα ασφάλειας, για τη διεξαγωγή της διαδικασίας ενημέρωσης και τον χρονικό προγραμματισμό της πραγματοποίησης των ενημερώσεων.

Από τους κανόνες: Η διατήρηση συγκεκριμένου χρονοδιαγράμματος ενημερώσεων – όπως κι η εφαρμογή βασικών διορθώσεων όταν ανακαλύπτονται τρωτά σημεία – είναι κρίσιμα για τη διατήρηση της ακεραιότητας της εταιρικής ασφάλειας. Με την έλευση απειλών όπως είναι τα ransomware, οι συχνές ενημερώσεις της ασφάλειας και της πλατφόρμας, καθώς κι η δημιουργία αντιγράφων ασφάλειας, είναι σημαντικά για να εξασφαλιστεί η ομαλή λειτουργία της επιχείρησης.

Πίνακας 1: Πολιτική ασφάλειας υπολογιστή

Εβδομαδιαίες ενημερώσεις

Δεδομένα:	Διορθώσεις ασφάλειας κι ενημερώσεις για τις εφαρμογές που είναι εγκατεστημένες.
Πρόγραμμα:	Κάθε Πέμπτη (ή κάποια άλλη μέρα) ξεκινώντας στις 8 μ.μ.
Κατάσταση ενέργειας:	Ο υπολογιστής πρέπει να είναι ανοιχτός για να δεχτεί ενημερώσεις.
Κατάσταση Login:	Ο υπολογιστής θα προσπαθήσει να εγκαταστήσει τις ενημερώσεις ανεξαρτήτως από το αν έχει συνδεθεί κάποιος στον υπολογιστή ή όχι. ΣΩΣΤΕ ΤΗ ΔΟΥΛΕΙΑ ΣΑΣ, ΑΦΟΥ Ο ΥΠΟΛΟΓΙΣΤΗΣ ΘΑ ΚΑΝΕΙ ΕΠΑΝΕΚΚΙΝΗΣΗ ΑΝΕΞΑΡΤΗΤΑ ΑΠΌ ΤΟ ΑΝ ΥΠΑΡΧΟΥΝ ΑΝΟΙΧΤΕΣ ΕΦΑΡΜΟΓΕΣ.
Ανακατεύθυνση:	Αν ο υπολογιστής δεν είναι ανοιχτός κατά το προγραμματισμένο update, οι ενημερώσεις των εφαρμογών θα γίνουν την επόμενη φορά που θα ανοίξει.
Αντίγραφα ασφάλειας:	Κάντε αντίγραφα ασφάλειας των σημαντικών αρχείων δύο φορές τον μήνα.

Αν είναι login in κάποιος χρήστης

Επισκόπηση:	Ο υπολογιστής θα επιχειρήσει να εγκαταστήσει τις ενημερώσεις, δίνοντας στον χρήση ευέλικτες επιλογές εγκατάστασης κι επανεκκίνησης για να μην επηρεαστεί το εργασιακό πρόγραμμα. Οι ενημερώσεις θα εγκατασταθούν κι ο υπολογιστής θα κάνει επανεκκίνηση αν ο χρήστης δεν απαντήσει στις ειδοποιήσεις.
Λήξη χρόνου αναβολής:	Αν η ενημέρωση δεν αναβληθεί μέσα σε 30 λεπτά, τότε θα εγκατασταθεί αυτόματα.
Αναβολή επανεκκίνησης:	Αν εγκατασταθεί μια ενημέρωση που χρειάζεται επανεκκίνηση, ο χρήστης μπορεί να αναβάλει την επανεκκίνηση μέχρι κι εφτά (7) φορές προτού γίνει αυτόματη επανεκκίνηση για να ολοκληρωθεί η εγκατάσταση. Η αναβολή διαρκεί 30 λεπτά προτού ειδοποιηθεί ξανά ο χρήστης.

Λήξη χρόνο επανεκκίνησης: Αν η επανεκκίνηση δεν αναβληθεί μέσα σε 30 λεπτά, ο υπολογιστής θα μας ενημερώσει πάλι σε 120 λεπτά (κι άλλη αναβολή). Μετά τις παραπάνω εφτά (7) αναβολές, ο χρήστης θα αναγκαστεί να κάνει επανεκκίνηση.

Συχνότητα επανεκκίνησης: Αν εγκατασταθεί ενημέρωση που απαιτεί επανεκκίνηση, ο υπολογιστής θα επανεκκινηθεί μία φορά.

Επίδραση στην απόδοση: Οι ενημερώσεις των εφαρμογών ποικίλουν σε αριθμό και μέγεθος. Η επίδραση στην απόδοση του υπολογιστή είναι αμελητέα σε γενικές γραμμές κι απλά ίσως χρειαστεί να γίνει μία επανεκκίνηση μετά την εγκατάσταση.

Αν δεν είναι logged in κάποιος χρήστης

Επισκόπηση: Ο υπολογιστής θα εγκαταστήσει τις ενημερώσεις και θα επανεκκινηθεί αυτόματα αν χρειαστεί.

Συχνότητα επανεκκίνησης: Αν εγκατασταθεί ενημέρωση που απαιτεί επανεκκίνηση, ο υπολογιστής θα επανεκκινηθεί μία φορά.

Σημαντική ειδοποίηση

Τα PLCs είναι εξίσου σημαντικά σε δίκτυα συστημάτων ελέγχου, όπως θα ήταν και σε κάθε άλλο περιβάλλον δικτύου. Η διαχείρισή τους πρέπει να γίνεται οπωσδήποτε με τη μεγαλύτερη προτεραιότητα. Κάθε πρόσβαση, συντήρηση, αναβάθμιση, δοκιμή, τροποποίηση και διακοπή λειτουργίας των PLCs, πρέπει να λαμβάνεται υπόψη, όπως επίσης πρέπει και να επιβάλλονται αυτές οι πολιτικές.

Βασικές αρχές πολιτικής

- Διόρθωση προεπιλεγμένων κωδικών

Αλλάξτε όλους τους προεπιλεγμένους κωδικούς. Η μη αλλαγή των εργοστασιακών κωδικών είναι ένα από τα πιο κοινά λάθη που μπορεί να κάνει ένας οργανισμός.

- Διασφάλιση ότι στο περιβάλλον ελέγχου βρίσκονται μόνο εξουσιοδοτημένα άτομα

Για λόγους ασφάλειας, πρέπει να βρίσκονται μόνο εξουσιοδοτημένα άτομα στο εταιρικό σύστημα ελέγχου.

- Περιορισμός πρόσβασης στα thumb drives

Οι χρήστες πρέπει να ενημερώνονται συχνά για τη χρήση συσκευών και νέων τεχνολογιών, ή αν αλλάξει κάτι στο μέλλον.

- Αναβάθμιση του firmware στην τελευταία έκδοση

Μια κοινή ενημέρωση λειτουργικού συστήματος ή του firmware, είναι μια ενημέρωση ασφάλειας που εκδίδεται για την προστασία του υπολογιστή/συστήματός σας από τα τρωτά σημεία που μπορούν να εκμεταλλευτούν hackers και ιοί.

Εικόνα 2.6 PLC Πηγή

Εικόνα 2.7 PLC Πηγή

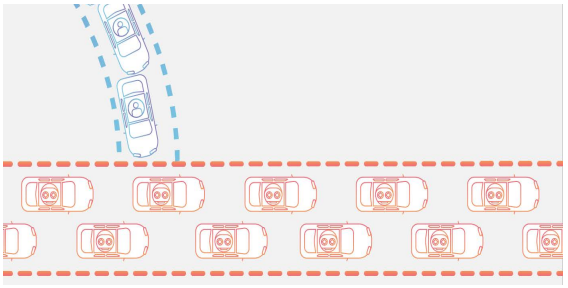
2.3 Επιθέσεις σε Βιομηχανικά Συστήματα

Description

2.3 Επιθέσεις σε Βιομηχανικά Συστήματα

Table of contents

Το **DOS** είναι ακρωνύμιο του **D**enial **o**f **S**ervice. Είναι ένας τύπος επίθεσης που πραγματοποιείται σε έναν υπολογιστή ή σε ένα δίκτυο και εμποδίζει την πρόσβαση των χρηστών στους πόρους του συστήματος. Κλείνει το site (web-server) που στοχεύετε. Για να το πετύχει αυτό, κάνει ταυτόχρονα πολλές αιτήσεις για υπηρεσίες προς τον server που φιλοξενεί το site, κι αυτός δεν μπορεί να τις ικανοποιήσει, οπότε κι αποτυγχάνει να τις διαχειριστεί. Όσο πραγματοποιείται μια επίθεση DoS, η κανονική κίνηση της σελίδας θα είναι είτε αργή είτε ανενεργή.

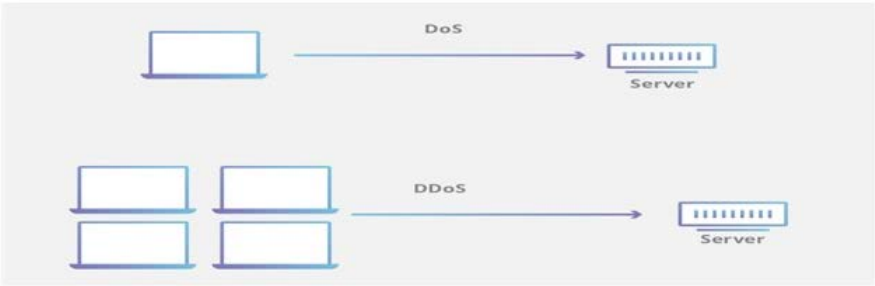


Εικόνα 2.8 – Κίνηση επίθεσης Dos Πηγή

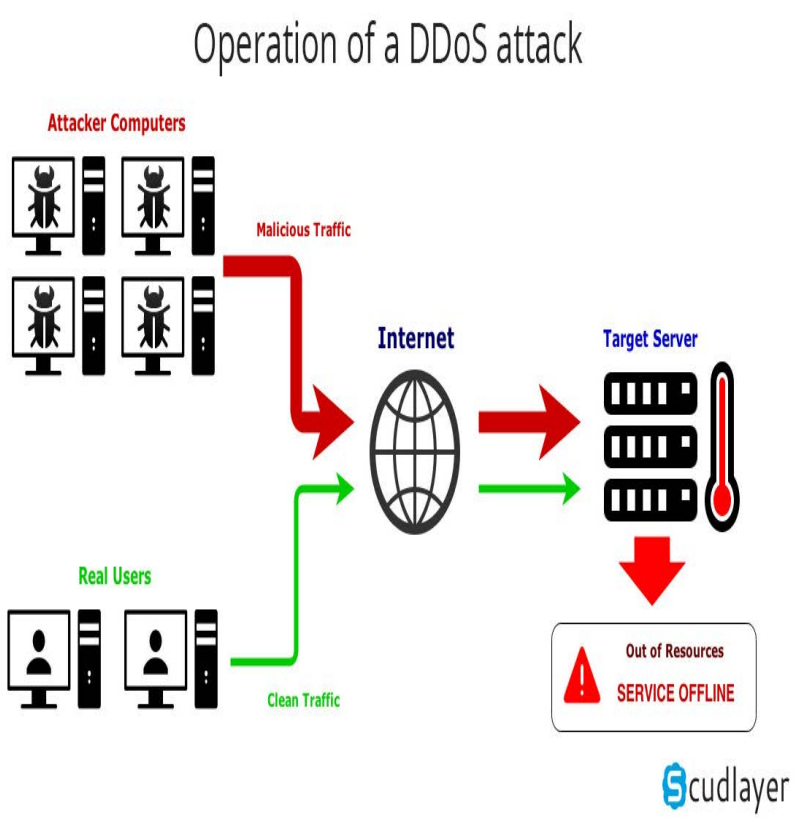
Η απομόνωση των επιχειρήσεων από το web μπορεί να οδηγήσει σε τεράστιο χάσιμο πελατών ή χρημάτων. Το διαδίκτυο και τα δίκτυα υπολογιστών τροφοδοτούν πολλούς οργανισμούς. Μερικοί από αυτούς, όπως υπηρεσίες ηλεκτρονικού εμπορίου (ecommerce) και πληρωμών για παράδειγμα, εξαρτώνται αποκλειστικά από το διαδίκτυο για την επιχειρηματική λειτουργία τους.

Υπάρχουν δύο τύποι επιθέσεων:

- **DoS**- αυτός ο τύπος επίθεσης γίνεται από έναν μοναδικό εξυπηρετητή (host).
- **Distributed DoS(DDoS)**- αυτή η επίθεση γίνεται στέλνοντας μεγάλο αριθμό αχρείαστων αιτημάτων στο σύστημα ή στο δίκτυο από πολλές διαφορετικές πηγές.



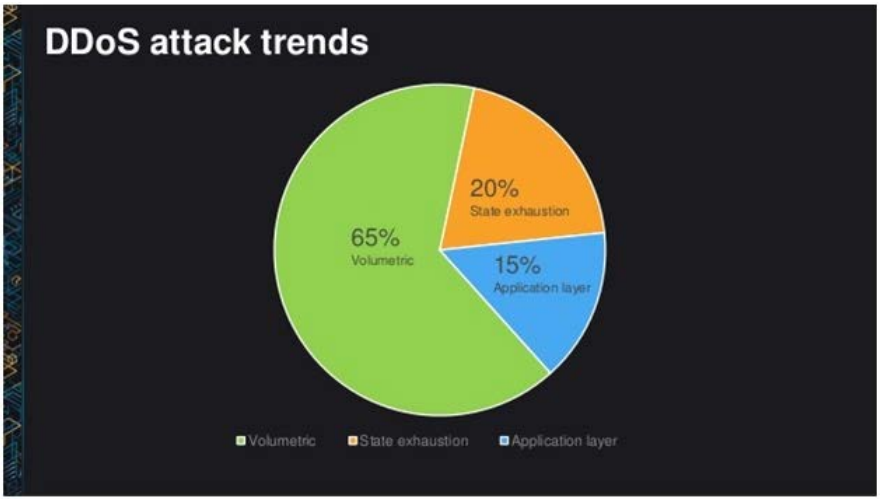
Εικόνα 2.9 – Τύποι επιθέσεων Dos Πηγή



Εικόνα 2.10 – Κατανόηση των επιθέσεων DDos Πηγή

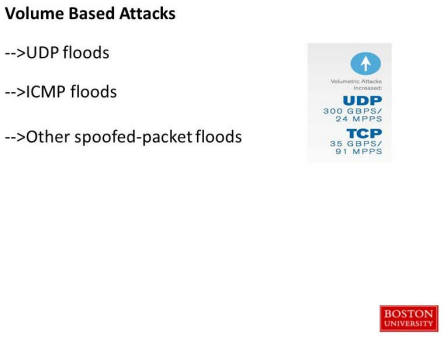
Υπάρχουν τρεις τύποι επιθέσεων DDoS:

- Volume-based Attacks(Ογκομετρικές επιθέσεις)
- Protocol Attacks(Επιθέσεις πρωτοκόλλου)
- Application Layer Attacks(Επιθέσεις εφαρμογών)



Εικόνα 2.11 – Τάσεις επιθέσεων DDos Πηγή

Οι ογκομετρικές επιθέσεις, όπως υποδεικνύει και το όνομά τους, βασίζονται στον όγκο. Λέγονται, επίσης, **κι επιθέσεις 3ου και 4ου Στρώματος.** Ο επιτιθέμενος χρησιμοποιεί βασικές τακτικές κι οι περισσότεροι διαθέσιμοι πόροι κερδίζονται σ' αυτό το «παιχνίδι». Αν καταφέρουν να υπερφορτώσουν και να ξεπεράσουν τους διαθέσιμους πόρους, τότε κερδίζουν. Στους περισσότερους ιδιοκτήτες site τελειώνουν εύκολα οι πόροι. Το μέγεθος της επίθεσης μετριέται σε bits ανά δευτερόλεπτο (**Bits per Second) (bps)**.



Εικόνα 2.12 – Ογκομετρικές επιθέσεις Πηγή

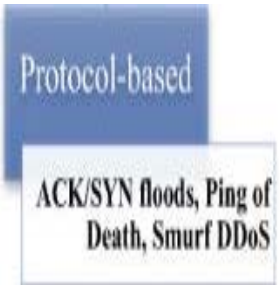
Ορισμένα floods είναι:

- **UDP Flood** – Μια επίθεση UDP flood αφορά στην αποστολή πολύ μεγάλου αριθμού πακέτων UDP σε τυχαίες θύρες ενός υπολογιστή, και ειδικά στη θύρα 53. Ο υπολογιστής που δέχεται επίθεση θα πρέπει πρώτα να δει αν ακούει κάποια υπηρεσία του σε εκείνη τη θύρα, κι αν αυτή δεν απαντάει, τότε αυτός θα πρέπει να απαντήσει με ένα πακέτο ICMP Destination Unreachable. Με αυτό τον τρόπο, η εισροή μεγάλου αριθμού πακέτων UDP στον υπολογιστή, τον αναγκάζει να απαντήσει με αντίστοιχα μεγάλο αριθμό πακέτων ICMP, πράγμα που εμποδίζει τους κανονικούς χρήστες να χρησιμοποιήσουν τις υπηρεσίες του. Μπορούν να χρησιμοποιηθούν εξειδικευμένα τείχη προστασίας για το φιλτράρισμα και το μπλοκάρισμα κακόβουλων πακέτων UDP.

- **ICMP Flood** – Ο επιτιθέμενος στέλνει πακέτα ICMP Echo Request σε έναν απομακρυσμένο εξυπηρετητή/χρήστη. Για να πετύχει μια τέτοια επίθεση, ο επιτιθέμενος πρέπει να έχει περισσότερο bandwidth από το θύμα. Αν το θύμα απαντήσει με πακέτο ICMP Echo Reply σε κάθε πακέτο ping (ICMP Echo Request), τότε καταναλώνει όλο το bandwidth του, με αποτέλεσμα να μην είναι πια διαθέσιμες οι υπηρεσίες του στους χρήστες. Μια τακτική αντιμετώπισης είναι: Αντί να απορρίπτει όλα τα πακέτα ping, το τείχος προστασίας καταγράφει τον αριθμό των πακέτων που λαμβάνει κι αν ο αριθμός ξεπερνάει ένα προκαθορισμένο όριο, τότε το τείχος προστασίας αρχίζει να τα απορρίπτει.

- **HTTP Flood** – Η επίθεση HTTP flood είναι τύπος επίθεσης denial of service, κατά την οποία ο επιτιθέμενος χειραγωγεί τα πρωτόκολλα HTTP και POST για να επιτεθεί σε έναν webserver ή σε μια εφαρμογή.

Επιθέσεις πρωτοκόλλου - Αυτός ο τύπος επίθεσης στοχεύει τα πρωτόκολλα. Αυτή η κατηγορία συμπεριλαμβάνει τις Synflood, Ping of Death, DNS flood και πολλές άλλες. Το μέγεθος της επίθεσης μετριέται σε πακέτα ανά δευτερόλεπτο (**Packets per Second)**.



Εικόνα 2.13 – Επιθέσεις πρωτοκόλλου

- **DNS Flood** – Ο επιτιθέμενος κανονίζει να στείλει έναν μεγάλο αριθμό αιτημάτων DNS στον στόχο, που είναι ένας σέρβερ DNS. Το θύμα δέχεται ταυτόχρονα τόσες πολλές αιτήσεις DNS, που αδυνατεί να τις διαχειριστεί κι έτσι καταλήγει να κλείσει λόγω υπερφόρτωσης στη μνήμη και στον επεξεργαστή.

- **SYN Flood** – Ο επιτιθέμενος στέλνει πολλαπλά αιτήματα SYN σε ένα θύμα. Ο υπολογιστής θύμα διαθέτει ένα μέρος στους πίνακές του για κάθε αίτημα που φτάνει και μετά στέλνει ένα πακέτο απάντησης SYN + ACK. Αν ο επιτιθέμενος δεν απαντήσει ή αν έχει κρύψει την πραγματική του διεύθυνση IP, η θέση στον πίνακα θα παραμείνει κρατημένη μέχρι να τελειώσει ο χρόνος αναμονής. Αν ο εισβολέας στείλει χιλιάδες αιτήματα SYN, τότε θα γεμίσουν οι θέσεις του πίνακα του θύματος και δε θα μπορούν να περάσουν οι έγκυρες συνδέσεις.

  Ο πιο αποτελεσματικός τρόπος αντιμετώπισης αυτού του ρίσκου είναι η καταγραφή του αριθμού των συνδέσεων με τις οποίες ξεκινά κάθε πελάτης κι η απαγόρευση της δημιουργίας νέων συνδέσεων, όταν ο αριθμός τους ξεπεράσει ένα προκαθορισμένο όριο. Ωστόσο, αν ο επιτιθέμενος στείλει κάθε αίτημα SYN από διαφορετική διεύθυνση IP, τότε η παραπάνω μέθοδος δε θα λειτουργήσει.

- **Ping of Death** – Ένα πακέτο ping πιάνει συνήθως 64 bytes (ή 84 bytes, αν προστεθεί κι η κεφαλίδα που προσθέτει το πρωτόκολλο IP). Πολλοί τύποι υπολογιστών δεν μπορούν να χειριστούν πακέτα ping μεγαλύτερα των 65535 bytes, που είναι και το μέγιστο όριο που επιτρέπει το πρωτόκολλο IP. Ως αποτέλεσμα, η επίθεση Ping Of Death αφορά στη συνεχόμενη αποστολή μεγάλων πακέτων ping σε έναν υπολογιστή, μέχρι να καταρρεύσει το σύστημα.

  Για την αντιμετώπιση αυτής της επίθεσης είναι σημαντικό να ελέγξουμε την εγκυρότητα των πακέτων κατά τη συγκρότηση των πακέτων IP. Έτσι μπορούμε να απορρίψουμε πακέτα IP που είναι μεγαλύτερα από το επιτρεπτό όριο και να αποφύγουμε το ρίσκο μιας τέτοιας επίθεσης.

Επιθέσεις επιπέδου εφαρμογών – Αυτός ο τύπος επίθεσης στοχεύει τρωτά σημεία σε λογισμικό, όπως είναι τα Windows, το Apache, το OpenBSD, κλπ., για την εκτέλεση της επίθεσης και την κατάρρευση του σέρβερ. Το μέγεθος της επίθεσης μετριέται σε αιτήματα ανά δευτερόλεπτο (**Requests per Second)**.

- **Application Attack** – Λέγεται κι επίθεση 7^{ου} επιπέδου. Είναι ένας από τους πιο δημοφιλείς τύπους επιθέσεων και στοχεύει συγκεκριμένα τρωτά σημεία στο επίπεδο εφαρμογών. Το μόνο που χρειάζεται είναι μια μικρή μετατροπή στον κώδικα και μια μικρή τροποποίηση για να ξεκινήσει η αποστολή πληροφοριών στους hackers. Είναι εξαιρετικά δύσκολο να αναγνωριστούν οι επιθέσεις 7^{ου} επιπέδου, αφού φαίνονται σαν κανονική κίνηση στο site.

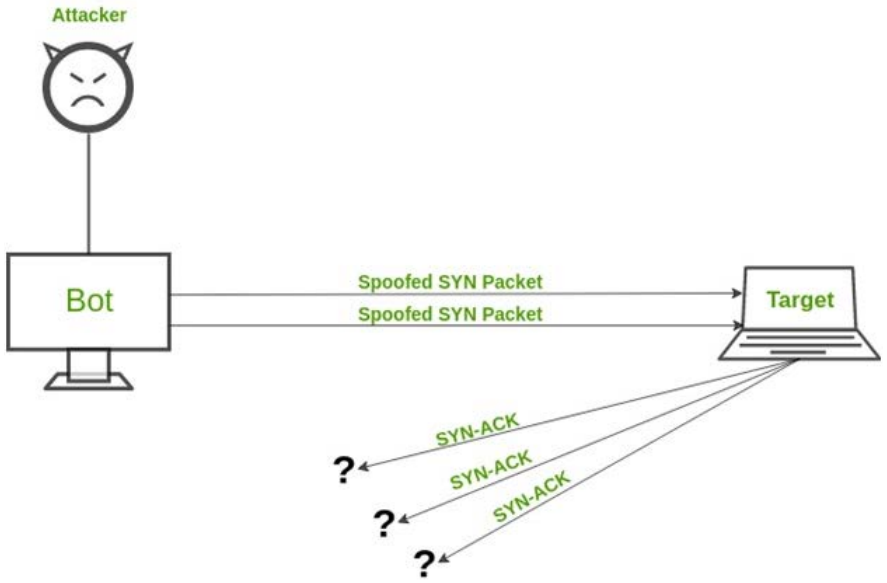
- **Slowloris** – Χρησιμοποιείται για την εκκίνηση του σέρβερ και την εκτέλεση μιας επίθεσης DDoS. Στέλνει τεράστιους αριθμούς αιτημάτων HTTP στον στόχο (webserver). Ο στόχος κρατά ανοιχτές όλες τις συνδέσεις κι έτσι υπάρχει σωστή πλημμύρα από ταυτόχρονες συνδέσεις.

- **Zero-day DDoS Attacks** – Αυτές είναι επιθέσεις νέου τύπου, που εκμεταλλεύονται τρωτά σημεία για τα οποία δεν έχει βγει ακόμα κάποιο patch. Το πιο κοινό παράδειγμα είναι η εκμετάλλευση τρωτών σημείων σε υπολογιστές με Linux.

Στην επίθεση **SYN Flood,** ο επιτιθέμενος στέλνει πολλαπλά αιτήματα SYN (Synchronization) (συγχρονισμού) στο θύμα, από πλαστή διεύθυνση IP (spoofed IP address). Το πρωτόκολλο TCP απαιτεί τα ακόλουθα τρία βήματα για να συνδέσει δύο υπολογιστές:

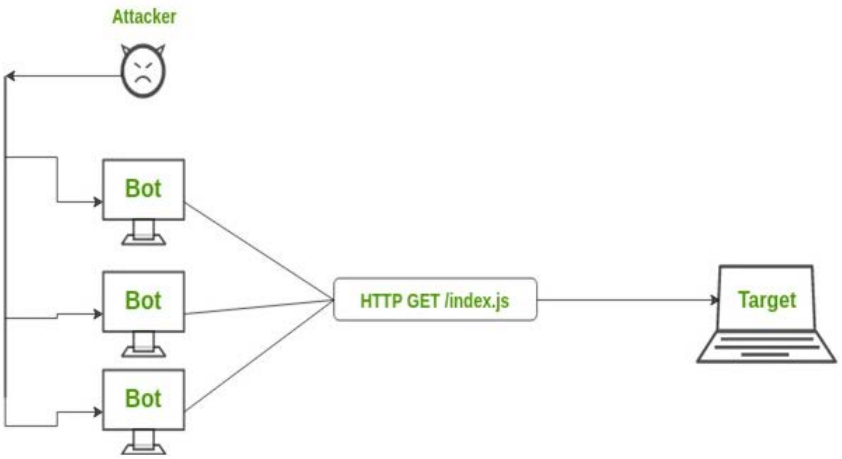
- Ο αποστολέας στέλνει πακέτο *SYN (Synchronize)*
- Ο παραλήπτης απαντά με πακέτο *SYN-ACK (Synchronize Acknowledge)*
- Ο αποστολέας στέλνει ένα πρόσφατο πακέτο ACK κι η σύνδεση θεωρείται επιτυχημένη.

Ο επιτιθέμενος στέλνει πολλαπλά αιτήματα SYN και δε στέλνει ACK, οπότε και συνεχίζει η διαδικασία, με στόχο να χαραμιστεί μεγάλο μέρος των υπολογιστικών πόρων και να υπάρξει αδυναμία εξυπηρέτησης άλλων χρηστών.



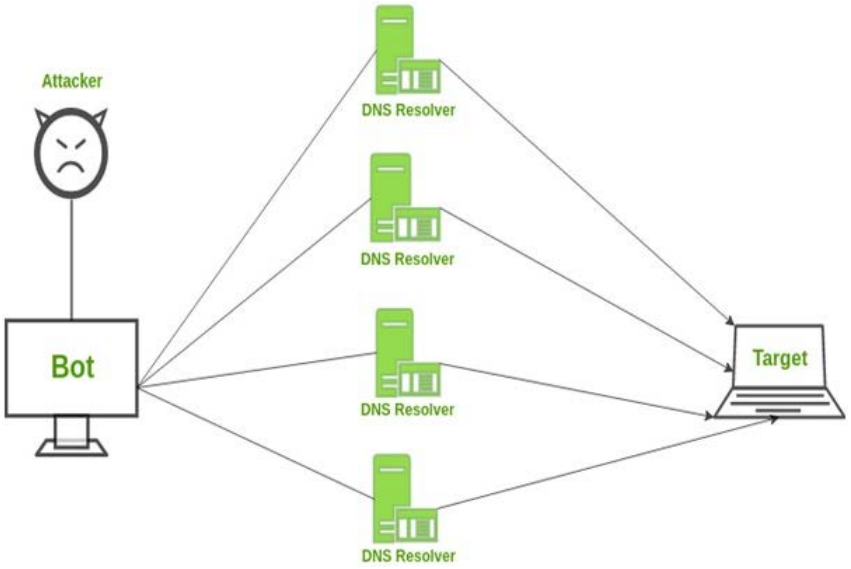
Εικόνα 2.14 – Επίθεση Syn flood Πηγή

Κατά την επίθεση **HTTP Flood** στέλνονται πολλαπλά αιτήματα HTTP GET ή POST εναντίον ενός web server ή μιας εφαρμογής. Η επίθεση αναγκάζει τον σέρβερ ή την εφαρμογή να αφιερώσει τους μέγιστους δυνατούς πόρους για να απαντήσει στο κάθε αίτημα.



Εικόνα 2.15 – Επίθεση HTTP flood Πηγή

Αυτές οι επιθέσεις είναι πολύ δημοφιλείς σήμερα και πραγματοποιούνται στα στρώματα 3 και 4. Χρησιμοποιούν ευρέως διαδεδομένους DNS servers από διαφορετικά σημεία της υφηλίου για να πλημμυρίσουν τον σέρβερ σας με κίνηση DNS response. Ο σέρβερ υπερφορτώνεται με ένα χαμό από απαντήσεις και δυσκολεύεται να λειτουργήσει λόγω της μείωσης των πόρων του, οπότε κι αδυνατεί να απαντήσει όπως πρέπει στην κανονική κίνηση DNS.



Εικόνα 2.16 – Επίθεση DNS flood Πηγή

Η αποτροπή επιθέσεων DDoS **είναι πιο δύσκολη** από την αποτροπή επιθέσεων DoS, δεδομένου ότι η κίνηση προέρχεται από πολυάριθμες διευθύνσεις IP (πηγές). Ένα τμήμα των συστημάτων ανακούφισης που μπορούν να χρησιμοποιηθούν, είναι:

Ορισμένες τεχνικές που μπορούν να χρησιμοποιηθούν, είναι:

1. **Blackhole routing**

Στη δρομολόγηση blackhole, η κίνηση του δικτύου κατευθύνεται σε μια «μαύρη τρύπα» (black hole). Τόσο η κακόβουλη, όσο κι η μη κακόβουλη κίνηση χάνονται μέσα σ' αυτή. Αυτό το αντίμετρο είναι χρήσιμο όταν ο σέρβερ δέχεται επίθεση DDoS κι όλη η κίνηση εκτρέπεται για να μην πέσει το δίκτυο.

2. **Rate limiting**

Μ' αυτή την τεχνική ελέγχουμε τον ρυθμό αποστολής και λήψης στην κίνηση μιας δικτυακής διασύνδεσης. Είναι αποτελεσματική στη μείωση της προόδου των web scrapers, καθώς και των προσπαθειών σύνδεσης brute-force. Ωστόσο, η τεχνική από μόνη της δύσκολα θα εμποδίσει συνδυαστικές επιθέσεις DDoS.

3. **Blacklisting / whitelisting**

Blacklisting λέγεται ο μηχανισμός μπλοκαρίσματος των διευθύνσεων IP, URLs, domains names κλπ., που αναφέρονται στη λίστα, κι η αποδοχή της κίνησης από όλες τις άλλες πηγές. Αντιθέτως, το whitelisting αφορά στον μηχανισμό που αποδέχεται όλες τις διευθύνσεις IP, URLs, domain names κλπ., που αναφέρονται στη λίστα, κι αρνείται την πρόσβαση κάθε άλλης πηγής στους πόρους του δικτύου.

Ένας οργανισμός μπορεί να ακολουθήσει την ακόλουθη στρατηγική για να θωρακιστεί απέναντι στις επιθέσεις Denial of Service.

- Οι επιθέσεις SYN flooding εκμεταλλεύονται σφάλματα στο λειτουργικό σύστημα (Windows, Linux, κλπ.). **Η εγκατάσταση διορθώσεων ασφάλειας** μειώνει την πιθανότητα τέτοιων επιθέσεων.
- **Τα Συστήματα εντοπισμού εισβολής (Intrusion detection systems) (IDS)** μπορούν να χρησιμοποιηθούν για την παρακολούθηση παράνομων δραστηριοτήτων.
- **Τα Routers(δρομολογητές)** μπορούν να ρυθμιστούν μέσω της λίστας ελέγχου πρόσβασης (Access Control List) για να περιορίσουν την πρόσβαση και να κόψουν την παράνομη κίνηση.
- Μπορούν να χρησιμοποιηθούν **τείχη προστασίας(firewalls)** για να σταματήσουν μια επίθεση DoS, εμποδίζοντας όλη την κίνηση που προέρχεται από τον επιτιθέμενο, αφού αναγνωρίσουν την IP του.

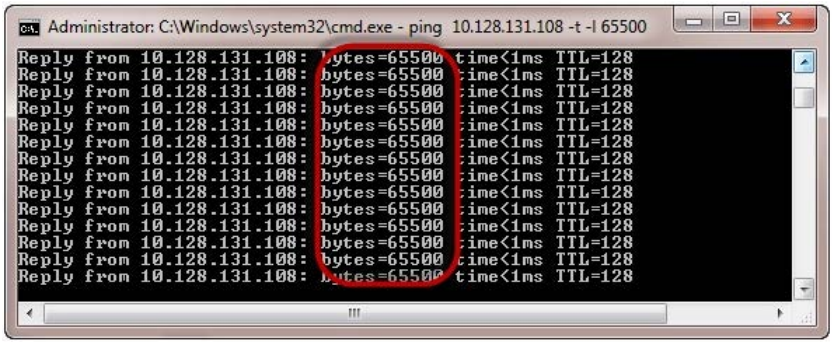
Εικόνα 2.17 – Μετριασμός επιθέσεων Dos Πηγή

Δραστηριότητα:

Ας υποθέσουμε ότι χρησιμοποιούμε Windows κι ότι έχουμε δύο υπολογιστές στο ίδιο δίκτυο. Οι επιθέσεις DOS είναι παράνομες σε συστήματα/δίκτυα στα οποία δεν έχουμε εξουσιοδότηση. Γι' αυτό τις εκτελούμε μόνο στο δικό μας σύστημα.

Ανοίγουμε τη γραμμή εντολών (command prompt) (cmd) των Windows.

Έχουμε ένα θύμα και πλημμυρίζουμε αυτή τη διεύθυνση IP με 65500 πακέτα.

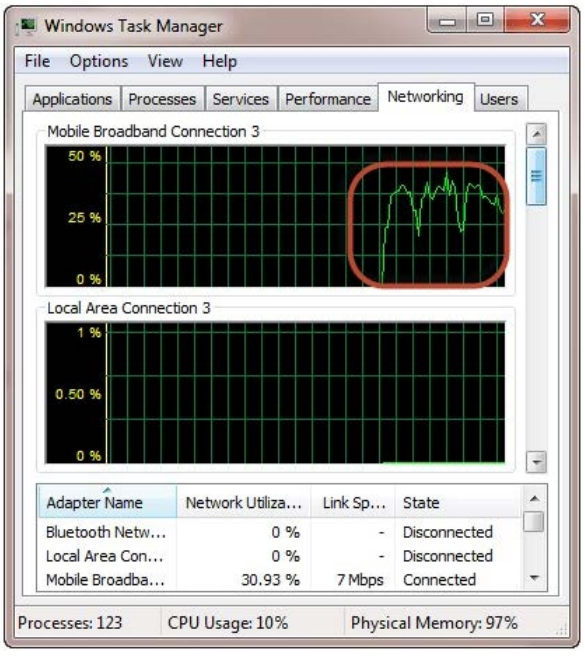


Εικόνα 2.18 Dos flooding(πλημμύρα)

Η επίθεση από έναν εξυπηρετητή έχει ελάχιστη επίδραση στον στόχο. Για να είναι πιο αποτελεσματική χρειάζεται περισσότερους υπολογιστές (Επίθεση DDoS).

Η επίθεση χρησιμοποιείται συχνά σε web servers, routers κλπ.

Για να ελέγξετε αν η επίθεση έχει επηρεάσει το θύμα, μπορείτε να ανοίξετε τη διαχείριση εργασιών (task manager) και να κάνετε κλικ στην καρτέλα δικτύωσης (networking).



Εικόνα 2.19 Έλεγχος δικτύου

Όπως βλέπουμε, η δραστηριότητα του δικτύου αυξήθηκε όταν πέτυχε η επίθεση.

- Ο στόχος μιας επίθεσης DOS είναι η άρνηση πρόσβασης των αληθινών πελατών σε έναν πόρο, δηλαδή σε ένα σύστημα, σε έναν σέρβερ και ούτω καθεξής.
- Υπάρχουν δύο τύποι επιθέσεων, η **DOS** κι η **DDoS**.
- Η επίθεση DOS μπορεί να γίνει χρησιμοποιώντας HTTP flood, DNS flood, SYN flood, επίθεση εφαρμογής, υπερχείλιση ενδιάμεσης μνήμης (buffer overflow) κλπ.
- Οι ενημερώσεις των λειτουργικών συστημάτων, τα τείχη προστασίας, τα συστήματα παρακολούθησης – όπως είναι το IDS (Intrusion detection system) – και οι ρυθμίσεις των router/switch, μπορούν να χρησιμοποιηθούν για την προστασία ενάντια στις επιθέσεις DoS.

Η επίθεση Man-in-the-Middle (MITM) γίνεται όταν η επικοινωνία ανάμεσα σε δύο συστήματα υποκλέπτεται από μια εξωτερική οντότητα. Αυτό μπορεί να συμβεί σε κάθε δίκτυο ή σε κάθε μορφή online επικοινωνίας, όπως είναι τα email, τα social media, το σερφάρισμα στο διαδίκτυο, οι online τραπεζικές υπηρεσίες κλπ.

Ο κοινός στόχος αυτών των επιθέσεων είναι η υποκλοπή προσωπικών πληροφοριών, όπως των στοιχείων ταυτοποίησης της σύνδεσής μας, τις πληροφορίες του λογαριασμού μας, τους αριθμούς των πιστωτικών καρτών μας, καθώς και κάθε άλλου ψηφιακού πόρου.

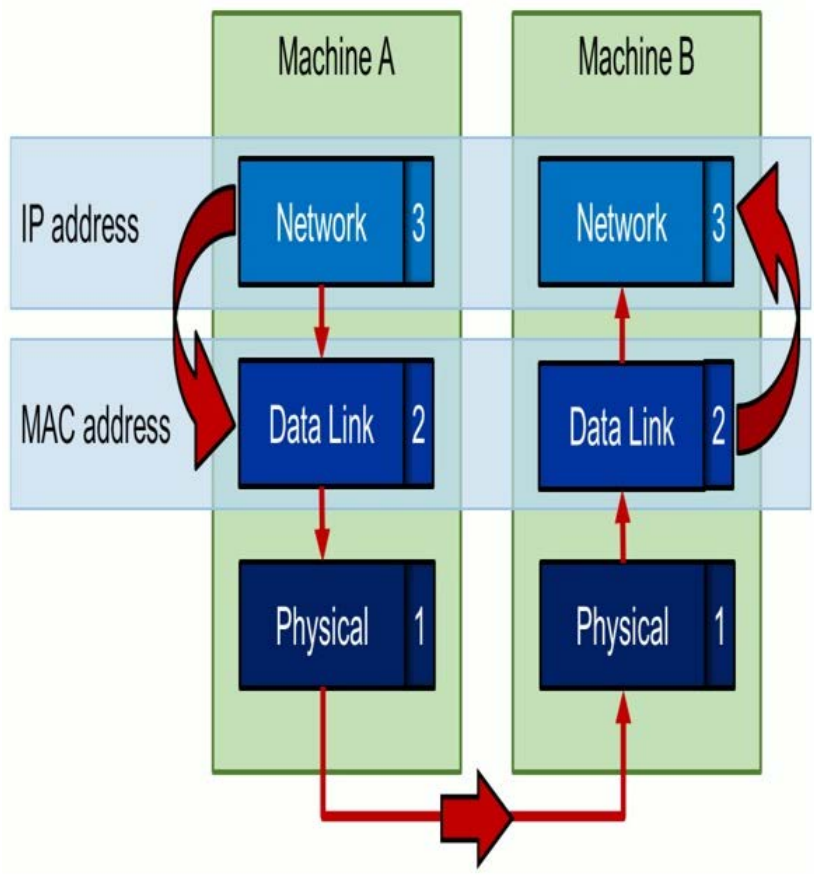
Το πρωτόκολλο protocol

Ο τρόπος λειτουργίας του πρωτοκόλλου ARP το αφήνει εκτεθειμένο σε επιθέσεις MiTM. Για να κατανοήσουμε την επίθεση, πρέπει να αποκτήσουμε κάποιες βασικές γνώσεις για το εν λόγω πρωτόκολλο.

Το πρωτόκολλο ARP (**Address Resolution Protocol) (πρωτόκολλο επίλυσης διευθύνσεων)**, βοηθάει τον εξυπηρετητή ενός δικτύου να μεταφράσει από τη διεύθυνση IP στη διεύθυνση MAC. Αυτό είναι κάτι που απαιτείται για να περάσουν δεδομένα από το Επίπεδο Δικτύου (επίπεδο 3) του μοντέλου OSI στο Επίπεδο Ζεύξης Δεδομένων (επίπεδο 2).

Ας πούμε ότι ο υπολογιστής Α θέλει να μεταφέρει δεδομένα στον υπολογιστή Β. Εστιάζοντας στα κατώτερα επίπεδα του μοντέλου OSI, βλέπουμε ότι θα έπρεπε να περάσει από το Επίπεδο Δικτύου, το Επίπεδο Ζεύξης Δεδομένων κι από το Φυσικό Επίπεδο (επίπεδο 1). Για να επικοινωνήσει το μηχάνημα Α με το μηχάνημα Β, το Α θα έπρεπε να γνωρίζει τη διεύθυνση IP του μηχανήματος Β, μια πληροφορία που είναι γνωστή στο Επίπεδο Δικτύου.

Το Επίπεδο Ζεύξης Δεδομένων επικοινωνεί χρησιμοποιώντας διευθύνσεις MAC. Άρα πρέπει να γίνει μετατροπή της διεύθυνσης IP του μηχανήματος Β σε διεύθυνση MAC (και το αντίθετο στον υπολογιστή-παραλήπτη). Αυτό απεικονίζεται στην παρακάτω εικόνα:



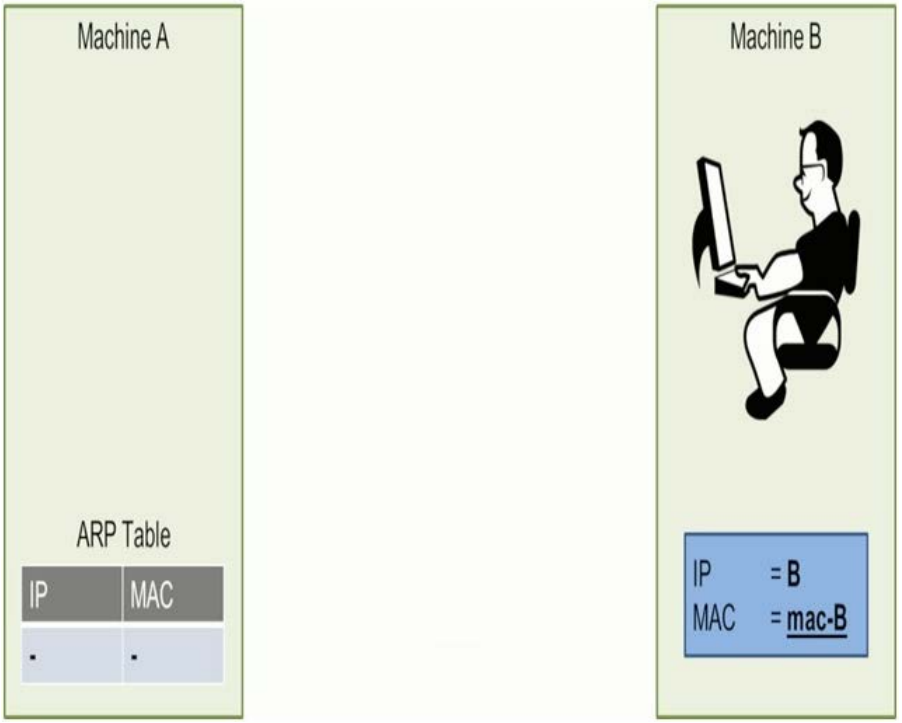
Εικόνα 2.20 Επίπεδα 1 ως 3 του μοντέλου OSI Πηγή

Επίπεδα 1 ως 3 του μοντέλου OSI

Η μετατροπή, ή μάλλον επίλυση, της διεύθυνσης IP σε διεύθυνση MAC (και το αντίστροφο) είναι το σημείο όπου εμπλέκεται το πρωτόκολλο ARP. Και τα δύο μηχανήματα θα έχουν έναν **πίνακα ARP,** με αποθηκευμένες τις διευθύνσεις IP και MAC όλων των γνωστών μηχανημάτων. Άρα πώς θα πάρει το μηχάνημα Α τη διεύθυνση MAC που αναλογεί στη διεύθυνση IP του μηχανήματος Β;

Το μηχάνημα Α απλά θα τη ζητήσει.

Μια απλοποίηση του πρωτοκόλλου ARP απεικονίζεται στην παρακάτω εικόνα:



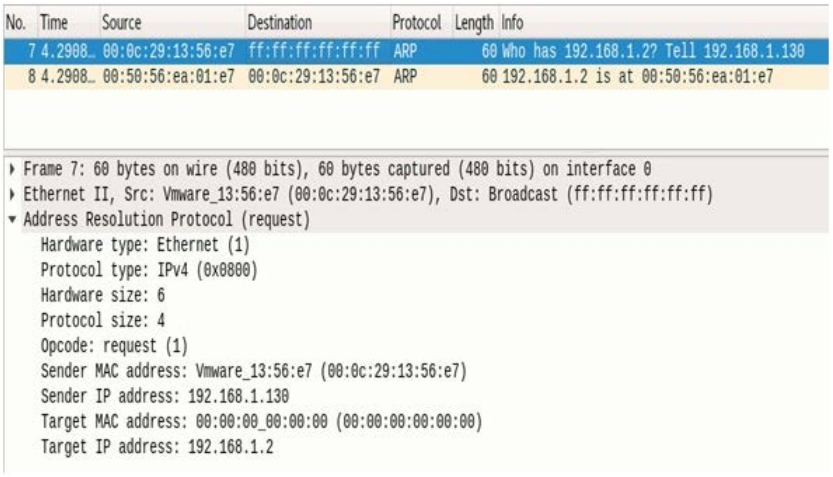
Εικόνα 2.21 Πρωτόκολλο ARP Πηγή

Σύνοψη των τριών βημάτων

1.Στο πρώτο βήμα του πρωτοκόλλου ARP, το μηχάνημα A στέλνει ένα **αίτημα ARP**. Είναι μια μετάδοση προς το δίκτυο με το ερώτημα "Ποιος έχει τη διεύθυνση MAC για τη διεύθυνση IP του μηχανήματος B;"
2.Το μηχάνημα B το γνωρίζει αυτό και στέλνει μια **απάντηση ARP, όπου δηλώνει** "Η διεύθυνση MAC του μηχανήματος B είναι η εξής (αναγράφει τη διεύθυνση)".
3.Το μηχάνημα A λαμβάνει την απάντηση ARP και γράφει (ή ενημερώνει) τα στοιχεία στον **πίνακα ARP**.

Στο τελευταίο βήμα βρίσκεται και το πρόβλημα αυτού του πρωτοκόλλου. Ωστόσο, προτού αναλύσουμε τα θέματά του, θα δούμε τα πακέτα ARP που μεταδίδονται στο δίκτυο.

Η παρακάτω εικόνα απεικονίζει τμήμα της κίνησης ενός δικτύου, όπως αποτυπώθηκε από το Wireshark.



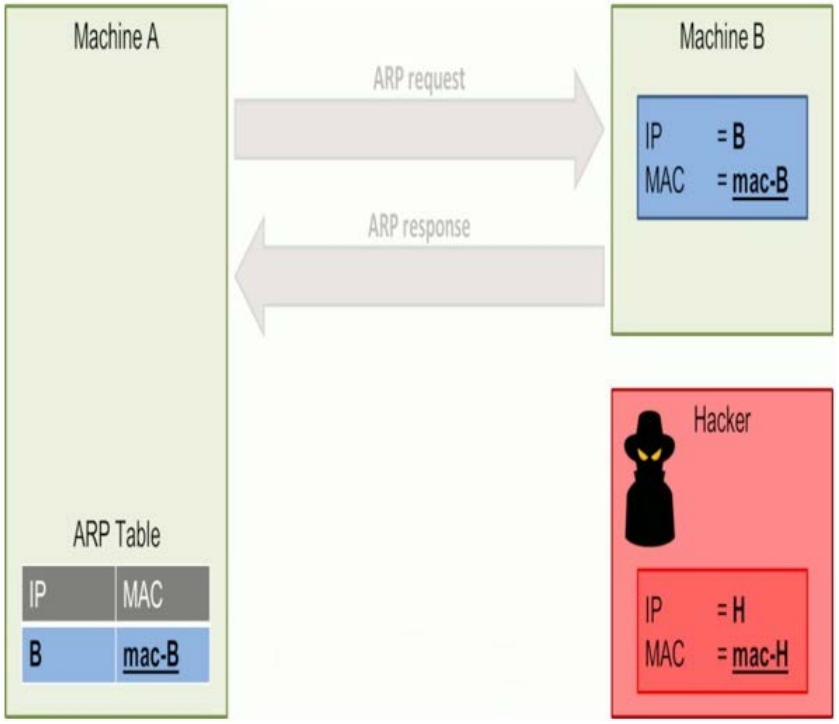
Εικόνα 2.22 ARP Κίνηση δικτύου ARP Πηγή

Παρατηρούμε την ύπαρξη δύο πακέτων, με τους αριθμούς 7 και 8.

- Το πρώτο πακέτο (7) εμπεριέχει το **αίτημα ARP** από έναν υπολογιστή με διεύθυνση MAC 00:0c:29:13:56:e7 προς έναν άλλο με διεύθυνση MAC ff:ff:ff:ff:ff:ff, άρα είναι μήνυμα μετάδοσης. Οπότε, εδώ η λογική είναι "Who has 192.168.1.2? Tell 192.168.1.130".
- Το δεύτερο πακέτο (8) είναι η **απάντηση ARP** από έναν υπολογιστή με διεύθυνση MAC 00:50:56:ea:01:e7 προς τη διεύθυνση MAC του αρχικού 7ου πακέτου. Το Wireshark ξέρει ότι η IP 192.168.1.2 έχει διεύθυνση MAC 00:50:56:ea:01:e7, που είναι η ίδια διεύθυνση MAC της πηγής του μηνύματος.

Το γεγονός ότι το μηχάνημα A ανανεώνει τον πίνακα ARP του με τις πληροφορίες από μια απάντηση ARP **χωρίς να αμφισβητεί την εγκυρότητα αυτής της πληροφορίας**, ανοίγει την πόρτα στο ARP spoofing (επίσης γνωστό κι ως **ARP poisoning**).

Ένας επιτιθέμενος μπορεί να στείλει μια κακόβουλη απάντηση ARP, χωρίς να έχει καν προηγηθεί αίτημα, που θα εμπεριέχει τη δική του διεύθυνση MAC και τη διεύθυνση IP ενός άλλου μηχανήματος. Το μηχάνημα στο οποίο έστειλε την απάντηση θα ανανεώσει χωρίς αμφισβήτηση τον πίνακα ARP του.



Εικόνα 2.23 Arp πλαστοπρωσοπεία(spoofing)Πηγή

Η παραπάνω εικόνα δείχνει το ίδιο σενάριο με πριν. Ωστόσο, τώρα έχει μπει κι ένας χάκερ στο δίκτυο μαζί με τα μηχανήματα A και B. Ο χάκερ έκανε τη δουλειά του στις φάσεις αναγνώρισης και σάρωσης, οπότε ξέρει ότι τα μηχανήματα A και B υπάρχουν στο δίκτυο, όπως επίσης ξέρει και τις διευθύνσεις IP τους.

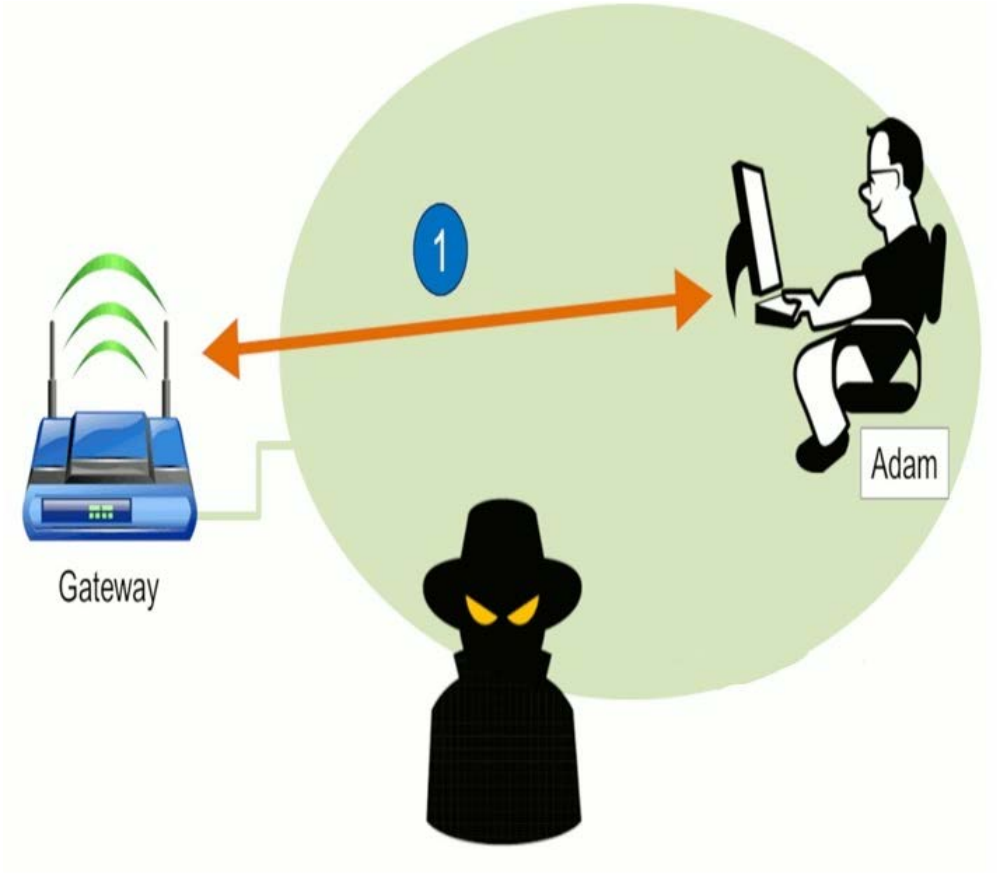
Σ' αυτό το παράδειγμα, ο χάκερ έχει διεύθυνση IP "H" και διεύθυνση MAC "mac-H". Στέλνει την κακόβουλη απάντηση ARP προς το μηχάνημα A με το μήνυμα "mac-H is the MAC-address of IP-address B". Το μηχάνημα A ανανεώνει τον πίνακα ARP του και η διεύθυνση IP του B είναι πια συνδεδεμένη με τη διεύθυνση MAC "H".

Από δω και πέρα, όποτε το μηχάνημα A θελήσει να στείλει μήνυμα στο B, θα μεταφράσει τη διεύθυνση IP του μηχανήματος B στη διεύθυνση MAC H και θα το στείλει στον χάκερ αντί για το μηχάνημα B.

Man-in-the-middle

Είδαμε πώς ένας επιτιθέμενος μπορεί να χρησιμοποιήσει κακόβουλο ARP για να κάνει ένα μηχάνημα να στείλει σ' αυτόν τα δεδομένα του αντί για τον σωστό προορισμό.

Ας υποθέσουμε ότι έχουμε το ακόλουθο σενάριο:



Εικόνα 2.24 Σενάριο arp spoofing Πηγή

Έχουμε μια προεπιλεγμένη πύλη δικτύου(gateway), έναν χάκερ και τον Αδάμ.

1. Ο Αδάμ συνδέεται στο δίκτυο. Ο επιτιθέμενος θα σαρώσει το δίκτυο για ν' ανακαλύψει ποιος άλλος είναι διαθέσιμος και τι διευθύνσεις IP και MAC έχει.

2. Τότε ο χάκερ στέλνει μια κακόβουλη απάντηση ARP στην πύλη δικτύου και στον Αδάμ. Στην ουσία, ο χάκερ λέει στην πύλη δικτύου ότι είναι ο Αδάμ και στον Αδάμ λέει ότι είναι η πύλη δικτύου.

3. Η πύλη δικτύου κι ο Αδάμ θα ενημερώσουν τους πίνακες ARP τους με τις νέες πληροφορίες. Εφεξής, θα στέλνουν τα δεδομένα τους στον χάκερ. Το ARP spoof ολοκληρώθηκε!

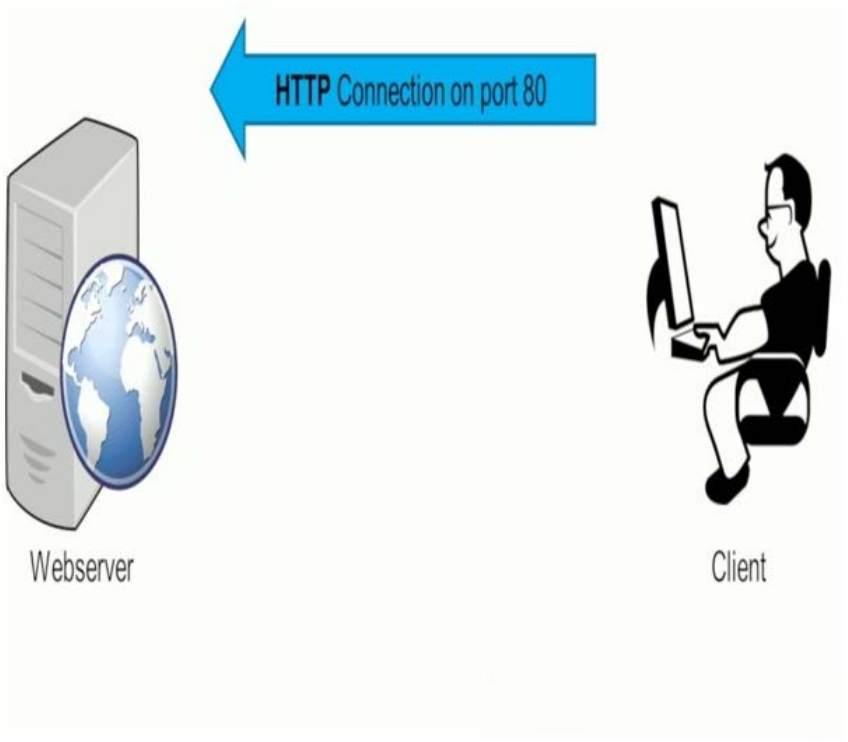
Ο επιτιθέμενος θα πρέπει να πάρει μερικά μέτρα προτού μπορέσει να υποκλέψει τα δεδομένα.

Σκεφτείτε το προηγούμενο σενάριο, όπου ο χάκερ είναι ανάμεσα στην πύλη δικτύου και τον Αδάμ. Ο χάκερ θα μπορεί να δει όλη την κίνηση και των δύο. Για παράδειγμα, αν ο Αδάμ ανοίξει μια ιστοσελίδα, ο χάκερ θα δει όλα τα δεδομένα λήψης και αποστολής προς αυτήν.

Τι γίνεται με το **HTTPS**? Αυτό είναι HTTP μέσω **TLS** (ή HTTP μέσω SSL). Σ' αυτό είναι κρυπτογραφημένα όλα τα δεδομένα της γραμμής, σωστά? Πράγματι, κι ακόμα δεν είναι εφικτή η αποκρυπτογράφηση σε ζωντανό χρόνο, οπότε ο χάκερ δε θα μπορεί να δει τα κρυπτογραφημένα περιεχόμενα της κίνησης HTTPS.

Η λύση: **εξαναγκάζει το θύμα να επικοινωνήσει μέσω HTTP**, που είναι αποκρυπτογραφημένο απλό κείμενο, αντί μέσω HTTPS.

Προτού εξηγήσω πώς γίνεται αυτό, ας δούμε πώς γίνεται μια συνεδρία HTTPS όταν πλοηγηθούμε στο www.google.com (για παράδειγμα):

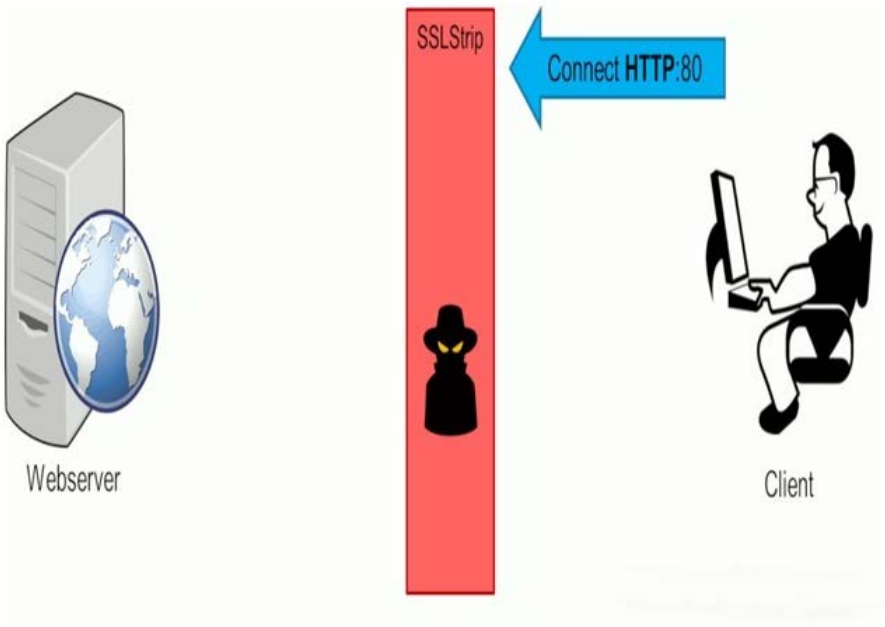


Εικόνα 2.25 Μια συνεδρία HTTPS Πηγή

Όταν πληκτρολογήσουμε www.google.com στον browser μας, αυτός θα συνδεθεί μέσω HTTP (στη θύρα 80) με το www.google.com. Δεδομένου ότι το google.com επιτρέπει μόνο συνδέσεις HTTPS, η σελίδα θα ζητήσει από τον χρήστη να χρησιμοποιήσει HTTPS και να επανασυνδεθεί μέσω της θύρας 443. Στο τελευταίο βήμα, η Google στέλνει το πιστοποιητικό.

Αναλογιστείτε το σενάριο όπου ο χάκερ βρίσκεται ανάμεσα στην επικοινωνία του σέρβερ με τον πελάτη. Ο χάκερ θα μπορεί να διαβάσει τα περιεχόμενα της κίνησης μέχρι τη στιγμή όπου ο πελάτης θα συνδεθεί μέσω HTTPS. Από εκεί και πέρα, όλα τα δεδομένα θα είναι κρυπτογραφημένα και δε θα είναι αναγνώσιμα από τον χάκερ. Νωρίτερα δηλώσαμε ότι αυτό μπορεί να παρακαμφθεί αναγκάζοντας τον πελάτη να συνεχίσει να επικοινωνεί μέσω HTTP. Θα χρησιμοποιήσουμε το SSLStrip για να το πετύχουμε αυτό.

Το SSLStrip, από τη Moxie Marlinspike, θα υφαρπάξει αόρατα την κίνηση HTTP ενός δικτύου, θα παρακολουθεί για συνδέσμους HTTPS κι ανακατευθύνσεις, και μετά θα χαρτογραφήσει αυτούς τους συνδέσμους είτε σε συνδέσμους HTTP που φαίνονται ολόιδιοι, ή σε ομόγραφους συνδέσμους HTTPS. Ας δούμε πώς γίνεται μια συνεδρία HTTPS, όταν ο χάκερ χρησιμοποιεί το SSLStrip ανάμεσα στον πελάτη και τον web server.



Εικόνα 2.26: SSLStrip Πηγή

Όπως και πριν, ο πελάτης πληκτρολογεί www.google.com στον browser, που θα επιχειρήσει να συνδεθεί μέσω HTTP με την ιστοσελίδα. Τώρα που είναι στη μέση το SSL Strip, η σύνδεση προωθείται στον επιθυμητό προορισμό. Ωστόσο, αντί να γίνει στον πελάτη η όλη ανακατεύθυνση προς HTTPS, το SSLStrip αναλαμβάνει να το κάνει στον υπολογιστή του χάκερ. Μετά το στήσιμο της σύνδεσης HTTPS, το SSLStrip θα στείλει **HTTP**-OK στον πελάτη. Ο browser του πελάτη νομίζει ότι αυτό είναι αποδεκτό, αφού δεν είδε ποτέ την ανακατεύθυνση σε HTTPS, οπότε και θα συνεχίσει να επικοινωνεί μέσω HTTP – μια μορφή που ο χάκερ μπορεί να διαβάσει αβίαστα.

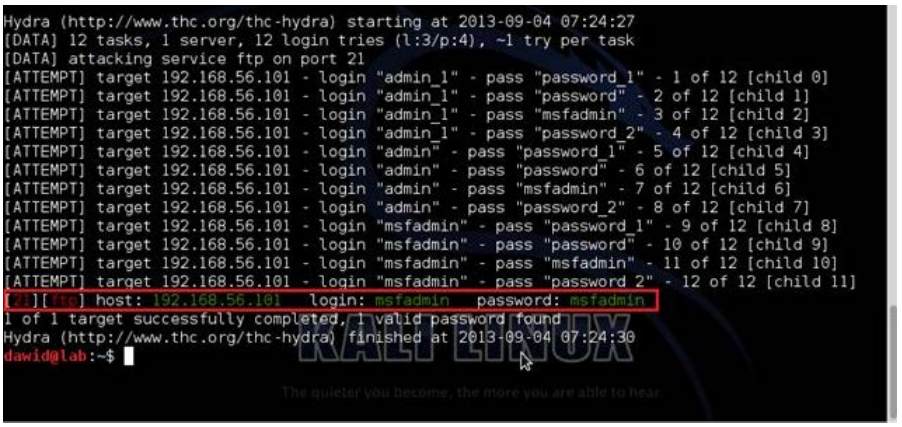
HTTP strict transport Security

Η ενεργοποίηση του HTTP strict transport security (HSTS) στην ιστοσελίδα σας, θα ενημερώσει τον browser να επικοινωνεί πάντα μέσω HTTPS. Αυτό γίνεται μέσω μιας ειδικής κεφαλίδας απάντησης HSTS. Με απλά λόγια, ο browser διατηρεί μια λίστα ιστοσελίδων από τις οποίες έλαβε αυτή την κεφαλίδα. Γι' αυτές τις ιστοσελίδες, ο browser θα ανοίξει αυτόματα μια σύνδεση HTTPS, ανεξαρτήτως του τρόπου που ο χρήστης προσπάθησε να συνδεθεί. Η πληκτρολόγηση του www.google.com δε θα ξεκινήσει έναν χορό ανακατευθύνσεων, αλλά θα καλέσει αυτόματα τη διεύθυνση www.google.com. Αυτό θα εμποδίσει τους χρήστες από το να συνδεθούν μέσω HTTP εξαρχής, αποφεύγοντας έτσι το SSLStrip και το κόλπο του. Φτάνει, βέβαια, να το υποστηρίζει ο browser σας.

Η πρωταρχική επίσκεψη ενός πελάτη σε μια ιστοσελίδα εξακολουθεί να μπορεί να γίνει μέσω HTTP κι ένας επιτιθέμενος μπορεί να υποκλέψει την κεφαλίδα HSTS από την απάντηση. Γι' αυτό κι οι περισσότεροι μοντέρνοι browsers έχουν φορτωμένη από πριν μια λίστα ιστοσελίδων HSTS. Στο τελευταίο κεφάλαιο θα δούμε περισσότερες πληροφορίες σχετικά με την αποτροπή.

Μια **επίθεση λεξικού** (**dictionary attack**) είναι μια επίθεση κωδικού, που επιχειρεί να βρει έναν κωδικό δοκιμάζοντας λέξεις από μια προκαθορισμένη λίστα ή λεξικό με πιθανούς κωδικούς.

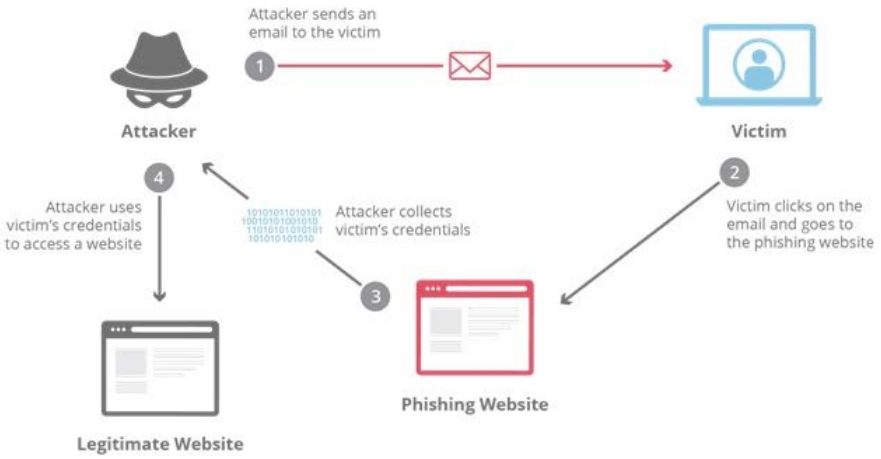
Η επίθεση λεξικού είναι η πιο απλή και γρήγορη επίθεση για την εύρεση ενός κωδικού. Χρησιμοποιεί ένα αρχείο με κοινές λέξεις, φράσεις ή κωδικούς, που ίσως έχουν χρησιμοποιηθεί από κάποιον ως κωδικοί. Οι χάκερς έχουν πρόσβαση σε βάσεις δεδομένων με 100,000 (ή και περισσότερους) κοινούς κωδικούς ή μπορούν να δημιουργήσουν και να βρουν μεγαλύτερα αρχεία. Η επίθεση συνοψίζει τους κωδικούς και συγκρίνει τις συνόψεις με τον κωδικό που θέλει να σπάσει. Αυτή η μέθοδος είναι ταχύτερη από άλλες.



Εικόνα 2.27: Επίθεση λεξικού

Phishing (Ηλεκτρονικό ψάρεμα)

Το Phishing αποτελεί παράδειγμα προσέγγισης κοινωνικής μηχανικής για την απόκτηση ευαίσθητων πληροφοριών (δεδομένα προσωπικής ταυτοποίησης), που συνήθως είναι usernames, passwords, αριθμοί πιστωτικών καρτών, πληροφορίες τραπεζικού λογαριασμού ή άλλα σημαντικά δεδομένα, για τη χρήση ή πώληση των κλεμμένων πληροφοριών. Αυτές θα χρησιμοποιηθούν με τη σειρά τους για να ξεγελάσουν συστήματα. Το Phishing συνήθως ξεκινάει με ένα email, που προσπαθεί να αποκτήσει ευαίσθητες πληροφορίες μέσω αλληλεπίδρασης με τον χρήστη, κάνοντάς τον να κάνει κλικ σε ένα κακόβουλο link ή να κατεβάσει μια μολυσμένη επισύναψη.



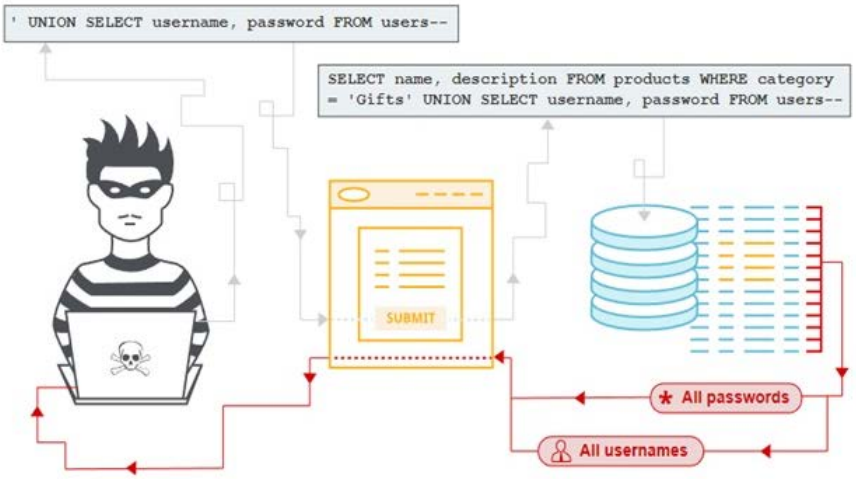
Εικόνα 2.28 Επίθεση phishing Πηγή

Για την αντιμετώπιση των επιθέσεων phishing, οι οργανισμοί κι οι εταιρείες πρέπει να δώσουν στους εργαζόμενους τρόπους αναγνώρισης τέτοιων επιθέσεων και αντίμετρα εναντίον τους. Οι πιο κοινές επιθέσεις phishing είναι emails, επισυναπτόμενα αρχεία με ιούς, καθώς και μολυσμένα links, που οδηγούν σε ιούς και ρίχνουν το bandwidth της σύνδεσης. Οι επιτιθέμενοι ενημερώνονται συνεχώς για τις νέες επιθέσεις, οπότε πρέπει να επιμορφώνετε συνεχώς τους εργαζόμενούς σας για να αποφύγετε τέτοιες επιθέσεις.

Το SQL Injection (SQLi) είναι ένας τύπος επίθεσης ένθεσης (injection attack), που δίνει τη δυνατότητα εκτέλεσης κακόβουλων εντολών SQL. Αυτές οι εντολές ελέγχουν έναν σέρβερ με βάση δεδομένων μέσω μιας διαδικτυακής εφαρμογής. Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τρωτά σημεία με το SQL Injection, για να παρακάμψουν τα μέτρα ασφάλειας. Παρακάμπτουν την ταυτοποίηση και την εξουσιοδότηση μιας ιστοσελίδας ή μιας διαδικτυακής εφαρμογής, και παίρνουν το περιεχόμενο ολόκληρης της βάσης δεδομένων SQL. Χρησιμοποιούν το SQL Injection και για να προσθέσουν, να τροποποιήσουν και να διαγράψουν αρχεία στη βάση δεδομένων.

Μια ευπάθεια σε SQL Injection μπορεί να επηρεάσει κάθε ιστοσελίδα ή εφαρμογή του web, που χρησιμοποιεί βάση δεδομένων SQL, όπως η **MySQL, Oracle, SQL Server, ή και άλλες**. Οι εγκληματίες μπορεί να τη χρησιμοποιήσουν για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στα ευαίσθητα δεδομένα σας: πληροφορίες πελατών, προσωπικά δεδομένα, εμπορικά μυστικά, πνευματική ιδιοκτησία κλπ. Οι επιθέσεις SQL Injection είναι από τις πιο παλιές, πιο συνηθισμένες και πιο επικίνδυνες ευπάθειες των διαδικτυακών εφαρμογών. Επιτρέπουν στον επιτιθέμενο να δει δεδομένα, που κανονικά δε θα μπορούσε να αποκτήσει. Αυτά ίσως είναι δεδομένα άλλων χρηστών, ή και κάθε είδους δεδομένα στα οποία έχει πρόσβαση η εφαρμογή. Σε πολλές περιπτώσεις, ένας επιτιθέμενος μπορεί **να τροποποιήσει** ή **να διαγράψει** αυτά τα δεδομένα, προκαλώντας μόνιμες αλλαγές στο περιεχόμενο ή στη συμπεριφορά της εφαρμογής.

Σε ορισμένες περιπτώσεις, ένας επιτιθέμενος μπορεί να κλιμακώσει μια επίθεση SQL injection, για να θέσει σε κίνδυνο τον υποκείμενο σέρβερ ή την υποδομή στο back-end, ή και για να κάνει μια επίθεση denial-of-service.



Εικόνα 2.29 SQL injection Πηγή

Παράγοντες για την κάθε βάση δεδομένων

Μερικές πηγαίες δυνατότητες της γλώσσας SQL ενσωματώνονται με τον ίδιο τρόπο σε δημοφιλείς πλατφόρμες βάσεων δεδομένων, οπότε πολλοί τρόποι ανίχνευσης κι εκμετάλλευσης ευπαθειών σε SQL injection λειτουργούν ολόιδια σε διαφορετικούς τύπους βάσεων δεδομένων.

Ωστόσο, υπάρχουν και πολλές διαφορές στις κοινές βάσεις δεδομένων. Αυτές σημαίνουν ότι μερικές τεχνικές ανίχνευσης κι εκμετάλλευσης του SQL injection λειτουργούν διαφορετικά στις διάφορες πλατφόρμες.

Τι μπορούν να κάνουν οι επιθέσεις SQL Injection?

Ένας επιτιθέμενος μπορεί να κάνει πολλά με το SQL injection σε μια ευπαθή ιστοσελίδα. Χρησιμοποιώντας μια ευπάθεια σε SQL injection, και υπό τις κατάλληλες συνθήκες, ένας επιτιθέμενος μπορεί να κάνει τα ακόλουθα:

- Να παρακάμψει τους μηχανισμούς ταυτοποίησης μιας εφαρμογής του web και να εξαγάγει ευαίσθητα δεδομένα
- Να ελέγξει εύκολα τη συμπεριφορά της εφαρμογής, που βασίζεται σε δεδομένα της βάσης
- Να προσθέσει περαιτέρω κακόβουλο κώδικα, που θα εκτελεστεί με την πρόσβαση των χρηστών στην εφαρμογή
- Να προσθέσει, τροποποιήσει και διαγράψει δεδομένα, αλλοιώνοντας τη βάση δεδομένων κι αχρηστεύοντας την εφαρμογή
- Να πάρει τα στοιχεία ταυτοποίησης ενός χρήστη που είναι εγγεγραμμένος σε μια ιστοσελίδα και να χρησιμοποιήσει τα δεδομένα για επιθέσεις σε άλλες σελίδες

Εικόνα 2.30 Επιθέσεις Sql injection Πηγή

Τα ακόλουθα πράγματα μπορεί να προκύψουν από το SQL injection:

- Το χακάρισμα του λογαριασμού κάποιου ατόμου.
- Η κλοπή κι η αντιγραφή των ευαίσθητων δεδομένων της ιστοσελίδας ή του συστήματος.
- Η αλλαγή των ευαίσθητων δεδομένων του συστήματος.
- Η διαγραφή των ευαίσθητων δεδομένων του συστήματος.
- Ο χρήστης μπορεί να συνδεθεί στην εφαρμογή ως άλλος χρήστης, ή ακόμα κι ως διαχειριστής.
- Ο χρήστης μπορεί να δει προσωπικές πληροφορίες που ανήκουν σε άλλους χρήστες – τις πληροφορίες των προφίλ τους, τις πληροφορίες των συναλλαγών τους κλπ.
- Ο χρήστης μπορεί να αλλάξει τις πληροφορίες ρύθμισης της εφαρμογής και τα δεδομένα των άλλων χρηστών.
- Ο χρήστης μπορεί να τροποποιήσει τη δομή της βάσης δεδομένων, ακόμα και να διαγράψει πίνακες από τη βάση δεδομένων της εφαρμογής.
- Ο χρήστης μπορεί να πάρει τον έλεγχο του σέρβερ της βάσης δεδομένων και να εκτελέσει εντολές όποτε το θελήσει.

Εικόνα 2.31 Αποτροπή του SQL injection Πηγή

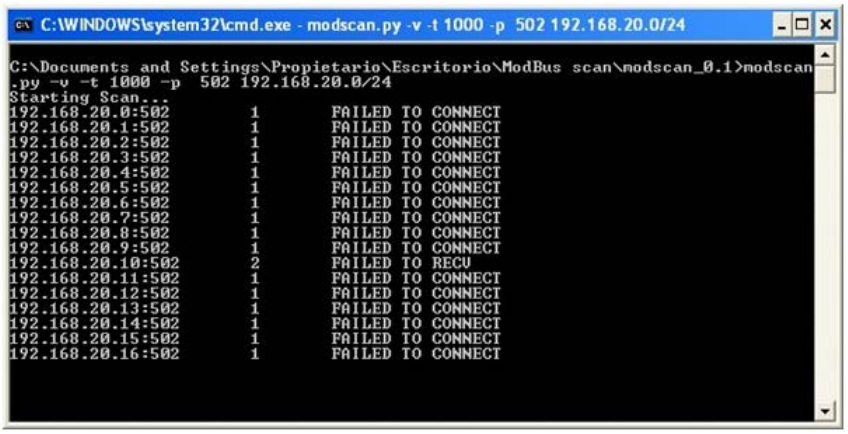
Υπάρχουν πολλοί τρόποι για την αντιμετώπιση των επιθέσεων SQL injection, ώστε να είστε καλύτερα προετοιμασμένοι και να αποφύγετε την πιθανή ζημιά που μπορεί να πάθετε. Μερικοί τρόποι είναι:

- Η ανακάλυψη των ευπαθειών σε SQL injection μέσω των διάφορων τεχνικών που είναι διαθέσιμες γι' αυτό το είδος επίθεσης.
- Η επισκευή των ευπαθειών σε SQL injection μέσω της χρήσης παραμετροποιημένων ερωτημάτων. Η βάση δεδομένων θα τους φέρεται πάντα ως δεδομένα αντί για τμήμα μιας εντολής SQL.
- Η αποκατάσταση των ευπαθειών σε SQL injection μέσω της χρήσης χαρακτήρων διαφυγής (escape characters), ώστε να αγνοηθούν οι ειδικοί χαρακτήρες.
- Η μετρίαση της επίδρασης των ευπαθειών σε SQL injection δια της επιβολής ελάχιστων προνομίων στη βάση δεδομένων. Με αυτό τον τρόπο, κάθε τμήμα του λογισμικού μιας εφαρμογής μπορεί να αποκτήσει πρόσβαση και να επηρεάσει μόνο τους πόρους που χρειάζεται.
- Η χρήση τείχους προστασίας διαδικτυακής εφαρμογής (Web Application Firewall) (WAF) για διαδικτυακές εφαρμογές που έχουν πρόσβαση σε βάσεις δεδομένων. Αυτό βοηθά στην αναγνώριση των αποπειρών επίθεσης SQL injection και μερικές φορές βοηθάει στο να εμποδιστούν και να μη φτάσουν στην εφαρμογή.

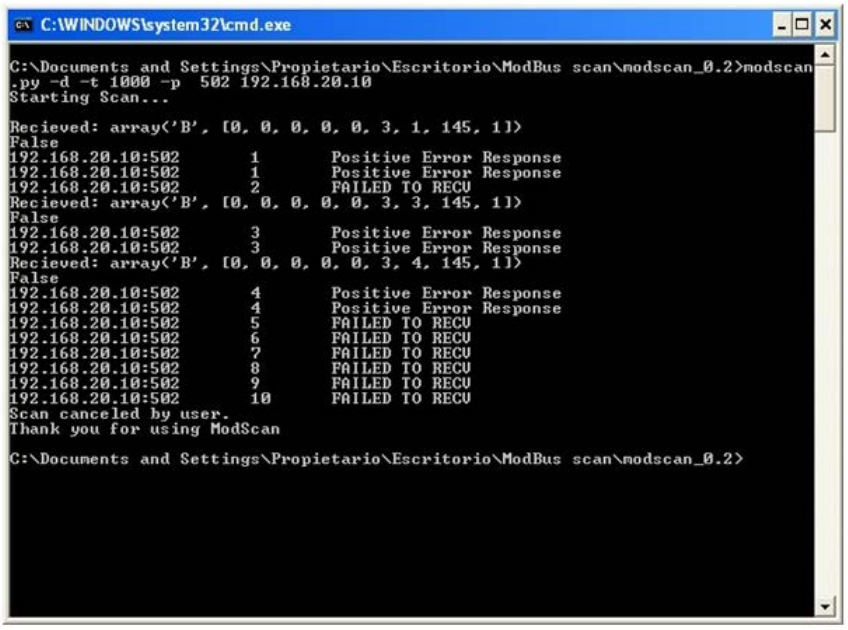
Το Modbus είναι ένα διαδεδομένο βιομηχανικό πρωτόκολλο επικοινωνίας με προδιαγραφές που είναι δημόσια διαθέσιμες (βασίζεται σε αρχιτεκτονική master/slave). Αυτήν τη στιγμή δεν υπάρχουν εκτενείς περιορισμοί στον χρόνο διαχείρισης των μπλοκ δεδομένων ενός βιομηχανικού συστήματος. Αυτό θα μπορούσε να ενσωματωθεί πολύ απλά και θα χρειαζόταν ελάχιστη ανάπτυξη. Αυτήν τη στιγμή υπάρχουν δύο υλοποιήσεις: Το Modbus series (με τρόπο λειτουργίας ASCII και RTU) και το Modbus/TCP.

Αδυναμίες πρωτοκόλλου

Στο Modbus, το μοτίβο λειτουργίας του στοιχείου slave επιβάλει την αποστολή απάντησης για κάθε πακέτο που παραλαμβάνει.Το εργαλείο Modscan εκμεταλλεύεται αυτήν τη δυνατότητα, κατευθύνει τα αιτήματα TCP (άρα κι είναι διαθέσιμο μόνο σε υλοποιήσεις Modbus/TCP) στην τυπική θύρα του Modbus, την 502, κι έτσι ανακαλύπτει τους slaves που είναι συνδεδεμένοι στο δίκτυο, όπως φαίνεται και στην παρακάτω εικόνα.

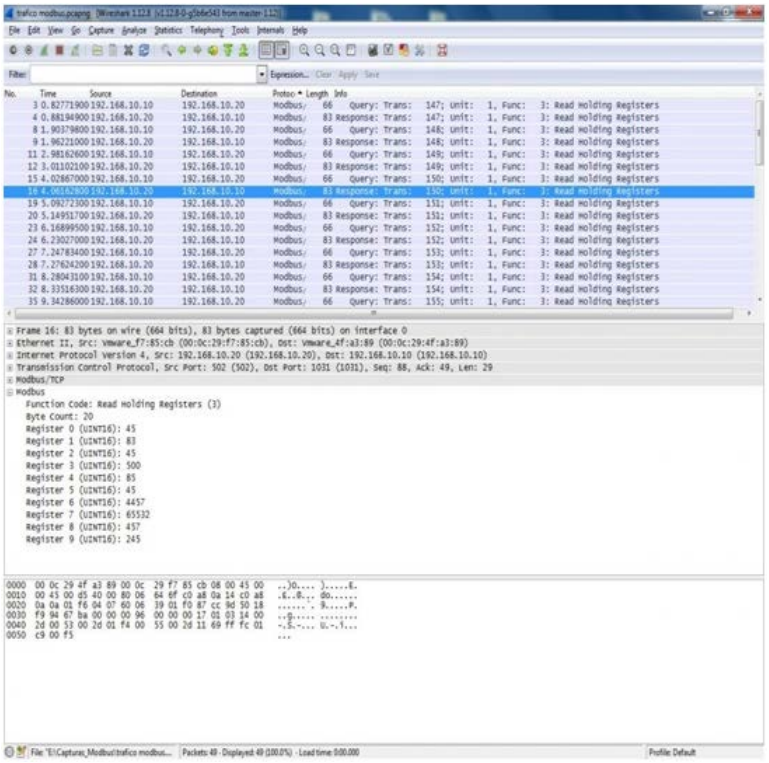


Εικόνα 2.32 Ανακαλύπτοντας τις διευθύνσεις IP των Modbus slaves μέσω του Modscan



Εικόνα 2.33 Βελτιστοποιώντας την αναζήτηση για slaves και την ταυτοποίηση των Modbus IDs

Μετά την αναγνώριση των slaves, είναι εύκολη η υποκλοπή της κίνησης με οποιοδήποτε εργαλείο που σχεδιάστηκε για την υποκλοπή της κίνησης ενός δικτύου. Η ανάλυση υποκλοπής δείχνει ότι οι επικοινωνίες δεν είναι κρυπτογραφημένες, άρα είναι πιθανή η αναγνώριση και η απευθείας ανάλυση των πληροφοριών και του μοτίβου λειτουργίας. Η παρακάτω εικόνα δείχνει την υποκλοπή κίνησης με ανάλυση της ροής δεδομένων.



Εικόνα 2.34 Ανάλυση κίνησης

Οι αδυναμίες του Modbus πηγάζουν από τις προδιαγραφές του, άρα και είναι αναπόσπαστες από το πρωτόκολλο. Αφού δεν αναμένονται αλλαγές στις προδιαγραφές, είναι απαραίτητη η εισαγωγή επιπρόσθετων στοιχείων ασφάλειας, για τον μετριασμό των ελαττωμάτων του.

Πέραν από αυτή την επιλογή, που είναι κι η πιο απλή, το πρώτο μέτρο που μπορούμε να σκεφτούμε είναι η υιοθέτηση μιας στρατηγικής κρυπτογράφησης για τις επικοινωνίες. Η κρυπτογράφηση των επικοινωνιών θα εμποδίσει την ανάλυση των πληροφοριών εν κινήσει, για την περίπτωση που υποκλαπούν.

Οι συσκευές που ενσωματώνουν αυτό το πρωτόκολλο συνήθως δεν μπορούν να κρυπτογραφήσουν τις επικοινωνίες, άρα πρέπει να χρησιμοποιηθούν εξωτερικά εργαλεία, που μπορούν να κρυπτογραφήσουν και ν' αποκρυπτογραφήσουν τις πληροφορίες που μεταφέρονται μέσω του καλωδίου Ethernet.

Αν κι είναι αποτελεσματική αυτή η λύση, είναι δύσκολη πρακτικά, αφού η χρήση εργαλείων κρυπτογράφησης φέρνει προβλήματα στη διαχείριση και τη διανομή κωδικών. Επιπλέον, η κρυπτογράφηση κι αποκρυπτογράφηση πληροφοριών πρέπει να επιτρέπεται απ' όλο τον βιομηχανικό εξοπλισμό για να χρησιμοποιηθεί από το πρωτόκολλο Modbus.

Επομένως, για να ελέγξουμε την κίνηση ανάμεσα στους slaves και τον master χρησιμοποιούμε τείχη προστασίας, που είναι κι η πιο δημοφιλής επιλογή. Τα συμβατικά τείχη προστασίας επιτρέπουν τον έλεγχο της κίνησης στο επίπεδο δικτύου, άρα οι διευθύνσεις του master και των slaves μπορούν να καθοριστούν ως έγκυρες, εμποδίζοντας ορισμένα είδη επιθέσεων πλαστοπροσωπίας. Τα τείχη προστασίας εφαρμογών επιτρέπουν την επιθεώρηση, συμπεριλαμβάνοντας όλα τα τμήματα δεδομένων της ροής.

Υπάρχει το Modbusfw, ένα module για iptables που φιλτράρει την κίνηση στο επίπεδο εφαρμογών για την ασφάλιση των δικτύων μέσω της χρήσης του πρωτοκόλλου Modbus/TCP. Επιτρέπει το φιλτράρισμα των πακέτων κίνησης του Modbus, που αναγνωρίζονται από το ID του slave, τον κώδικα λειτουργίας, το μέγεθος του πακέτου ή τον αριθμό αναφοράς. Με αυτό τον τρόπο μπορεί να αποφευχθεί η εγγραφή σε εξοπλισμό που θα έπρεπε να γίνονται μόνο αναγνώσεις, ή και το αντίθετο, ενώ μπορεί να γίνει και φιλτράρισμα της χρήσης διαγνωστικών κωδικών λειτουργίας (όπως αυτοί που χρησιμοποιούνται σε συγκεκριμένα εργαλεία σάρωσης δικτύου Modbus) κλπ.

Τα τείχη προστασίας επιτρέπουν τον έλεγχο κίνησης σε διαφορετικά δίκτυα, αλλά είναι χρήσιμο να χρησιμοποιούνται συνδυαστικά με συστήματα εντοπισμού κι αποτροπής εισβολής (intrusion detection and prevention systems) (IDS/IPS) για τον εντοπισμό δράσεων άλλου είδους.

Για το Snort IDS, καθώς και για όσα βασίζονται σε αυτό, υπάρχει μια επέκταση (extension) για τη διερμηνεία του πρωτοκόλλου Modbus. Υπάρχει η δυνατότητα να καθοριστούν κανόνες ελέγχου κίνησης για το Modbus, που θα βασίζονται σε τιμές που πρέπει να εμπεριέχουν διαφορετικά bytes δεδομένων σε μια ροή Modbus/TCP.

Η χρήση συστημάτων IDS/IPS για την επίβλεψη του πρωτοκόλλου Modbus επιτρέπει την αναγνώριση της χρήσης μη επιτρεπτών λειτουργιών, καθώς και την αναγνώριση της αποστολής πακέτων δεδομένων από μη ελεγχόμενες διευθύνσεις IP, βοηθώντας έτσι στον εντοπισμό πιθανών επιθέσεων DoS.

2.4 Νόμος Υπηρεσιών της Πληροφορίας και Ηλεκτρονικό Εμπόριο

Description

Η οδηγία 2000/31/EC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου του 2000 αφορά σε ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας. Πιο συγκεκριμένα, αφορά στο ηλεκτρονικό εμπόριο στην Ενιαία Αγορά (οδηγία για το ηλεκτρονικό εμπόριο).

Ορισμένες παράγραφοι του νόμου:

- Προκειμένου να εξασφαλιστούν η ασφάλεια δικαίου και η εμπιστοσύνη του καταναλωτή, η παρούσα οδηγία πρέπει να καθορίζει ένα σαφές γενικό πλαίσιο, που να καλύπτει ορισμένες νομικές πτυχές του ηλεκτρονικού εμπορίου στην εσωτερική αγορά.

- Η ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας μπορεί σε πολλές περιπτώσεις να αντικατοπτρίζει στο κοινοτικό δίκαιο, κατά τρόπο συγκεκριμένο, μια γενικότερη αρχή, ήτοι την ελευθερία έκφρασης, όπως κατοχυρώνεται στο άρθρο 10 παράγραφος 1 της σύμβασης για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, την οποία έχουν επικυρώσει όλα τα κράτη μέλη. Για το λόγο αυτό, οι οδηγίες που καλύπτουν την παροχή υπηρεσιών της πληροφορίας πρέπει να εξασφαλίζουν ότι μπορεί κανείς να επιδίδεται στην εν λόγω δραστηριότητα ελεύθερα βάσει του ως άνω άρθρου, με μόνη επιφύλαξη τους περιορισμούς που ορίζει η παράγραφος 2 του εν λόγω άρθρου και το άρθρο 46 παράγραφος 1 της συνθήκης. Η παρούσα οδηγία δεν έχει σκοπό να θίξει τους εθνικούς θεμελιώδεις κανόνες και αρχές που αφορούν την ελευθερία την έκφρασης.

Ολόκληρος ο επίσημος νόμος:

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN

Υπηρεσίες της κοινωνίας της πληροφορίας Σκοπός του νόμου

Ο νόμος παρέχει τις προϋποθέσεις για τους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας, τους οργανισμούς που αναλαμβάνουν την επίβλεψη και την ευθύνη για τις παραβιάσεις αυτού του νόμου.

Περισσότερες πληροφορίες για τον νόμο http://unpan1.un.org/intradoc/groups/public/documents/un-kmb/unpan041622~1.htm

E-commerce – Τυπικοί ευρωπαϊκοί κανονισμοί

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=LEGISSUM%3Al24204

Η Ντιρεκτίβα Ηλεκτρονικού Εμπορίου (e-Commerce Directive 2000/31/EC), που υιοθετήθηκε το 2000, στήνει ένα πλαίσιο Ενιαίας Αγοράς για το ηλεκτρονικό εμπόριο, που προσφέρει νομική σιγουριά τόσο στις επιχειρήσεις, όσο και στους καταναλωτές.

- Προκειμένου να εξασφαλιστούν η ασφάλεια δικαίου και η εμπιστοσύνη του καταναλωτή, η παρούσα οδηγία πρέπει να καθορίζει ένα σαφές γενικό πλαίσιο, που να καλύπτει ορισμένες νομικές πτυχές του ηλεκτρονικού εμπορίου στην εσωτερική αγορά.

Table of contents

Η οδηγία 2000/31/EC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου του 2000 αφορά σε ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας. Πιο συγκεκριμένα, αφορά στο ηλεκτρονικό εμπόριο στην Ενιαία Αγορά (οδηγία για το ηλεκτρονικό εμπόριο).

Ορισμένες παράγραφοι του νόμου:

- Προκειμένου να εξασφαλιστούν η ασφάλεια δικαίου και η εμπιστοσύνη του καταναλωτή, η παρούσα οδηγία πρέπει να καθορίζει ένα σαφές γενικό πλαίσιο, που να καλύπτει ορισμένες νομικές πτυχές του ηλεκτρονικού εμπορίου στην εσωτερική αγορά.
- Η ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας μπορεί σε πολλές περιπτώσεις να αντικατοπτρίζει στο κοινοτικό δίκαιο, κατά τρόπο συγκεκριμένο, μια γενικότερη αρχή, ήτοι την ελευθερία έκφρασης, όπως κατοχυρώνεται στο άρθρο 10 παράγραφος 1 της σύμβασης για την προστασία των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών, την οποία έχουν επικυρώσει όλα τα κράτη μέλη. Για το λόγο αυτό, οι οδηγίες που καλύπτουν την παροχή υπηρεσιών της πληροφορίας πρέπει να εξασφαλίζουν ότι μπορεί κανείς να επιδίδεται στην εν λόγω δραστηριότητα ελεύθερα βάσει του ως άνω άρθρου, με μόνη επιφύλαξη τους περιορισμούς που ορίζει η παράγραφος 2 του εν λόγω άρθρου και το άρθρο 46 παράγραφος 1 της συνθήκης. Η παρούσα οδηγία δεν έχει σκοπό να θίξει τους εθνικούς θεμελιώδεις κανόνες και αρχές που αφορούν την ελευθερία την έκφρασης.

Υπηρεσίες της κοινωνίας της πληροφορίας και σκοπός του νόμου

(1) Ο νόμος παρέχει τις προϋποθέσεις για τους παρόχους υπηρεσιών της κοινωνίας της πληροφορίας, τους οργανισμούς που αναλαμβάνουν την επίβλεψη και την ευθύνη για τις παραβιάσεις αυτού του νόμου.

Περισσότερες πληροφορίες για τον νόμο
http://unpan1.un.org/intradoc/groups/public/documents/un-kmb/unpan041622~1.htm

E-commerce – Τυπικοί ευρωπαϊκοί κανονισμοί

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=LEGISSUM%3Al24204

Η Ντιρεκτίβα Ηλεκτρονικού Εμπορίου (e-Commerce Directive 2000/31/EC), που υιοθετήθηκε το 2000, στήνει ένα πλαίσιο Ενιαίας Αγοράς για το ηλεκτρονικό εμπόριο, που προσφέρει νομική σιγουριά τόσο στις επιχειρήσεις, όσο και στους καταναλωτές.

Σκοπός της Ντιρεκτίβας ηλεκτρονικού εμπορίου

Η Ντιρεκτίβα θεσμοθετήθηκε για την αποσαφήνιση και τον εναρμονισμό των κανονισμών των online επιχειρήσεων σε όλη την Ευρώπη. Στόχος της Ντιρεκτίβας είναι να ενθαρρύνει τη μεγαλύτερη χρήση του ηλεκτρονικού εμπορίου γκρεμίζοντας τα φράγματα που υπάρχουν σε όλη την Ευρώπη, καθώς και να δώσει σιγουριά στους καταναλωτές μέσα από την αποσαφήνιση των δικαιωμάτων και των υποχρεώσεων τόσο των καταναλωτών, όσο και των επιχειρήσεων.

Αντικείμενο των Κανονισμών Ηλεκτρονικού Εμπορίου (Ντιρεκτίβα ΕC) 2002

Οι Κανονισμοί Ηλεκτρονικού Εμπορίου (Ντιρεκτίβα ΕC) 2002, που τέθηκαν σε ισχύ στις 21 Αυγούστου του 2002, μεταθέτουν τις κύριες προϋποθέσεις της Ντιρεκτίβας Ηλεκτρονικού Εμπορίου στο Αγγλικό Δίκαιο.

Οι Κανονισμοί αφορούν στις «υπηρεσίες της κοινωνίας της πληροφορίας». «Ο εν λόγω ορισμός καλύπτει κάθε υπηρεσία που συνήθως παρέχεται εξ αποστάσεως έναντι αμοιβής, μέσω εξοπλισμών ηλεκτρονικής επεξεργασίας (συμπεριλαμβανομένης της ψηφιακής συμπίεσης) και αποθήκευσης δεδομένων και κατόπιν ατομικού αιτήματος του αποδέκτη της υπηρεσίας».

Αυτό συμπεριλαμβάνει τους περισσότερους τύπους online υπηρεσιών και υπηρεσιών πληροφόρησης, όπως είναι οι:

- Η online διαφήμιση αγαθών ή υπηρεσιών (δηλαδή μέσω internet, email, διαδραστικής τηλεόρασης ή κινητού τηλεφώνου)
- Η πώληση αγαθών ή υπηρεσιών στο διαδίκτυο ή μέσω email, ασχέτως του αν τα αγαθά ή οι υπηρεσίες παραδίδονται

ηλεκτρονικά

- Η μετάδοση ή η αποθήκευση ηλεκτρονικού περιεχομένου ή η παροχή πρόσβασης σε ένα δίκτυο επικοινωνιών

Ολόκληρος ο επίσημος νόμος:

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN

Οι συστάσεις της Ευρωπαϊκής Ένωσης για την καταπολέμηση των ψηφιακών επιθέσεων (cyberattacks). Ισχύουν οι ακόλουθες οδηγίες:

- Μελέτη της ENISA: "ΨΗΦΙΑΚΗ ΑΣΦΑΛΕΙΑ ΒΙΟΜΗΧΑΝΙΑΣ 4.0: ΠΡΟΚΛΗΣΕΙΣ & **ΠΡΟΤΑΣΕΙΣ, Μάιος 2019"**: https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport

Η ιδιοποίηση των προτάσεων της ENISA στοχεύει στη βελτίωση της ψηφιακής ασφάλειας της Βιομηχανίας 4.0 σε όλη την Ευρωπαϊκή Ένωση, στο να βάλει θεμέλια για την επερχόμενη δουλειά, καθώς και στο να αποτελέσει τη βάση για τις μελλοντικές εξελίξεις. Σε αυτήν τη σύντομη μελέτη, η ENISA διερευνά έναν ολιστικό και αναλυτικό τρόπο αντιμετώπισης των θεμάτων ψηφιακής ασφάλειας (cybersecurity) στη Βιομηχανία 4.0, όπου οι δυσκολίες κι οι προτάσεις σχετίζονται με μία από τις ακόλουθες τάξεις: Άνθρωποι, Διεργασίες και Τεχνολογίες.

- **Αυτή η μελέτη στοχεύει στις "Οδηγίες Ψηφιακής Ασφάλειας και Καλύτερες Πρακτικές για Υπηρεσίες Έκτακτης Ανάγκης, Ιούνιος 2018"**: https://eena.org/wp-content/uploads/2018/11/Cybersecurity-Guidelines-and-Best-Practices-for-Emergency-Services.pdf

Αυτή η μελέτη της EENA (European Emergency Number Association) (Ευρωπαϊκός Οργανισμός Αριθμού Έκτακτης Ανάγκης) θέλει να επιστήσει την προσοχή των Οργανισμών Δημόσιας Ασφάλειας στην επίδραση των ψηφιακών ευπαθειών, ρίσκων κι απειλών, οπότε και δίνει μερικές προτάσεις για τη μετρίασή τους. Η ψηφιακή ασφάλεια, για τους σκοπούς αυτού του εγγράφου, αναφέρεται στις τεχνολογίες, στις διεργασίες και στις πρακτικές που σχεδιάστηκαν για την προστασία χρηστών, δικτύων, υπολογιστών, προγραμμάτων και δεδομένων από επίθεση, ζημιά ή μη εξουσιοδοτημένη πρόσβαση.

- **ISACA, "Έλεγχος ψηφιακής ασφάλειας"**: https://m.isaca.org/About-ISACA/advocacy/Documents/CyberSecurityAudit_mis_Eng_1017.pdf

Αυτός ο οδηγός εστιάζει σε τρία μέρη: διευθυντικό έλεγχο, εκτιμήσεις ρίσκου κι ελέγχους των συστημάτων ελέγχου ψηφιακής ασφάλειας. Επιπλέον, συμπεριλαμβάνει πρωτεύοντα θέματα ασφάλειας, ελέγχου κι απειλών για την ψηφιακή ασφάλεια.

- **Αυτή η μελέτη της ENISA εστιάζει στις "Καλές Πρακτικές για την Ασφάλεια του Διαδικτύου των Πραγμάτων (Internet of Things) (IoT), σε σχέση με την Έξυπνη Παραγωγή, Νοέμβριος 2018"**: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport

Αυτή η μελέτη της ENISA στοχεύει στην αντιμετώπιση των προκλήσεων ασφάλειας κι ιδιωτικότητας, που σχετίζονται με την εξέλιξη των βιομηχανικών συστημάτων κι υπηρεσιών, όπως αυτές παρουσιάστηκαν με την εισαγωγή των καινοτομιών IoT. Οι κύριοι στόχοι ήταν η συλλογή καλών πρακτικών για τη διασφάλιση της ασφάλειας του Διαδικτύου των Πραγμάτων στο πλαίσιο της Βιομηχανίας 4.0/Έξυπνης Παραγωγής, καθώς κι η χαρτογράφηση των σχετικών προκλήσεων, απειλών, ρίσκων κι επιθετικών σεναρίων κατά της ασφάλειας κι ιδιωτικότητας.

- **Εσωτερική Αναφορά 8228 του NIST (Draft) "Προβληματισμοί για τη Διαχείριση της Ψηφιακής Ασφάλειας του Διαδικτύου των Πραγμάτων (IoT) και Κίνδυνοι Ιδιωτικότητας, Σεπτέμβριος 2019"**: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf

Σκοπός αυτής της μελέτης είναι να βοηθήσει τις επιχειρήσεις να καταλάβουν και να χειριστούν τους κινδύνους στην ψηφιακή ασφάλεια και στην ιδιωτικότητα , που σχετίζονται με τις συσκευές του Διαδικτύου των Πραγμάτων (IoT). Επιπλέον, το κείμενο μιλάει για τα προβλήματα στην ψηφιακή ασφάλεια και στην ιδιωτικότητα, καθώς και για τις προκλήσεις στην ψηφιακή ασφάλεια και τον μετριασμό των κινδύνων ιδιωτικότητας για συσκευές IoT.

- **Τμήμα Ψηφιακού, Πολιτιστικού, Ενημερωτικού & Αθλητικού "Κώδικα Πρακτικής» για την Ασφάλεια Καταναλωτών του IoT, Οκτώβριος 2018"**: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

Ο κυβερνητικός κώδικας πρακτικής για την ασφάλεια καταναλωτών του IoT για κατασκευαστές, με οδηγίες για καταναλωτές που έχουν έξυπνες συσκευές στο σπίτι.

Πρακτικά Παραδείγματα

SQL Injection

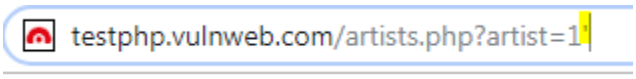
Υπάρχουν αυτοματοποιημένα εργαλεία που μπορείτε να χρησιμοποιήσετε για να δείτε αν μια ιστοσελίδα έχει τέτοιου είδους ευπάθεια. Μερικά από αυτά τα εργαλεία είναι:

- **SQLMap**
- **Havij**

Μια ιστοσελίδα που μπορείτε να εξασκηθείτε είναι η παρακάτω:

http://testphp.vulnweb.com/artists.php?artist=1

Το πρώτο που πρέπει να γίνει είναι να βάλετε μια απλή απόστροφο στο τέλος του url (Εικόνα 1).



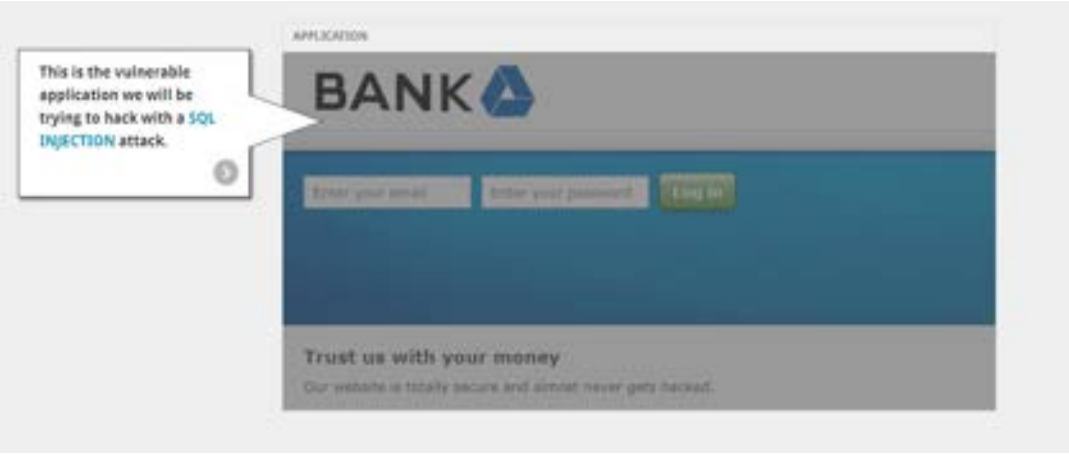
Εικόνα 1: Έλεγχος για SQL INJECTION

Αν πάρουμε το παρακάτω σφάλμα

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

Καταλαβαίνουμε ότι η ιστοσελίδα είναι ευπαθής σε τέτοιου είδους επίθεση. Μπορείτε να βρείτε ένα αναλυτικό οδηγό στο παρακάτω link.

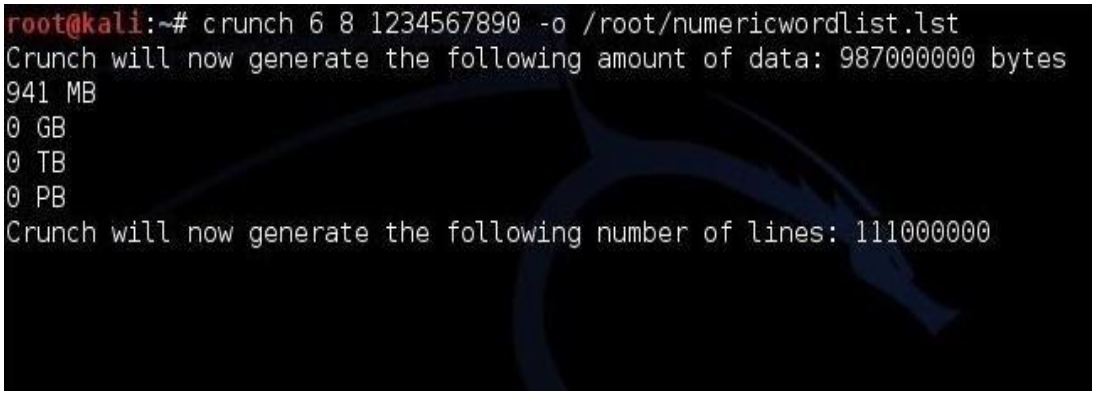
SQL demo



Dictionary attack

Σε αυτή την επίθεση οι επιτιθέμενοι είτε φτιάχνουν δικά τους λεξικά με passwords, είτε χρησιμοποιούν έτοιμα με σκοπό να ανακαλύψουν τους κωδικούς μας.

Παρακάτω(Εικόνα 2) βλέπουμε ένα παράδειγμα δημιουργίας ενός τέτοιου λεξικού με το εργαλείο Crunchπου υπάρχει στο Kali linux



Εικόνα 2 Δημιουργία λεξικού με το Crunch

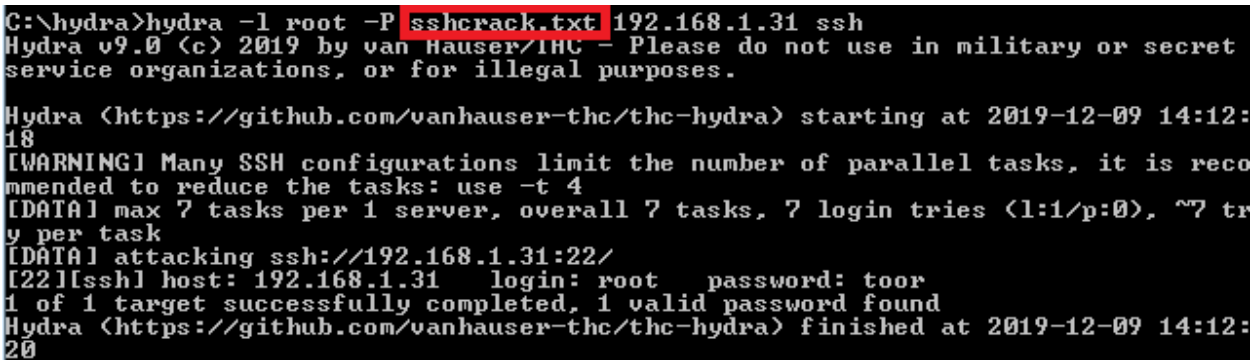
Όπου το πρώτο νούμερο 6 είναι το ελάχιστο μήκος του κωδικού και το δεύτερο 8 το μεγαλύτερο. Επιπλέον φαίνεται ότι ζητάμε να περιέχει μόνο αριθμούς απο 0-9.

Ερώτηση

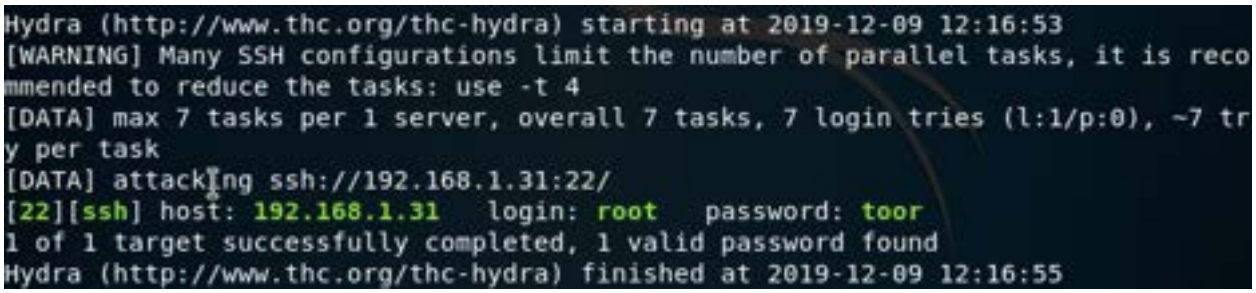
Ποια εντολή χρειαζόμαστε για να ζητήσουμε πεζούς χαρακτήρες (a-z) ;

Απάντηση : crunch 6 8 abcdefghiklmnopqrstuvwxyz -o /root/loweralpha.lst

Παρακάτω βλέπουμε στις (Εικόνες 3– 4) ένα παράδειγμα σπασίματος του ssh service(port 22)



Εικόνα 3 Σπάζοντας το ssh service σε Windows



Εικόνα 4 Σπάζοντας το ssh service σε Linux

Προσπαθήστε να κάνετε το ίδιο χρησιμοποιώντας το έτοιμο λεξικό με όνομα "rockyou"(κατεβάστε το απο εδώ).

Υπενθύμιση

Να χρησιμοποιείτε :

1) Ισχυρούς κωδικούς
Οι κωδικοί σας πρέπει να είναι μήκους τουλάχιστον 12 χαρακτήρων, και πάντα συνδυασμός γραμμάτων, αριθμών και ειδικών συμβόλων. Χρησιμοποιείτε συνδυασμό κεφαλαίων και πεζών χαρακτήρων.

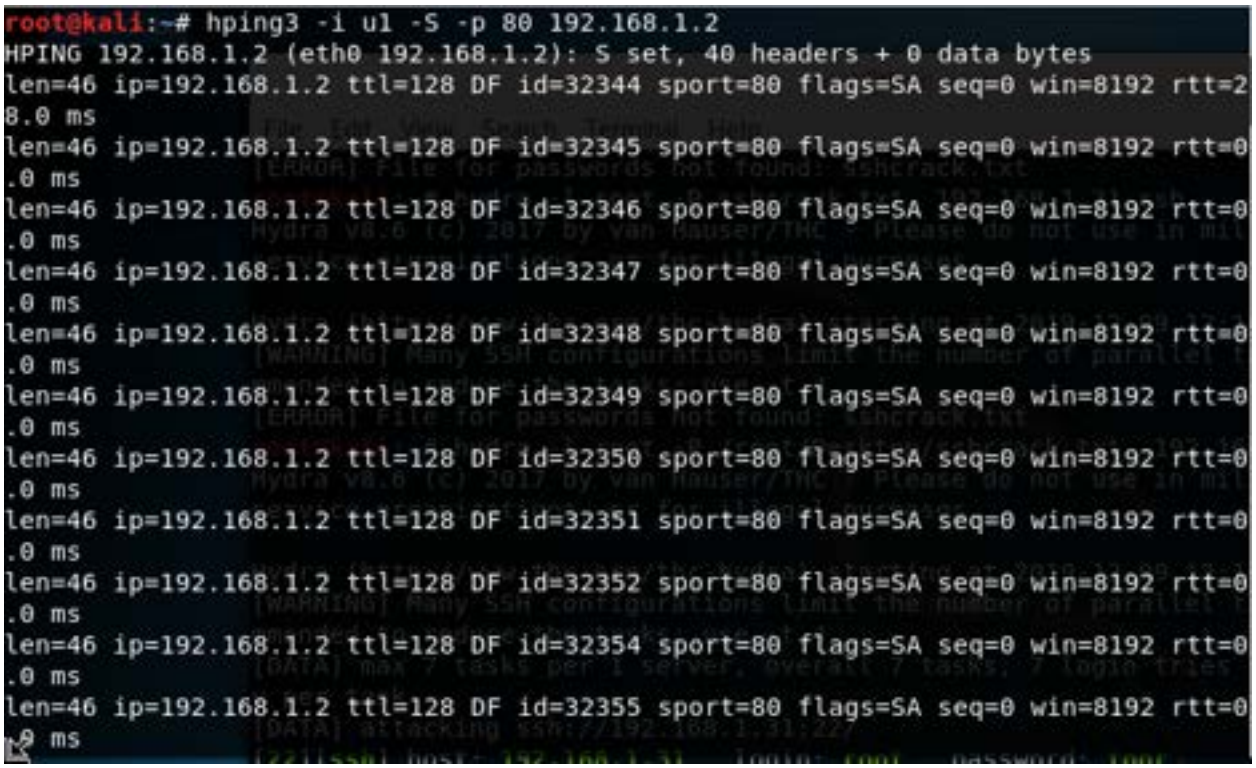
2) Μοναδικούς κωδικούς
Πρέπει να έχετε μοναδικό κωδικό για κάθε σας λογαριασμό. Ποτέ μην χρησιμοποιείτε τον ίδιο κωδικό για όλους σας τους λογαριασμούς.

3) Κωδικούς περιορισμένης διάρκειας
Οι κωδικοί σας θα πρέπει να ανανεώνονται τουλάχιστον κάθε τρείς μήνες για κάθε λογαριασμό σας. Μην χρησιμοποιείτε εκ νέου παλιότερούς σας κωδικούς.

DOS Attack

Η επίθεση αυτή αποσκοπεί στον τερματισμό λειτουργίας ενός μηχανήματος ή δικτύου ώστε να μην είναι προσβάσιμο απο τους νόμιμους χρήστες του.

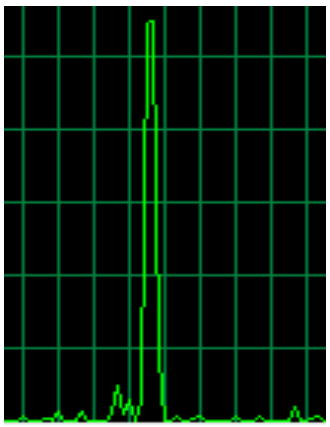
Το **hping3** είναι ένα δικτυακό εργαλείο που στέλνει πακέτα TCP/IP και δείχνει την απάντηση του μηχανήματος στόχου, όπως ακριβώς κάνει η εντολή ping με απαντήσεις ICMP (Εικόνα 5).



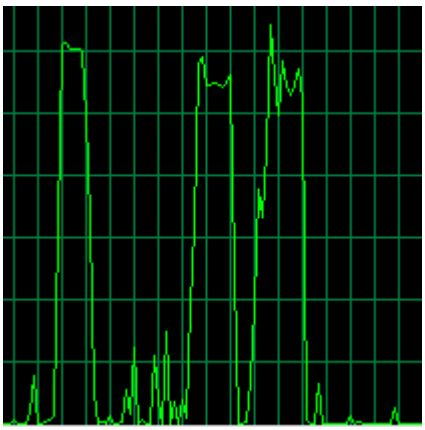
Εικόνα 1 Το εργαλείο hping3

Όπου: i — χρόνος αναμονής, — u1- 1 microsecond -S — SYN πακέτα -p — αριθμός πόρτας

Επιτεθήκαμε στο δικό μας τοπικό δίκτυο και τα αποτελέσματα της δραστηριότητας στο δίκτυο φαίνονται στις εικόνες 6 & 7.

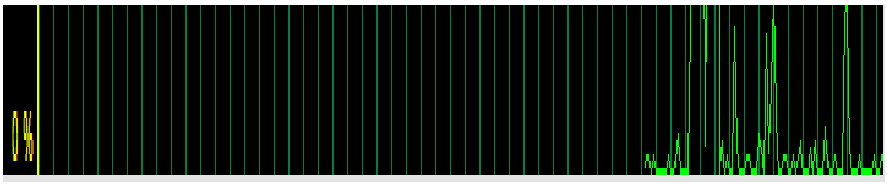


Εικόνα 6 Η δραστηριότητα 15-20 δευτερόλεπτα μετά την επίθεση



Εικόνα 7 Μετά απο 1-2 λεπτά

Όπως μπορούμε να δούμε η δραστηριότητα στο δίκτυο μας αυξήθηκε σημαντικά όταν η επίθεση ήταν επιτυχής.



Εικόνα 8 Συνήθης δικτυακή δραστριότητα

No.	Time	Source	Destination	Protocol	Length	Info
3635…	10.305082	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5758 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305087	192.168.1.2	192.168.1.31	TCP	58	80 → 5758 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305119	192.168.1.31	192.168.1.2	TCP	60	5758 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305147	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5759 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305152	192.168.1.2	192.168.1.31	TCP	58	80 → 5759 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305184	192.168.1.31	192.168.1.2	TCP	60	5759 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305223	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5760 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305229	192.168.1.2	192.168.1.31	TCP	58	80 → 5760 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305261	192.168.1.31	192.168.1.2	TCP	60	5760 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305289	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5761 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305294	192.168.1.2	192.168.1.31	TCP	58	80 → 5761 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305326	192.168.1.31	192.168.1.2	TCP	60	5761 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305354	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5762 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305360	192.168.1.2	192.168.1.31	TCP	58	80 → 5762 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305390	192.168.1.31	192.168.1.2	TCP	60	5762 → 80 [RST] Seq=1 Win=0 Len=0

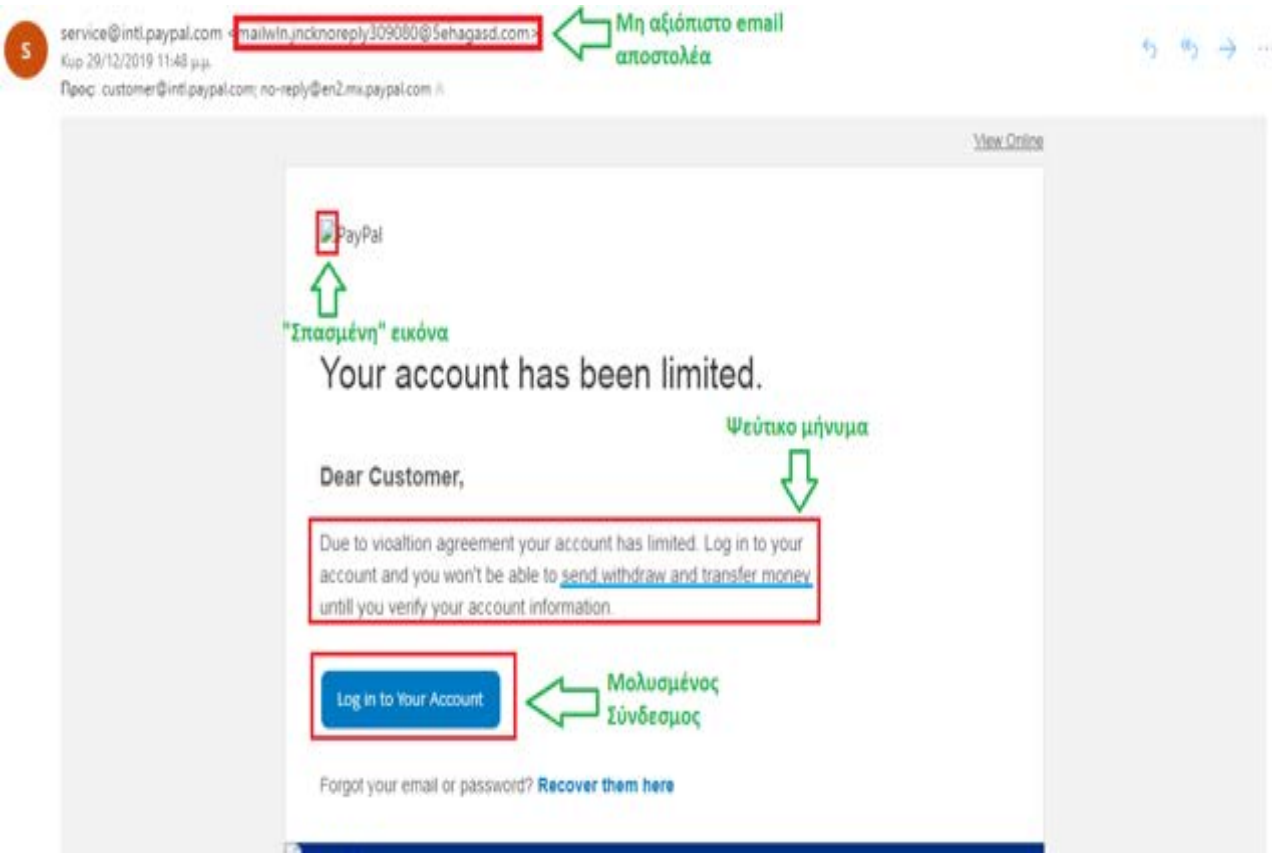
Εικόνα 9 Τα πακέτα που συνέλαβε το Wireshark κατά την επίθεση

Απο την Εικόνα 9 είναι προφανές ότι το μηχάνημα που κάνει την επίθεση στέλνει συνέχεια πακέτα SYN(Dosattack) στο μηχάνημα στόχο.

Phishing email

Γενικότερα το phishing είναι όταν κάποιος προσπαθεί να υποκλέψει προσωπικές σας πληροφορίες online με διάφορους τρόπους. Συνήθως γίνεται με email και πάντοτε ο αποστολέας του μηνύματος δεν είναι αυτός που φαίνεται να είναι. Ας δούμε ένα παράδειγμα:

Στην εικόνα 10 βλέπουμε ένα κλασσικό phishing email παράδειγμα



Εικόνα 10 Παράδειγμα phishing email

Υπάρχουν επιπλέον και άλλες κατηγορίες email phishing.

Οι βασικές είναι:

- Μολυσμένα επισυναπτόμενα αρχεία(με επεκτάσεις .JS, .DOC, .HTML).
- Μακροεντολές ενσωματωμένες σε αρχεία κειμένου.
- Εκμετάλλευση των κοινωνικών δικτύων για εγκατάσταση επεκτάσεων στον browser.
- LinkedIn Phishing Attacks (για την υποκλοπή των διαπιστευτηρίων του χρήστη).

Ένα καλό online demo για να καταλάβετε αν ένα email είναι αληθινό ή όχι (phishing)είναι το ακόλουθο:

Phishing demo

Co-funded by the
Erasmus+ Programme
of the European Union

ΕΝΟΤΗΤΑ 3

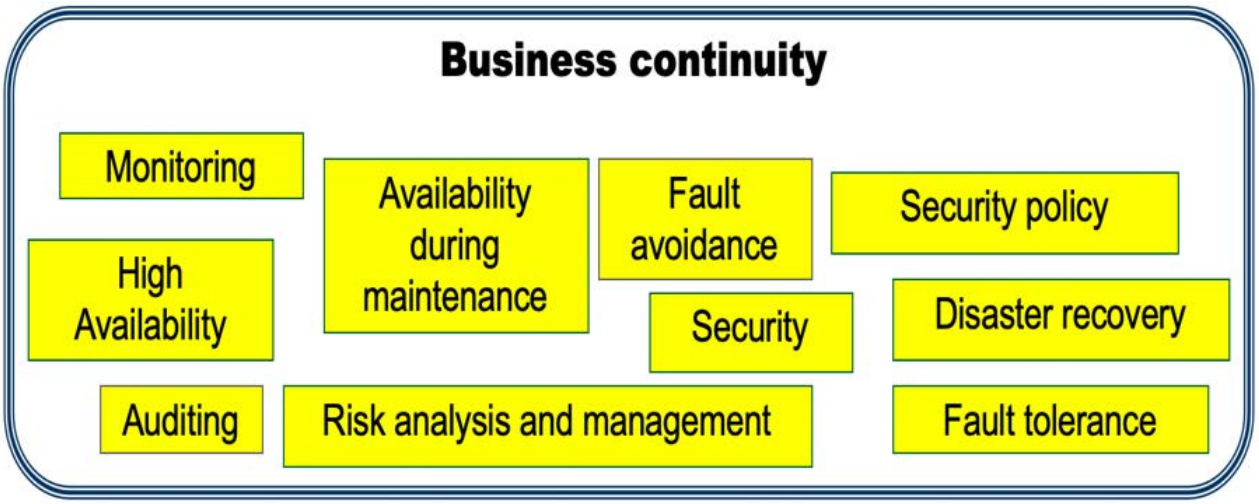
Εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα σε βιομηχανικά περιβάλλοντα

3.1 Διαθεσιμότητα

Description

Table of contents

Η επιχειρησιακή συνέχεια εξαρτάται από πολλούς παράγοντες. Στον τομέα των διαχειριστών συστήματος, είναι επιτακτικό να ανησυχούμε για την επίδραση της τεχνολογικής υποδομής στην επιχείρηση.



Εικόνα 3.1. Επιχειρησιακή συνέχεια

Η τεχνολογική υποδομή πρέπει να διασφαλίζει την επιχειρησιακή συνέχεια και την αδιάλειπτη λειτουργία εντός των **παραμέτρων** που έχουν προβλεφθεί για μια επιχείρηση με τέτοια υποδομή.

Ασφαλές σύστημα (ασφαλής τεχνολογική υποδομή) (secure technological infrastructure) θεωρείται αυτό που συνεχίζει να λειτουργεί εντός των ποιοτικών και ποσοτικών παραμέτρων (**SLA**- Service Level Agreement). Κάθε απόκλιση από αυτές τις παραμέτρους θεωρείται αποτυχία.

Αυτές οι παράμετροι αφορούν στην τριάδα της ασφάλειας υπολογιστών: **Εχεμύθεια**, **Ακεραιότητα** και **Διαθεσιμότητα**.

Για τον σχεδιασμό ενός ασφαλούς συστήματος που διασφαλίζει την επιχειρησιακή συνέχεια πρέπει να ζυγίσουμε **το κόστος** και **τα πλεονεκτήματα** ώστε να **πάρουμε ένα αποδεκτό ποσοστό αποτυχίας.**

Δεν υπάρχουν παντελώς ασφαλή συστήματα, που εγγυούνται απόλυτα ότι δε θα γίνει ποτέ καμία αποτυχία (0% πιθανότητα αποτυχίας).

Αν και η πιθανότητα αποτυχίας είναι χρήσιμο δεδομένο, στην πράξη χρησιμοποιείται η μονάδα MTBF - Mean Time Between Failures,που δείχνει τον μέσο χρόνο που πέρασε ανάμεσα στις αποτυχίες κι εκφράζεται συνήθως σε ώρες.

Η επιχειρησιακή συνέχεια εξαρτάται από πολλούς παράγοντες. Στον τομέα των διαχειριστών συστήματος, είναι επιτακτικό να ανησυχούμε για την επίδραση της τεχνολογικής υποδομής στην επιχείρηση.

$$Availability = \frac{Operation\ time\ without\ failures}{Total\ time}$$

Εικόνα 3.2. Διαθεσιμότητα

Παράδειγμα: Αν ένας σέρβερ(Server) αποτύχει στη λειτουργία του 18 μέρες μέσα σε ένα έτος(δηλαδή γύρω στο 5% του χρόνου λειτουργίας – ένα έτος ισούται με 365 μέρες), τότε:

Διαθεσιμότητα = (365-18)/365 = 0.95

Η διαθεσιμότητά του υπολογίζεται στο 95%.

Η Πλήρης Ανοχή σε Βλάβες διασφαλίζει ότι η βλάβη ενός εξαρτήματος δεν επηρεάζει τις λειτουργικές παραμέτρους.

Παράδειγμα: RAID1.

Η εφεδρική συστοιχία ανεξάρτητων δίσκων (Redundant Array of Independent Disks) (RAID) είναι ένα κοινό παράδειγμα ανοχής σε βλάβες, που βασίζεται στον πλεονασμό. Το RAID 1 (κατοπτρισμός) (Mirroring) χρησιμοποιεί μια συστοιχία από N ολόιδιους (τουλάχιστον 2) δίσκους, που περιέχουν όλοι τους τις ίδιες πληροφορίες. Μπορεί να υποστηρίξει την ταυτόχρονη αποτυχία N - 1 δίσκων.

Η ανοχή σε βλάβες συνήθως επιτυγχάνεται μέσω των πλεοναζόντων εξαρτημάτων. Δεν είναι πάντα δυνατή η τέλεια και άμεση αντικατάσταση του χαλασμένου εξαρτήματος.

Σε αυτή την περίπτωση έχουμε μια προσωρινή υποβάθμιση των παραμέτρων λειτουργίας (*Graceful Degradation*).

Αν η υποβάθμιση είναι σημαντική ή παρατεταμένη, τότε το σύστημα μετονομάζεται σε *Fail soft*, από *Fault Tolerant*.

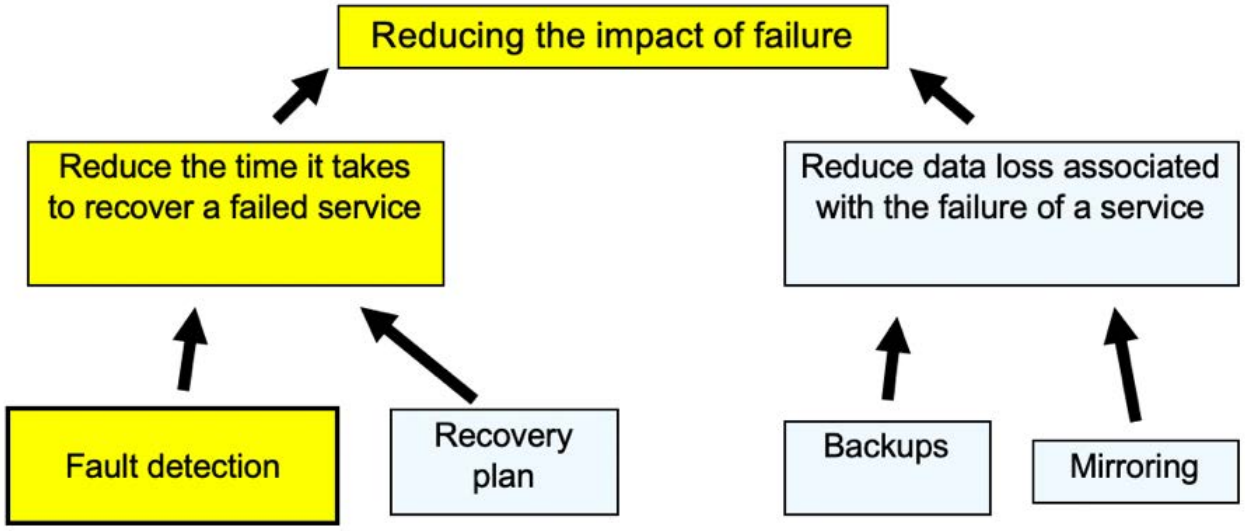
Ένα σύστημα ονομάζεται *Fail safe* αν η βλάβη προκαλέσει μη διαθεσιμότητα χωρίς να επηρεάσει την ακεραιότητά του.

Παράδειγμα: UPS χωρίς γεννήτρια.

Η αποφυγή των βλαβών αφορά στην αποτροπή τους. Βασίζεται σε πολλά μέτρα κοινής λογικής:

- Χρήση αποδεδειγμένα ποιοτικών εξαρτημάτων
- Περιβαλλοντικός έλεγχος (θερμοκρασία, υγρασία, σκόνη)
- Ενεργειακός έλεγχος(σταθερότητα και φιλτράρισμα)
- Έλεγχος φυσικής πρόσβασης, συμπεριλαμβάνοντας τις επικοινωνιακές γραμμές
- Έλεγχος απομακρυσμένης πρόσβασης (τείχος προστασίας, επαλήθευση στοιχείων)
- Πρόληψη και πυρόσβεση
- Δοκιμή της απόδοσης των εξαρτημάτων προτού μπουν σε λειτουργία
- Απλοποίηση της διαχείρισης συστήματος, όπως με την εικονικοποίηση (virtualization) λόγου χάρη
- Έλεγχος δικαιωμάτων και προνομίων διαχείρισης
- Δημοσιοποίηση της Πολιτικής Ασφαλείας και εκπαίδευση χρηστών και χειριστών
- Εφαρμογή όλων των ενημερώσεων του λογισμικού
- Εγγυήσεις αυθεντικότητας(αξιόπιστοι μηχανισμοί επιβεβαίωσης γνησιότητας)
- Παρακολούθηση(επιτρέπει τον εντοπισμό πιθανών σημείων βλάβης)
- Έλεγχος της υλοποίησης πόρων(περιορισμός / εφεδρεία). Π.χ.: CPU,RAM,DISCO,NETWORK

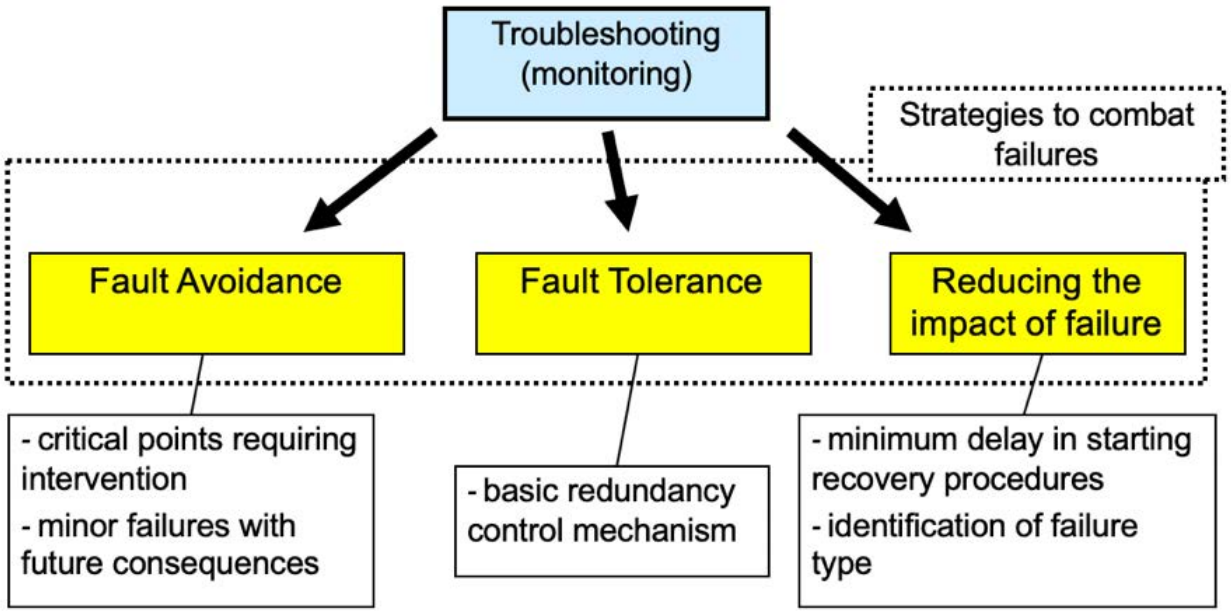
Όσο προσεκτικά και να παρθούν τα μέτρα στους τομείς **της πρόληψης βλαβών** και **της ανοχής σε βλάβες**, αυτές είναι αδύνατον να εξαλειφθούν εντελώς, οπότε η έσχατη λύση είναι η **ελάττωση της επίδρασης των βλαβών.**



Εικόνα 3.3. Ελάττωση της επίδρασης των βλαβών

Για περισσότερες πληροφορίες σχετικά με τον κατοπτρισμό, δείτε Παράγραφος 1.2 Ανοχή σε βλάβες

Για διάφορους λόγους, ο εντοπισμός βλαβών έχει απευθείας σχέση με τα τρία συμπληρωματικά παρακλάδια σφάλματος, όπως φαίνεται στην εικόνα 3.4.



Εικόνα 3.4. Επίλυση προβλημάτων

Παρακολούθηση

Ο εντοπισμός των βλαβών θα έπρεπε να είναι αυτοματοποιημένος, 24/7. Αυτή η διαδικασία αφορά στην περιοδική εκτέλεση δοκιμών στα εξαρτήματα της υποδομής του υπολογιστή:

- Χρόνοι απόκρισης των υπηρεσιών
- Κατάσταση εσωτερικών συσκευών

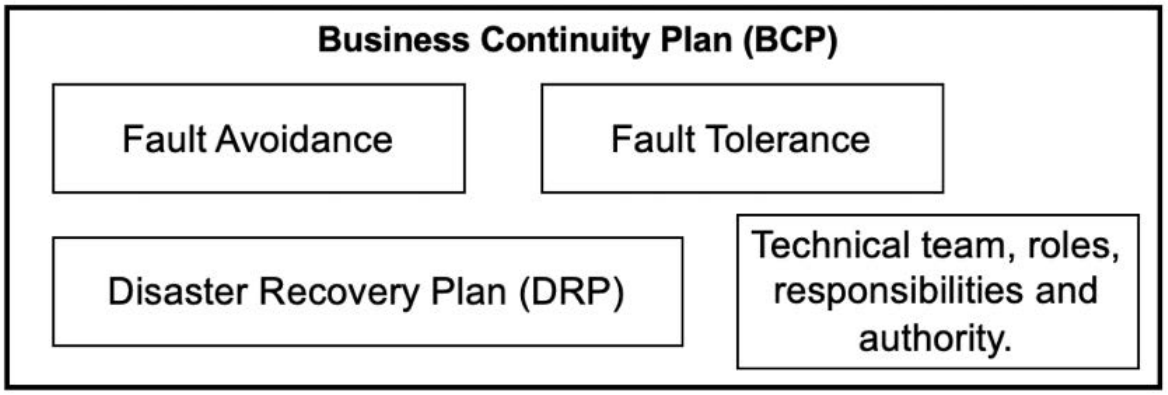
- Μετρήσεις (θερμοκρασίες κλπ.)
- Ανωμαλίες στα αρχεία δραστηριοτήτων
- Όγκοι και τύποι της δικτυακής κίνησης
- Εντοπισμός ανωμαλιών και εισβολέων

Μόλις εντοπιστεί μια ανωμαλία, το σύστημα παρακολούθησης πρέπει να ενημερώσει τους διαχειριστές το συντομότερο δυνατόν, για να ξεκινήσει η διαδικασία αποκατάστασης. Συνήθως χρησιμοποιείται το email για αυτήν τη δουλειά, αλλά είναι προτιμότερο να ενισχυθεί αυτή η επιλογή και με κάποια μορφή άμεσου μηνύματος.

Σε μερικά συστήματα ίσως είναι δυνατόν να καθοριστούν αυτόματοι μηχανισμοί αποκατάστασης για ορισμένες ανωμαλίες.

Ο σκοπός του Σχεδίου Επιχειρησιακής Συνέχειας (Business Continuity Plan) (BCP) είναι να καθορίσει συγκεκριμένες συνθήκες και διαδικασίες για τη διασφάλιση της επιχειρησιακής συνέχειας.

Το Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery Plan) (DRP) είναι ένα από τα πιο σημαντικά στοιχεία του BCP (μπερδεύονται μερικές φορές), αλλά το BCPείναι πιο εμπεριστατωμένο.

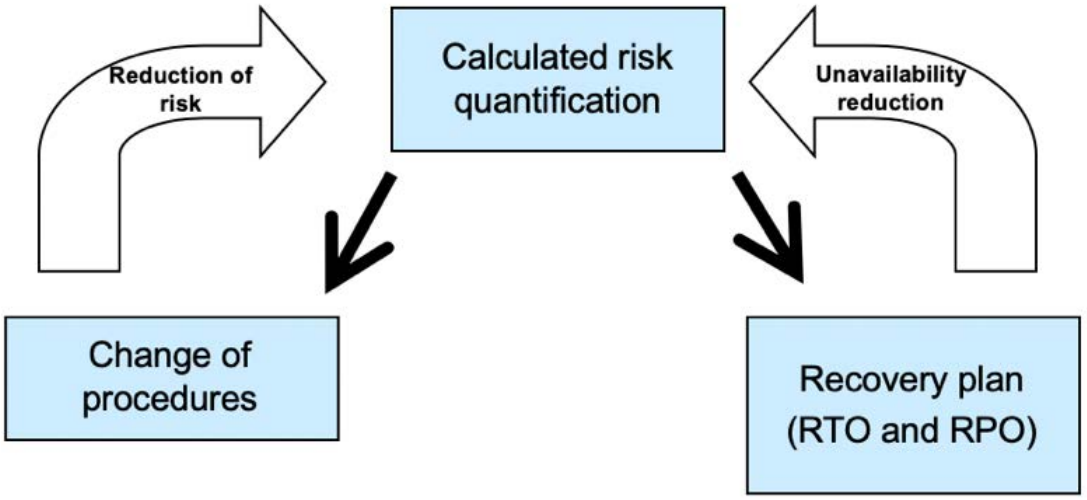


Εικόνα 3.5. Σχέδιο Επιχειρησιακής Συνέχειας

Ένα σχέδιο επιχειρησιακής συνέχειας πρέπει να απαρτίζεται από:

- Προτεραιότητες κι ευθύνες
- Κυρίως ρίσκα και μέτρα ελαχιστοποίησής τους
- Προτεινόμενες στρατηγικές
- Σχέδιο Β'
- Ρόλοι κι ευθύνες
- Συνθήκες ενεργοποίησης του Σχεδίου Επιχειρησιακής Συνέχειας
- Διεργασίες έκτακτης αποκατάστασης

Η εκτίμηση ρίσκου μπορεί να γίνει χρησιμοποιώντας φόρμες/ έρευνες (surveys),που όταν προσδιορίσουμε συγκεκριμένες παραμέτρους, μας επιτρέπουν να κάνουμε θεωρητικό προσδιορισμό του ρίσκου στον τομέα που αναλύουμε.



Εικόνα 3.6. Εκτίμηση ρίσκου

Στόχος Σημείου Ανάκτησης

Στις υπηρεσίες όπου επιτρέπεται η απώλεια δεδομένων λόγω καταστροφής, ο Στόχος Σημείου Ανάκτησης (Recovery Point Objective) (RPO) ορίζει τον μέγιστο όγκο δεδομένων που μπορούν να χαθούν. Το RPO ορίζει μια συγκεκριμένη χρονική στιγμή λειτουργίας πριν την καταστροφή, μετά την οποία θα χαθούν όλες οι αλλαγές.

Ο χρόνος ανάμεσα στα αντίγραφα ασφάλειας δεν πρέπει ποτέ να ξεπερνάει εκείνον του RPO. Αν χρησιμοποιείται και κατοπτρισμός, το RPO είναι μηδενικό ή πολύ κοντά στο μηδέν (αν ο κατοπτρισμός είναι παράλληλος, τότε το RPO είναι μηδενικό).

Στόχος Χρόνου Ανάκτησης

Άρα ο Στόχος Χρόνου Ανάκτησης (Recovery Time Objective) (RTO) είναι ο μέγιστος χρόνος που το σύστημα μπορεί να μείνει εκτός λειτουργίας.

Στην περίπτωση σφάλματος πρέπει να ξεκινήσει η διαδικασία αποκατάστασης (ακόμα κι αν είναι εξάρτημα ενός πλεονάζοντος συστήματος).

Ο όρος **ανάκαμψη από καταστροφή (disaster recovery)** αφορά περισσότερο σε γεγονότα με μεγάλη επίδραση, όπως μεγάλες φυσικές καταστροφές, με σχεδόν ολοκληρωτική φυσική καταστροφή.

Η ανάκαμψη από καταστροφή είναι κρίσιμη για την επιχειρησιακή συνέχεια. Ο στόχος είναι η ελαχιστοποίηση της διακοπής και της πιθανής απώλειας δεδομένων.

Η ανάκαμψη από καταστροφή αφορά αποκλειστικά στην προετοιμασία και τον σχεδιασμό:

- Κατοπτρισμός για απομακρυσμένη τοποθεσία
- Τακτικά αντίγραφα ασφάλειας που αποθηκεύονται σε απομακρυσμένη τοποθεσία
- Εφεδρικός εξοπλισμός, αποθηκευμένος σε απομακρυσμένη τοποθεσία
- Σενάρια καταστροφής με δικά τους σχέδια ανάκαμψης

1.7.1 Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery Plan)

Σκοπός του DRP είναι η ελαχιστοποίηση της διακοπής και της απώλειας δεδομένων στην περίπτωση καταστροφής.

Το DRP καθορίζει σενάρια καταστροφής και διαδικασίες ανάκαμψης για το καθένα από αυτά. Και αυτό πρέπει να έχει μέγιστο αποδεκτό χρόνο διακοπής για την αποκατάσταση της λειτουργίας.

1.7.2 Backup/Restore

Σε περίπτωση καταστροφής με απώλεια δεδομένων ή ρυθμίσεων του λογισμικού, το αντίγραφο ασφάλειας επιτρέπει **την αναδημιουργία του συστήματος στην ίδια κατάσταση που είχε κατά την ημερομηνία που έγινε το αντίγραφο.**

Η συχνότητα δημιουργίας αντιγράφων πρέπει να εξαρτάται από τη συχνότητα αλλαγής των δεδομένων και να ρυθμιστεί ανάλογα για το κάθε στοιχείο της υποδομής.

Ο ακριβής χρόνος της δημιουργίας αντιγράφων πρέπει να προσαρμοστεί στις ώρες λειτουργίας. Τα καθημερινά αντίγραφα θα πρέπει να γίνονται μετά το κλείσιμο της εταιρείας.

Οι δίσκοι υψηλής χωρητικότητας έχουν χαμηλό κόστος αυτήν τη στιγμή, οπότε και είναι προτιμότεροι ως λύση από τις πιο παραδοσιακές (με πολύ αργή πρόσβαση) λύσεις με μαγνητική ταινία.

Αυτά τα πιο αργά μέσα είναι περισσότερο κατάλληλα για αντίγραφα αρχειοθέτησης παρά για αντίγραφα ασφάλειας.

Τα αργά μέσα προκαλούν και προβλήματα κατά τη δημιουργία αντιγράφων, κάνοντας την όλη διαδικασία ιδιαίτερα χρονοβόρα. Η δημιουργία των αντιγράφων μπορεί να επηρεάσει τη διαθεσιμότητα του συστήματος. Συνήθως, τα διάφορα αρχεία πρέπει να κλειδωθούν για να μην υποστούν αλλαγές κατά την αντιγραφή.

1.7.3 Σχέδιο Backup/Restore

Ένας τρόπος μείωσης του χρόνου διαδικασίας αντιγραφής είναι η χρήση **επαυξητικών (incremental)**αντιγράφων ή **διαφορικών** (**differential)** αντιγράφων. **Όπως και να έχει, όμως, το αρχικό σημείο είναι πάντα ένα πλήρες αντίγραφο**.

Ένα επαυξητικό αντίγραφο περιέχει τα δεδομένα που έχουν αλλάξει από το προηγούμενο επαυξητικό αντίγραφο (ή το πλήρες αντίγραφο, αν είναι το πρώτο).

Ένα διαφορικό αντίγραφο περιέχει τα δεδομένα που έχουν αλλάξει από το τελευταίο πλήρες αντίγραφο.

-**Επαυξητικά** αντίγραφα: Πρέπει να διατηρείται μεγάλος αριθμός επαυξητικών αντιγράφων .Πέραν από τον χώρο που καταλαμβάνουν, η διαδικασία αντικατάστασης είναι εξαιρετικά χρονοβόρα.

- **Διαφορικά** αντίγραφα: Ο όγκος του διαφορικού αντιγράφου μεγαλώνει όσο αυξάνονται οι αλλαγές στο πλήρες αντίγραφο.

Και εδώ πρέπει να σεβαστούμε τις ώρες λειτουργίας. Τα πλήρη αντίγραφα γίνονται συνήθως Κυριακές, ενώ τα επαυξητικά ή τα διαφορικά αντίγραφα γίνονται τις άλλες μέρες της εβδομάδας (αλλά αυτό εξαρτάται από τις ώρες λειτουργίας).

Δεν πρέπει ποτέ να διαγράψουμε ένα αντίγραφο ασφάλειας προτού ολοκληρωθεί επιτυχώς το επόμενο. Πολλές φορές είναι επιθυμητό να κρατήσουμε τουλάχιστον άλλο ένα πιο παλιό αντίγραφο, αν όχι και περισσότερα.

Το προηγούμενο αντίγραφο μπορεί να μεταφερθεί σε ένα πιο οικονομικό μέσο αποθήκευσης, προτού κάνουμε το νέο αντίγραφο.

Αν και μπορούμε να βάλουμε το αντίγραφο σε πυρίμαχο κουτί, ιδανικά θα έπρεπε να το στείλουμε **σε διαφορετική γεωγραφική τοποθεσία (off-site)**.

Υπάρχουν ορισμένα μειονεκτήματα:

-Ασφάλεια: Είναι απαραίτητο να διασφαλίσουμε την αυθεντικότητα και την εχεμύθεια (π.χ.: VPN).

-Ταχύτητα πρόσβασης: Επηρεάζει τον χρόνο που απαιτείται για το αντίγραφο.

-Αξιοπιστία: Η ανάκτηση είναι δυνατή μόνο αν λειτουργεί η σύνδεση με το δίκτυο.

Το εναλλακτικό σχέδιο είναι σημαντικό κομμάτι του BCP και καθορίζει εναλλακτικές μεθοδολογίες για την αδιάκοπη λειτουργία της επιχείρησης, όταν δεν είναι διαθέσιμοι οι "κανονικοί" πόροι.

Μπορεί να είναι δύσκολη η ενσωμάτωσή του σε οργανισμούς που εξαρτώνται πολύ από συστήματα υπολογιστή.

Πρέπει να καθορίζει:

- Τι είδος καταστροφής οδηγεί στην έναρξη του εναλλακτικού σχεδίου.

- Τα ακριβή μέτρα που πρέπει να παρθούν.

- Τις ανάγκες σε προσωπικό και υλικά ή εξοπλισμό.

- Ποιες "κανονικές" διαδικασίες προβλέπονται στο εναλλακτικό σχέδιο και ποιες θα είναι μη διαθέσιμες (περιορισμοί στη λειτουργία της επιχείρησης).

- Πώς θα ενσωματωθούν στο σύστημα οι διαδικασίες που εκτελέστηκαν σύμφωνα με το εναλλακτικό σχέδιο, μετά την ανάκτηση του συστήματος.

Η Πολιτική Ασφαλείας είναι ένα έγγραφο που ορίζει συγκεκριμένους κανόνες για την προστασία της υποδομής και των δεδομένων.

Είναι σημαντικό στοιχείο για τη διασφάλιση της επιχειρησιακής συνέχειας, ειδικά στον τομέα της πρόληψης βλαβών.

Η Πολιτική Ασφαλείας πρέπει να είναι πιο αόριστη από ένα εγχειρίδιο χρήστη, πρέπει να δείχνει «τι δεν μπορεί να γίνει», «τι μπορεί να γίνει», αλλά δεν πρέπει να περιλαμβάνει και το «πώς γίνεται».

Για λόγους ασφάλειας και για να διευκολυνθεί η προσαρμογή της στην εξέλιξη του οργανισμού, δεν πρέπει να περιλαμβάνει τεχνικές πτυχές της υλοποίησης.

Η Πολιτική Ασφαλείας πρέπει να είναι περιεκτική και εύκολη στην ανάγνωση και κατανόηση. Προτείνουμε τη χρήση των πέντε W της δημοσιογραφίας: ***Who*, *What*, *Where*, *When*, *Why* (Ποιος, Τι, Πού, Πότε, Γιατί).**

Η περιοριστική φύση της Πολιτικής Ασφαλείας πρέπει να προκύπτει από την προγενέστερη εκτίμηση των ρίσκων ασφάλειας. Είναι δυνατός ο προσδιορισμός του κινδύνου επίθεσης, μέσω της χρήσης ερωτηματολογίων για τον οργανισμό / επιχείρηση και την υποδομή του.

Χαρακτηριστικά:

- Δημόσιο έγγραφο, εύκολα προσβάσιμο από όλους τους χρήστες
- Υποχρεωτικό ανάγνωσμα για όλους τους χρήστες
- Ταυτοποιεί τους διάφορους ρόλους μέσα στον οργανισμό (χρήστες, διαχειριστές κλπ.)
- Ορίζει ξεκάθαρα τους στόχους της ασφάλειας
- Ενημερώνει τους χρήστες ως προς τις διάφορες απειλές προς το σύστημα
- Τονίζει τη σημασία της τήρησης των κανόνων από όλους (χωρίς εξαιρέσεις)
- Δικαιολογεί την ύπαρξη των επιβεβλημένων κανονισμών (οι χρήστες πρέπει να συμφωνήσουν)
- Αναφέρει συγκεκριμένες επαφές για την αποσαφήνιση περίπλοκων ερωτημάτων
- Καθορίζει τον τρόπο αντιμετώπισης περιπτώσεων που δεν αναφέρονται στην "πολιτική ασφαλείας"
- Αναφέρει τις συνέπειες της παράβασης των κανονισμών(με αόριστο τρόπο, αφού μπορεί να υπάρξει ασυμφωνία με τη νομοθεσία και / ή με τις εργασιακές συμβάσεις)
- Τονίζει την ανάγκη ύπαρξης αρχείων δραστηριοτήτων για τους ελέγχους (audits)
- Συνάδει με το βάθος της προσέγγισης πολλαπλών παρακλαδιών
- Γίνεται να επιβληθεί στους χρήστες(υπάρχει η δυνατότητα παρακολούθησης της συμμόρφωσης στους κανόνες)

Η πολιτική πρέπει να λέει τι επιτρέπεται και να απαγορεύει όλα τα υπόλοιπα. Το ρίσκο μεγαλώνει αν πούμε τι απαγορεύεται και επιτρέψουμε όλα τα άλλα.

Πολιτικές για:

- Πιστοποίηση (authentication)
- Φυσική πρόσβαση
- Λογική πρόσβαση
- Χρήση εσωτερικού δικτύου(σύνδεση συσκευών στο δίκτυο,...)
- Χρήση διαδικτύου(πρόσβαση σε ιστοσελίδες, έλεγχος περιεχομένου,...)
- Κωδικοί(κανόνες για τον ορισμό, αποθήκευση και χρήση τους)
- Χρήση email

- Ιδιωτικότητα (εχεμύθεια. Αρχεία δραστηριοτήτων και πρόσβαση σε αυτά)
- Διαχείριση εργασιακών συστημάτων.

3.2 Εμπιστευτικότητα Δεδομένων

Description

Table of contents

Εμπιστευτικότητα ορίζεται η εγγύηση ότι υπάρχει επαρκές επίπεδο μυστικότητας σε κάθε επεξεργαστικό κόμβο και ότι παρεμποδίζεται η διαρροή πληροφοριών.

Η εμπιστευτικότητα πρέπει να ενσωματωθεί σε ολόκληρο το σύστημα κι όχι μόνο σε ορισμένα τμήματά του.

Μπορεί να επιτευχθεί μέσω:

- Της κρυπτογράφησης των δεδομένων που αποθηκεύονται και μεταδίδονται
- Ασφαλών επικοινωνιών

Μπορεί να παρακαμφθεί από:

- Παρακολούθηση επικοινωνιών
- Κοινωνική μηχανική
- Κλοπή κωδικών

Η αποθήκευση δεδομένων παίζει ρόλο κλειδί σε ένα υπολογιστικό/βιομηχανικό σύστημα, όπου αυξάνεται καθημερινά η ανάγκη για πληροφορίες, καθώς και η σημασία τους. Αυτές τις μέρες, και σε πολλές περιπτώσεις, οι πληροφορίες είναι τα πιο πολύτιμα αγαθά μιας εταιρείας.

Υπάρχουν πολλά διαθέσιμα μέσα για την αποθήκευση δεδομένων. Αυτά διαφέρουν σε χωρητικότητα, ποιότητα και κόστος. Σε επαγγελματικά συστήματα, είναι σημαντικό να επιλέξουμε τα μέσα που θα διασφαλίσουν ότι δε θα υπάρξει απώλεια πληροφοριών.

Τα Pendrives (στικάκι USB) και οι εξωτερικοί σκληροί δίσκοι είναι τα φτηνότερα μέσα της σημερινής αγοράς. Έχουν μερικά προβλήματα ως αποτέλεσμα της κακής ποιότητας κατασκευής και της κακής διαχείρισής τους από τους χρήστες.

Αυτά τα μέσα μπορούν να χρησιμοποιηθούν για την αποθήκευση μη κρίσιμων πληροφοριών. Εντούτοις, προτείνεται και η δημιουργία αντιγράφου σε άλλο μέσο.

Συνήθως, αυτό το είδος εξοπλισμού δεν ενσωματώνει ασφάλεια δεδομένων ή κρυπτογράφηση, οπότε αν χαθεί, υπάρχει η περίπτωση να δημοσιοποιηθούν κρίσιμα δεδομένα.

Εικόνα 3.7. PenDrive

«Το cloud computing (υπολογιστικό νέφος) είναι ένας γενικός όρος για οτιδήποτε αφορά στην παροχή υπηρεσιών φιλοξενίας μέσω του διαδικτύου. Αυτές οι υπηρεσίες διαχωρίζονται ευρέως σε τρεις κατηγορίες: Υποδομή ως Υπηρεσία (Infrastructure-as-a-Service) (IaaS), Πλατφόρμα ως Υπηρεσία(Platform-as-a-Service)(PaaS) και Λογισμικό ως Υπηρεσία (Software-as-a-Service)(SaaS).Το όνομα, «υπολογιστικό νέφος», ήταν έμπνευση από το σύμβολο του σύννεφου, που χρησιμοποιείται συχνά για να απεικονίσει το διαδίκτυο στα διάφορα διαγράμματα.

Μια υπηρεσία cloud έχει τρία ιδιαίτερα χαρακτηριστικά, που τη διαφοροποιούν από την παραδοσιακή φιλοξενία ιστοσελίδων(webhosting). Πωλείται κατά παραγγελία (ondemand), συνήθως με το λεπτό ή με την ώρα. Είναι ελαστική– ένας χρήστης μπορεί να χρησιμοποιήσει όσο πολύ ή όσο λίγο θέλει μια υπηρεσία και σε οποιαδήποτε στιγμή. Ο πάροχος είναι αυτός που διαχειρίζεται πλήρως την υπηρεσία (ο καταναλωτής χρειάζεται μόνο έναν προσωπικό υπολογιστή και πρόσβαση στο διαδίκτυο). Σημαντικές καινοτομίες στην εικονικοποίηση (virtualization) και στα κατανεμημένα συστήματα πληροφορικής (distributed computing), καθώς επίσης κι η βελτιωμένη πρόσβαση σε Internet υψηλής ταχύτητας, έχουν αυξήσει το ενδιαφέρον στο cloud computing.

Το cloud μπορεί να είναι ιδιωτικό ή δημόσιο. Ένα δημόσιο cloud πουλάει υπηρεσίες σε οποιονδήποτε στο διαδίκτυο(αυτήν τη στιγμή, ο μεγαλύτερος πάροχος δημοσίου cloud είναι η Amazon WebServices) .Ένα ιδιωτικό cloud είναι ένα ιδιόκτητο δίκτυο ή κέντρο δεδομένων (data center),που παρέχει υπηρεσίες φιλοξενίας σε περιορισμένο αριθμό ατόμων. Είτε είναι ιδιωτικό είτε δημόσιο, στόχος του cloud computing είναι η παροχή εύκολης και κλιμακωτής πρόσβασης σε υπολογιστικούς πόρους και υπηρεσίες IT.

Το ιδιωτικό cloud είναι ένας τύπος cloud computing που προσφέρει αντίστοιχα πλεονεκτήματα με το δημόσιο cloud, συμπεριλαμβάνοντας τη δυνατότητα κλιμάκωσης και αυτοεξυπηρέτησης, αλλά μέσω ιδιόκτητης αρχιτεκτονικής. Σε αντίθεση με τα δημόσια clouds, που προσφέρουν υπηρεσίες σε πολλαπλούς οργανισμούς, ένα ιδιωτικό cloud είναι αφιερωμένο στις ανάγκες και στους στόχους ενός μοναδικού οργανισμού.

Ως αποτέλεσμα, το ιδιωτικό cloud είναι ιδανικό για επιχειρήσεις με δυναμικές ή απρόβλεπτες υπολογιστικές ανάγκες, που χρειάζονται άμεσο έλεγχο στα περιβάλλοντά τους για να πληρούν τις προαπαιτήσεις ασφάλειας, εταιρικής διακυβέρνησης (business governance) ή συμμόρφωσης με τις κανονιστικές διατάξεις (regulatory compliance requirements).»

[1] πηγή: searchcloudcomputing.techtarget.com

Δικτυακά αποθηκευτικά μέσα

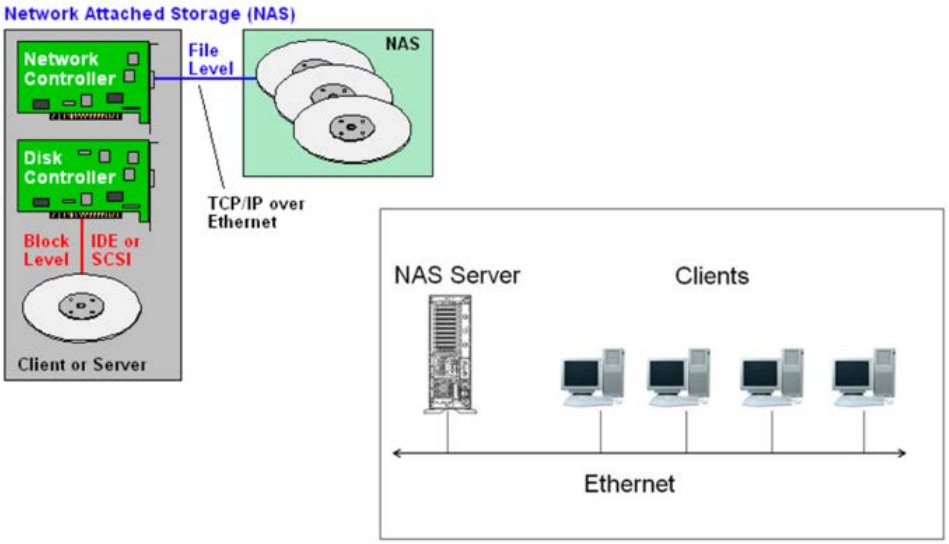
Τα δικτυακά αποθηκευτικά μέσα (Network Attached Storage)(NAS) είναι ένας τύπος αποθήκευσης που χρησιμοποιείται συχνά σε εταιρείες, διότι είναι ένας οικονομικός τρόπος παροχής μεγάλου αποθηκευτικού χώρου σε πολλαπλούς χρήστες.

Τα πιο σημαντικά χαρακτηριστικά τους είναι:

- Εύκολα στην εγκατάσταση και ρύθμιση.
- Εύκολη μέθοδος διασφάλισης πλεονασμού RAID σε πολλαπλούς χρήστες.
- Σας επιτρέπει να θέσετε δικαιώματα πρόσβασης σε φακέλους κι αρχεία για τους χρήστες.
- Υψηλή χρήση των αποθηκευτικών πόρων.

Αυτό το είδος αποθήκευσης έχει και μερικά μειονεκτήματα:

- Χρησιμοποιεί δικτυακούς πόρους(έχει τουλάχιστον μία διεύθυνση IP).
- Υπάρχει καθυστέρηση στη μεταφορά (latency)κι ίσως έχει και θέματα στη μεταφορά δεδομένων.
- Η απόδοση επηρεάζεται από τη διαθεσιμότητα του δικτύου.



Εικόνα 3.8. Δικτυακά Αποθηκευτικά Μέσα

Τα δίκτυα είναι από τη φύση τους ένα καλό μέσο διεξαγωγής επιθέσεων:

- Δεδομένου ότι πρόκειται για μετάδοση πληροφοριών, μπορούν να χρησιμοποιηθούν για την απομακρυσμένη επίθεση σε συστήματα που προφυλάσσονται από τη φυσική πρόσβαση (Content Delivery Network) (Δίκτυο Διανομής Περιεχομένου).

- Είναι εκτενή, οπότε είναι πολύ δύσκολο να ελέγξουμε αποτελεσματικά τη φυσική πρόσβαση, κάτι που γίνεται πρακτικά αδύνατο στα ασύρματα δίκτυα. Αν και ο έλεγχος φυσικής πρόσβασης δεν παρέχει εγγυήσεις, δεν πρέπει να παραλείπεται ποτέ.

Η πιστοποίηση και η κρυπτογράφηση είναι δύο κρίσιμα εργαλεία για την εξουδετέρωση πολλών επιθέσεων, αλλά ίσως δεν αρκούν.

Ο καταμερισμός των δικτύων σε διακριτές ζώνες ασφάλειας έχει κρίσιμη σημασία. Συνήθως γίνεται σε τρεις ζώνες:

- Content Delivery Network (εκεί βρίσκονται οι σέρβερ)
- Εσωτερικό δίκτυο χρηστών (intranet)
- Εξωτερικά δίκτυα (Internet)

Ο διαχωρισμός των ζωνών διασφαλίζεται με τη διασύνδεση μέσω routers,που αναλύουν και φιλτράρουν τις πληροφορίες που καθορίζουν τα τείχη προστασίας.

1.5.1. Συνδέσεις Wifi

Στα ασύρματα δίκτυα, ο έλεγχος φυσικής πρόσβασης είναι παντελώς αδύνατος(σε τέτοιου είδους δίκτυα, το σήμα μεταδίδεται μέσω των διαθέσιμων ραδιοφωνικών κυμάτων). Αν και τα ενσύρματα τοπικά δίκτυα υποστηρίζουν μεταγωγή πακέτων (packet switching)στο δεύτερο επίπεδο (π.χ.Ethernet), αυτά τα switches (μεταγωγείς)δε διαχωρίζουν τις εκπομπές τομέα (broadcast domains) και η λειτουργία τους μπορεί να τεθεί σε κίνδυνο. Από την πλευρά της ασφάλειας, μια υποδομή τέτοιου είδους πρέπει να θεωρείται πάντα αντίστοιχη με ένα δίκτυο μεριζόμενων μέσων επικοινωνίας (shared transmission medium): κάθε πακέτο που εκπέμπεται από κάποιον κόμβο παραδίδεται σε όλους τους άλλους κόμβους του δικτύου.

Στην αγορά υπάρχουν διάφοροι αλγόριθμοι που επιτρέπουν την κρυπτογράφηση των πακέτων που κυκλοφορούν στα δίκτυα WIFI.

Τα πιο κοινά παραδείγματα αυτών των αλγόριθμων ασφάλειας είναι:

- WEP-Wired Equivalent Privacy(Πρότυπο του 1999 ως το 2004.Μπορεί να σπάσει. Έχει εγκαταλειφθεί)
- WPA - WiFi Protected Access –Βελτιωμένη έκδοση του WEP. Σπάει εύκολα.
- WPA2-WiFi Protected Access έκδοση 2.Η κρυπτογράφηση AES(Advanced Encryption Standard) είναι η πιο σημαντική βελτίωση του WPA2 σε σχέση με το WPA.

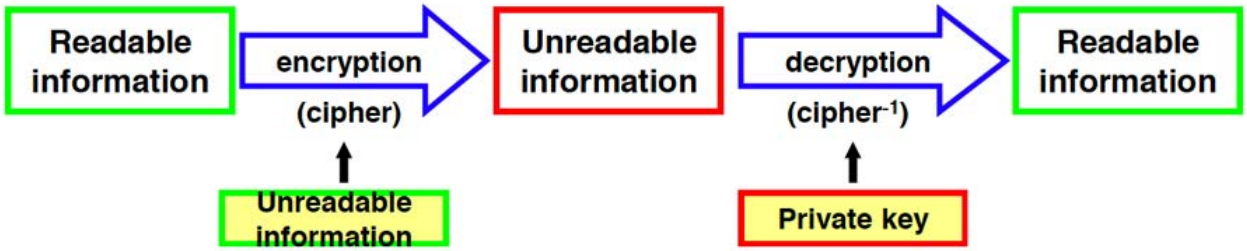
1.5.2. Ασφαλής Μεταφορά Δεδομένων - Ψηφιακές Υπογραφές

Η ψηφιακή υπογραφή είναι ένας τρόπος να διασφαλιστεί η αυθεντικότητα και/ ή η εχεμύθεια. Βασίζεται σε ένα ψηφιακό πιστοποιητικό, που αποτελείται από δύο κλειδιά(ένα ιδιωτικό, που θα το ξέρει μόνο ο ιδιοκτήτης του πιστοποιητικού, και ένα δημόσιο κλειδί, που είναι δημόσια γνωστό).Αυτή η μέθοδος λέγεται ασύμμετρη κρυπτογράφηση (asymmetric encryption),διότι ένα κρυπτογραφημένο μήνυμα μπορεί να αποκρυπτογραφηθεί μόνο με το άλλο κλειδί.

PKI (Public Key Infrastructure) (Υποδομή Δημοσίου Κλειδιού)

- Χρησιμοποιείται για κρυπτογράφηση, αποκρυπτογράφηση και πιστοποίηση (ψηφιακή υπογραφή)
- Το δημόσιο κλειδί αποκαλύπτεται ελεύθερα και μπορεί να χρησιμοποιηθεί για κρυπτογράφηση.
- Η αποκρυπτογράφηση γίνεται με το ιδιωτικό κλειδί (μυστικό).
- Δεν είναι αμφίδρομη, διότι το ζεύγος κλειδιών επιτρέπει την εχεμύθεια μόνο κατά μία έννοια.

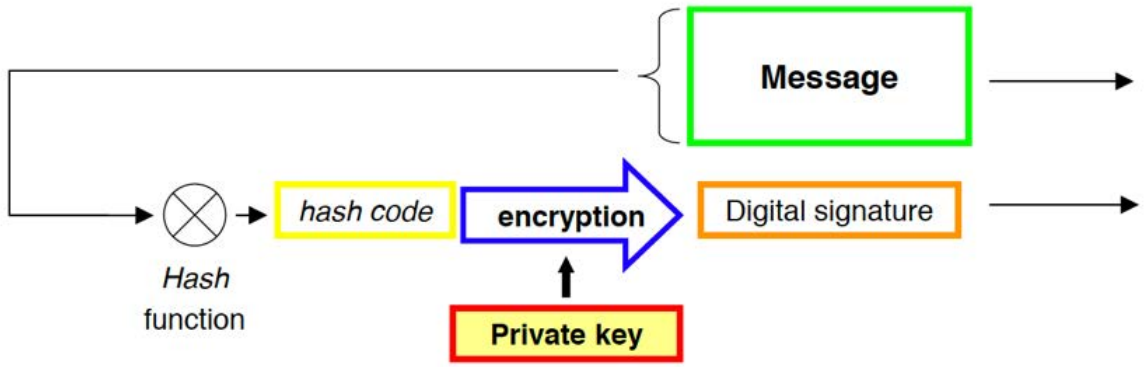
Ο διαχωρισμός των ζωνών διασφαλίζεται μέσω της διασύνδεσης των routers,που αναλύουν και φιλτράρουν τις πληροφορίες που καθορίζουν τα τείχη ασφάλειας.



Εικόνα 3.9. Ψηφιακή Υπογραφή

Ένα ζευγάρι δημόσιου κλειδιού/ιδιωτικού κλειδιού διασφαλίζει την εχεμύθεια μόνο προς μια κατεύθυνση. Για αμφίδρομη εχεμύθεια, χρειάζονται δύο ζευγάρια κλειδιών. Η εφαρμογή της αμφίδρομης κρυπτογράφησης με το ιδιωτικό κλειδί σε έναν κωδικό κατακερματισμού (hashcode) επιτρέπει την απλή ενσωμάτωση όλων των λειτουργιών μιας ψηφιακής υπογραφής , επιβεβαιώνοντας:

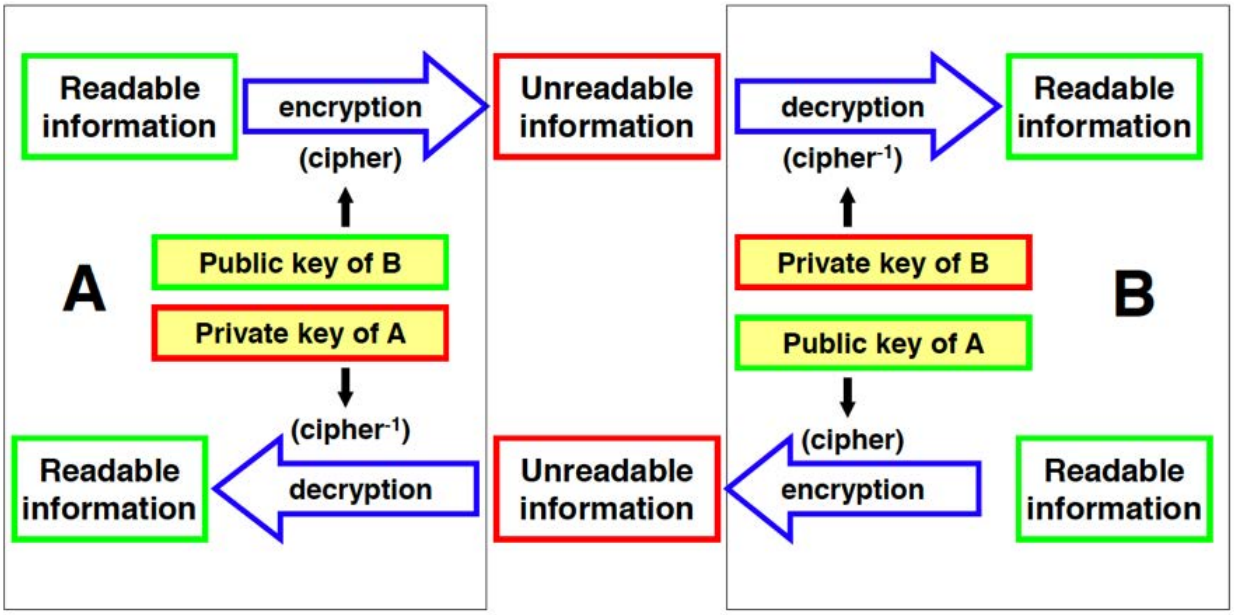
- Την ακεραιότητα του περιεχομένου
- Την πιστοποίηση του δημιουργού
- Τη μη απόρριψη (μόνο ο δημιουργός έχει το ιδιωτικό κλειδί)



Εικόνα 3.10. Ακεραιότητα και αυθεντικότητα

1.5.2.1.Εχεμύθεια με κρυπτογραφήματα ασύμμετρου κλειδιού

Η χρήση ενός δημοσίου κλειδιού για την κρυπτογράφηση μηνύματος διασφαλίζει την εχεμύθεια, αφού το κρυπτογραφημένο μήνυμα θα αποκρυπτογραφηθεί μόνο με το ιδιωτικό κλειδί του χρήστη.



Εικόνα 3.11. Εχεμύθεια με κρυπτογραφήματα ασύμμετρου κλειδιού

3.3 Ακεραιότητα Δεδομένων

Description

Table of contents

Η ακεραιότητα μπορεί να οριστεί ως εμπιστοσύνη προς την αξιοπιστία του συστήματος και την αποτροπή της μη εξουσιοδοτημένης αλλαγής δεδομένων.

Διασφαλίζει ότι οι επιθέσεις και τα σφάλματα δε θέτουν σε κίνδυνο τις πληροφορίες και το σύστημα.

Μπορεί να επιτευχθεί μέσω:

- Καλής διαχείρισης των δυνατοτήτων του συστήματος
- Μηχανισμούς εντοπισμού εισβολέων
- Κατάλληλου ελέγχου πρόσβασης

Χωρίς εγγύηση ακεραιότητας, ένα σύστημα μπορεί να λειτουργεί με λανθασμένα δεδομένα χωρίς να το ξέρει.

Τα αντίγραφα ασφάλειας και η αποθήκευσή τους είναι ένα από τα πιο σημαντικά μέτρα που πρέπει να πάρει μια εταιρεία για να προστατέψει τη δουλειά της.

Είναι σημαντικό να:

- Κάνουμε τακτικά αντίγραφα ασφάλειας (η περιοδικότητα πρέπει να εκτιμάται ανά περίπτωση)

- Φτιάχνουμε αντίγραφα ασφάλειας σε αξιόπιστα μέσα ή στο εταιρικό cloud(αυτό θα πρέπει να έχει πλεονάζοντα αντίγραφα ασφάλειας)

- Αν χρησιμοποιούμε φυσικά μέσα για τα αντίγραφα ασφάλειας, οι συσκευές πρέπει να βρίσκονται σε ασφαλή κι απομακρυσμένη τοποθεσία.

1.1.1. Σωστό και ασφαλές μέρος για τα αντίγραφα ασφαλείας

Το μέρος που βρίσκονται τα αντίγραφα ασφάλειας είναι κρίσιμο για την όλη διαδικασία. Λόγω των απρόβλεπτων καταστροφών, τα αντίγραφα ασφάλειας πρέπει να βρίσκονται σε πάνω από μία τοποθεσία. Οι εταιρείες μπορούν να διατηρούν ένα τοπικό αντίγραφο ασφάλειας στις εγκαταστάσεις τους, αλλά πρέπει να έχουν κι άλλο ένα αντίγραφο σε εξωτερική τοποθεσία (είτε στο cloud είτε σε κάποια άλλη εταιρική εγκατάσταση).

1.1.2. Κατακερματισμός (Hash) των αρχείων με αντίγραφα ασφαλείας

Τα αρχεία των αντιγράφων ασφάλειας πρέπει να κατακερματιστούν (hashed) για να διασφαλιστεί ότι δεν έχουν τροποποιηθεί.

Η διαδικασία χρησιμοποιεί έναν αλγόριθμο κρυπτογράφησης, όπως είναι ο MD5. Η χρήση τέτοιων αλγόριθμων σε ένα αρχείο, δίνει έναν αριθμό/κώδικα που παίζει τον ρόλο του αναγνωριστικού. Αν έχει αλλάξει το αρχείο, το αποτέλεσμα της εφαρμογής του αλγορίθμου θα είναι διαφορετικό και έτσι θα εντοπιστεί αν έχει γίνει κάποια μη εξουσιοδοτημένη αλλαγή.

Όταν γίνει ένα αντίγραφο ασφάλειας, δημιουργείται ένας κώδικας κατακερματισμού, που βασίζεται στην εφαρμογή ενός αλγόριθμου κρυπτογράφησης. Ο κατακερματισμός μπορεί να χρησιμοποιηθεί αργότερα για να κριθεί το αν άλλαξε το αρχείο.

1.1.3. Δοκική των αντιγράφων ασφαλείας (2)

«Φανταστείτε ότι οδηγείτε και ξαφνικά ακούτε έναν δυσοίωνο ήχο από το πίσω μέρος του αυτοκινήτου σας: θαμπ, θαμπ, θαμπ. Καθώς δυσκολεύει ο έλεγχος του αυτοκινήτου, αρχίζετε να συνειδητοποιείτε τι έγινε: Σας έσκασε το λάστιχο.

Κανένα πρόβλημα. Βρείτε ένα ασφαλές σημείο και βγάλτε τη ρεζέρβα από το πορτμπαγκάζ. Να, όμως, που είναι και αυτή σκασμένη.

Οι διαχειριστές αποθηκευτικού χώρου περνάνε μια αντίστοιχη κρίση κάθε μέρα. Λόγω απροσεξίας, λάθους ή βλάβης στο κεντρικό μέσο αποθήκευσης, χρειάζεται ξαφνικά να ανοίξουμε συγκεκριμένα αρχεία, που είναι αποθηκευμένα στα μέσα με τα αντίγραφα ασφάλειας (backup media). Αλλά τα αντίγραφα ασφάλειας λείπουν, είναι παλιά ή είναι ελαττωματικά. Όπως ο άτυχος οδηγός, έτσι καο ο διαχειριστής αποθηκευτικού χώρου αντιμετωπίζει πια μια δύσκολη κατάσταση, που θα μπορούσε εύκολα να είχε αποφευχθεί με στοιχειώδη προσχεδιασμό, όπως είναι η δοκιμή των αντιγράφων ασφάλειας.

Να τι πρέπει να κάνετε.

1. Καταλάβετε τη σοβαρότητα της τακτικής δοκιμής των αντιγράφων ασφάλειας. Όπως είναι σημαντικό να δοκιμάζετε μια ρεζέρβα για να βεβαιωθείτε ότι θα λειτουργήσει όταν τη χρειαστείτε, έτσι πρέπει να δοκιμάζετε και τα αντίγραφα ασφάλειας, είπε ο Girish Dadge, διευθυντής προϊόντος της Sungard Availability Services. Πρόσθεσε ότι «Η δοκιμή των αντιγράφων σας, σας δίνει την ευκαιρία να βεβαιωθείτε ότι λειτουργούν σωστά οι πολιτικές και τα προγράμματά σας για τα αντίγραφα ασφάλειας».

2. Καταστρώστε τεκμηριωμένο πλάνο δοκιμής των αντιγράφων ασφάλειας. «Η εξοικείωση με το τεκμηριωμένο πλάνο δοκιμών διασφαλίζει ότι οι υπάλληλοι έχουν τις ικανότητες και την εμπειρία που απαιτείται για την επιτυχή ανάκτηση δεδομένων, και δίνει αυτοπεποίθηση στον οργανισμό», είπε ο Eamonn Fitzmaurice, πρωτοπόρος σε παγκόσμιο επίπεδο στην προστασία δεδομένων, που εργάζεται στην εταιρεία υπηρεσιών IT, HPEPointnext.

3. Κάντε ρουτίνα τη δοκιμή των αντιγράφων ασφάλειας. Για να διασφαλιστεί η εγκυρότητα και η ακεραιότητα ενός αντιγράφου, είναι σημαντικό να γίνονται τακτικές δοκιμές ανάκτησης. «Δεν είναι ασυνήθιστο να βρούμε οργανισμούς με συστήματα που δεν προστατεύονται από ένα πρόγραμμα backup», μας εξήγησε ο Fitzmaurice. Η τακτική και διεξοδική δοκιμή των αντιγράφων είναι μια στρατηγική που μπορεί να τονίσει τις ανωμαλίες, ώστε να παρθούν διορθωτικά μέτρα.

4. Δοκιμάστε μια ολιστική προσέγγιση. Οι οργανισμοί πρέπει να καταλάβουν τη δομή των δεδομένων τους και τον λόγο που φτιάχνουν αντίγραφα ασφάλειας. Μετά πρέπει να αναπτύξουν ένα πλάνο δοκιμής αντιγράφων, που να πληροί τις προϋποθέσεις τους.

Κάθε οργανισμός έχει διαφορετικούς στόχους για τα αντίγραφά του. «Για παράδειγμα, η τραπεζική βιομηχανία χρειάζεται αντίγραφα για συμμόρφωση, έλεγχο και νομικούς λόγους», είπε ο Dadge. «Οιοργανισμοίυγείαςέχουνπροσωπικάδεδομένα, οπότε πρέπει να εστιάσουν στην ασφάλεια, στην αποθήκευση και στις νομικές απαιτήσεις.Όλεςοιδοκιμέςεπαναφοράςκιανάκτησηςθαπρέπεινασυμπεριλαμβάνουν δοκιμές δεδομένων, εφαρμογών και κατάστασης συστήματος», πρότεινε ο Dadge.

5. Κάντε τακτικές δοκιμές σύμφωνα με τα τακτικά προγράμματα. Ιδανικά, η δοκιμή πρέπει να γίνεται μετά από κάθε νέο backup,για να διασφαλιστεί ότι η ανάκτηση δεδομένων μπορεί να γίνει επιτυχώς. Ωστόσο, αυτό δεν είναι πάντα πρακτικό, λόγω έλλειψης διαθέσιμων πόρων ή λόγω χρονικών περιορισμών. «Κάθε οργανισμός πρέπει να κάνει κατ'ελάχιστον εβδομαδιαίες ή μηνιαίες επαναφορές συστημάτων, εφαρμογών και μεμονωμένων αρχείων, ελέγχοντας ότι τα δεδομένα είναι έγκυρα και προσβάσιμα όπως πρέπει», είπε ο Marty Puranik, CEO της Atlantic.Net, που είναι πάροχος υπηρεσιών φιλοξενίας στο cloud. «Αυτό θα δώσει στον οργανισμό σας κι ένα ρεαλιστικό χρονικό πλαίσιο ανάκτησης, όταν συμβεί η καταστροφή».

Δεν είναι όλα τα δεδομένα ίσα. Αυτό πρέπει να επιδρά στην τακτικότητα της δοκιμής των αντιγράφων. «Μερικά δεδομένα είναι πιο σημαντικά από άλλα», είπε ο Atif Malik, διευθυντής στην μονάδα CIO Advisory της KPMG. Για παράδειγμα, τα δεδομένα συμμόρφωσης και ρύθμισης του νόμου Sarbanes-Oxley θεωρούνται πιο σημαντικά από τα δεδομένα μάρκετινγκ. «Πρέπει να τεθούν σε εφαρμογή συστήματα ελέγχου για τον μετριασμό των ρίσκων, με βάση τη σημασία των δεδομένων», συμβούλεψε ο Malik.

6. Εκμεταλλευτείτε πλήρως την αυτοματοποίηση. Η αυτοματοποίηση θα πρέπει να παίξει κεντρικό ρόλο σε κάθε στρατηγική δοκιμής των αντιγράφων ασφάλειας. «Οι οργανισμοί πρέπει να προσπαθήσουν να αυτοματοποιήσουν όσο πιο πολύ γίνεται τη δοκιμή των αντιγράφων τους, για να διασφαλιστεί η συνοχή κι η εγκυρότητα των δεδομένων, καθώς επίσης και για να μειωθεί το βάρος στο προσωπικό που έχει αναλάβει τη δοκιμή των backups»,πρότεινε ο Puranik. «Κάντε δοκιμές ανάκτησης πλήρων συστημάτων σε εικονικά μηχανήματα, όπως επίσης και δοκιμές ανάκτησης εφαρμογών, βάσεων δεδομένων και μεμονωμένων αρχείων», πρόσθεσε.

7. Βεβαιωθείτε ότι η δοκιμή καλύπτει τα πάντα. Αν η δοκιμή του backup δε δοκιμάζει την επαναφορά όλου του εργασιακού όγκου, τότε δε θεωρείται πραγματική δοκιμή. «Πολλοί οργανισμοί θα επαναφέρουν απλά κάνα δυο αρχεία από το αρχείο και θα θεωρήσουν ότι έκαναν τη δοκιμή με επιτυχία», ανέφερε ο Chris Wahl, επικεφαλής τεχνολόγος στον πάροχο διαχείρισης δεδομένων cloud,Rubrik. «Αυτή η ροή εργασιών δεν έχει καμία σχέση με την πραγματική επαναφορά πολύπλοκων εφαρμογών και πρέπει να αποφεύγεται όταν γίνεται μια πραγματική δοκιμή των αντιγράφων».

8. Κάντε τη δοκιμή αντιγράφων αναπόσπαστο τμήμα της εταιρικής ανάπτυξης εφαρμογών και της κυκλοφορίας τους. Οι δοκιμές των αντιγράφων πρέπει να είναι στο μυαλό όλων όσων αναπτύσσουν και παρουσιάζουν νέες εφαρμογές στον οργανισμό. «Οι πιο επιτυχημένες στρατηγικές διαχείρισης εταιρικών δεδομένων απαιτούν να γνωρίζουμε πώς και πότε πρέπει να κάνουμε δοκιμές εγκυρότητας των αντιγράφων, προτού επιτρέψουμε στα δεδομένα να προχωρήσουν στην παραγωγή», μας εξήγησε ο Wahl.

9. Διασφαλίστε την ακρίβεια των αντιγράφων. Μετά την ανάκτηση των δεδομένων, οι διαχειριστές αποθηκευτικού χώρου και βάσεων δεδομένων μπορούν να κάνουν έναν αρχικό «λογικό έλεγχο» των δεδομένων. «Ωστόσο, οι τελικοί χρήστες των εταιρικών εφαρμογών είναι συχνά στην πιο κατάλληλη θέση να αναγνωρίσουν αν τα ανακτημένα δεδομένα είναι ακριβή και συμφωνούν με τα αυθεντικά», παρατήρησε ο Fitzmaurice.

10. Να έχετε παραπανίσια backups. Μην κάνετε ποτέ backupσε μια κασέτα ή σε ένα συγκεκριμένο σετ κασετών. «Αν χρησιμοποιείτε κασέτες, να τις αντικαθιστάτε τακτικά», πρότεινε ο Brian Engert, επικεφαλής προγραμματιστής στην εταιρεία σχεδιασμού λογισμικού για τρίτους πελάτες, Soliant Consulting.

[2] πηγή: https://searchdatabackup.techtarget.com/tip/Ten-important-steps-for-testing-backups

Άσκηση 1. Αντίγραφο (backup) κρίσιμων πληροφοριών

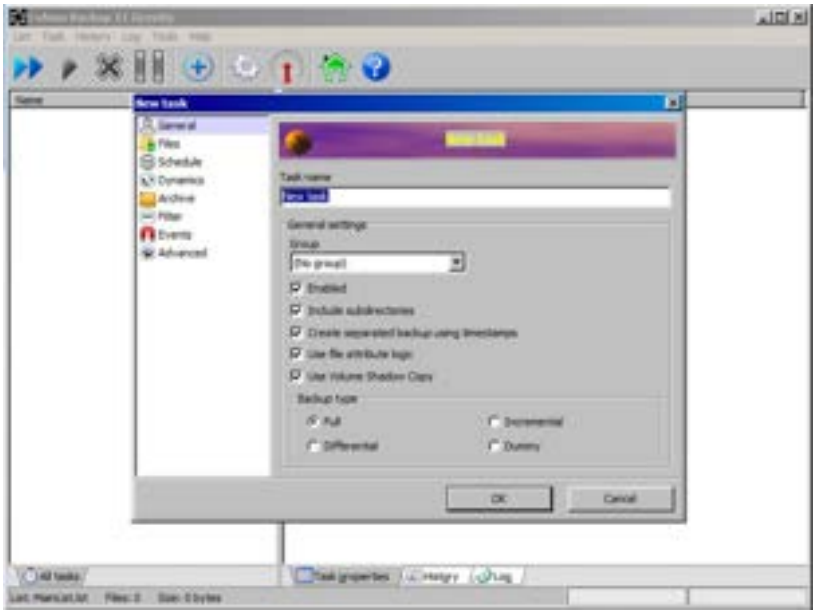
Στο internet θα βρείτε πολλές λύσεις για να πάρετε backup. Μερικές απο αυτές είναι:

- COBIAN BACKUP (https://www.cobiansoft.com)
- GOOGLE BACKUP AND SYNC (https://www.google.com/intl/en-GB_ALL/drive/download/backup-and-sync)
- ACRONIS (https://www.acronis.com/en-us/business/overview/)

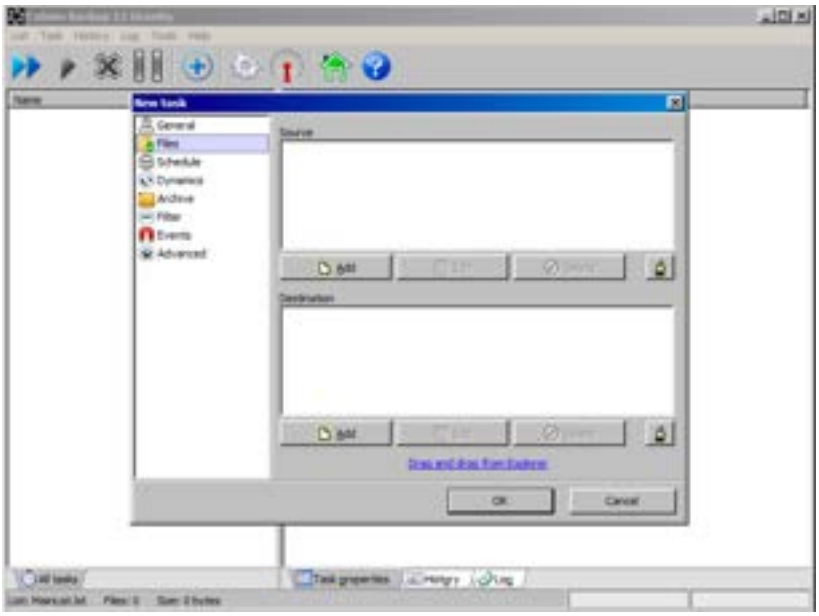
Χρησιμοποιήστε ένα από αυτά για να δημιουργήσετε ένα τοπικό αντίγραφο ασφαλείας σε μια εξωτερική τοποθεσία (σκληρός δίσκος, pendrive, sdcard, κ.λπ.) ή για να δημιουργήσετε ένα απομακρυσμένο αντίγραφο ασφαλείας (remote backup) σε μια offsite τοποθεσία.

Παράδειγμα για το Cobian Backup:

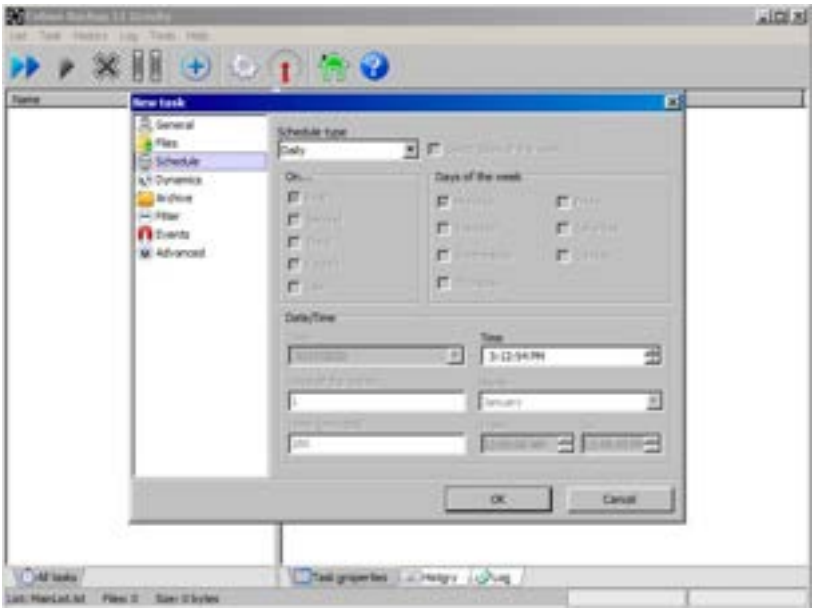
1. Κατεβάστε και εγκαταστήστε το πρόγραμμα.
2. Δημιουργήστε μια νέα εργασία (Task → New task) και επιλέξτε τον τύπο του αντιγράφου ασφαλείας (backup) που θέλετε (Full, Incremental and Differential)



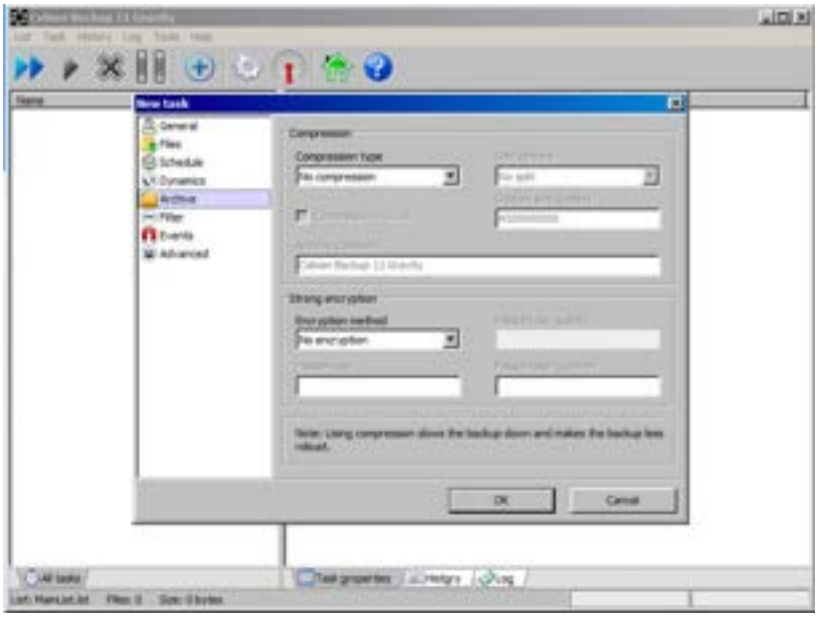
3. Στο μενού Files επιλέξτε τα αρχεία που θέλετε να περιέχονται στο backup καθώς και το που αυτό θα αποθηκευτεί (μπορεί να είναι ένας τοπικός κατάλογος, ένας εξωτερικός δίσκος ή μια τοποθεσία προσβάσιμη μέσω ftp).



4. Στο μενού Schedule επιλέξτε την συχνότητα με την οποία θα γίνεται το backup (καθημερινά, εβδομαδιαία ή μηνιαία).



5. Στο μενού Archive μπορείτε να επιλέξετε να γίνεται συμπίεση αν είναι σημαντικό να συμπιέζετε τα δεδομένα πριν απο το backup.



Παρατηρήσεις

Παρατήρηση 1: Τα αντίγραφα ασφαλείας των πληροφοριών μιας εταιρείας πρέπει να γίνονται με γνώση και εξουσιοδότηση της διοίκησης.

Παρατήρηση 2: Τα αντίγραφα ασφαλείας πρέπει να συμμορφώνονται με τους κανονισμούς της Ευρωπαϊκής Ένωσης (ΕΕ) που περιγράφονται στον Γενικό Κανονισμό Προστασίας Δεδομένων. Για παράδειγμα, είναι σημαντικό να κατανοήσετε εάν μπορείτε να δημιουργήσετε αντίγραφα ασφαλείας δεδομένων που σχετίζονται με άτομα για τοποθεσίες εκτός ΕΕ (και στην περίπτωση που πρέπει να το κάνετε ποιες προϋποθέσεις πρέπει να διασφαλίσετε).

Άσκηση 2. Ασφαλής επικοινωνία μέσω e-mail.

Για να λάβετε κρυπτογραφημένο email ή να στείλετε ψηφιακά υπογεγραμμένο email, πρέπει να έχετε ένα ψηφιακό πιστοποιητικό.

Για να εγκαταστήσετε το ψηφιακό σας πιστοποιητικό στο Mozilla Thunderbird ώστε να υπογράφετε ψηφιακά ή να κρυπτογραφείτε τα email, ακολουθήστε αυτές τις οδηγίες:

1. Στο Thunderbird, κάντε κλικ στο "Μενού" και μετά τοποθετήστε το δείκτη του ποντικιού πάνω από την ενότητα "Επιλογές" ή "Προτιμήσεις".

2. Κάντε κλικ στην ενότητα "Ρυθμίσεις λογαριασμού". Στη συνέχεια κάντε κλικ στην καρτέλα "Ασφάλεια".

3. Κάντε κλικ στο κουμπί "Προβολή πιστοποιητικών". στη συνέχεια κάντε κλικ στο κουμπί "Εισαγωγή".

4. Εντοπίστε το αντίγραφο ασφαλείας για το πιστοποιητικό σας και κάντε κλικ στο "Άνοιγμα".

5. Θα σας ζητηθεί να εισαγάγετε τον κωδικό πρόσβασης του πιστοποιητικού. Εισάγετε τον κωδικό και στη συνέχεια κάντε κλικ στο "ΟΚ". (Ο κωδικός πρόσβασης δημιουργίας αντιγράφων ασφαλείας είναι ο κωδικός πρόσβασης που επιλέξατε κατά την εξαγωγή / δημιουργία αντιγράφων ασφαλείας του πιστοποιητικού.)

Διαμορφώστε το Thunderbird με ένα προεπιλεγμένο πιστοποιητικό

1. Στο Thunderbird, κάντε κλικ στο "Μενού" και μετά τοποθετήστε το δείκτη του ποντικιού πάνω από την ενότητα "Επιλογές" ή "Προτιμήσεις".

2. Κάτω από την "Επικεφαλίδα λογαριασμού email" (ίσως χρειαστεί να την αναπτύξετε), κάντε κλικ στο "Ασφάλεια".

3. Δίπλα στο πλαίσιο "Χρησιμοποιήστε αυτό το πιστοποιητικό για να υπογράψετε ψηφιακά τα μηνύματα που στέλνετε", κάντε κλικ στο "Επιλογή".

4. Επιλέξτε το σωστό ψηφιακό πιστοποιητικό για χρήση. Λάβετε υπόψη ότι η διεύθυνση email του λογαριασμού σας πρέπει να αντιστοιχεί στη διεύθυνση email του πιστοποιητικού.

5. Δίπλα στο πλαίσιο "Χρησιμοποιήστε αυτό το πιστοποιητικό για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων που σας έχουν σταλεί", κάντε κλικ στο "Επιλογή".

6. Κατά τη σύνταξη ενός νέου email, κάντε κλικ στο μενού Ασφάλεια και επιλέξτε "Ψηφιακή υπογραφή αυτού του μηνύματος".

Περισσότερες οδηγίες σχετικά με τον τρόπο χρήσης ψηφιακών πιστοποιητικών στο Mozilla Thunderbird μπορείτε να δείτε εδώ:
https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages#w_sending-a-digitally-signed-and-or-encrypted-emai

Κρυπτογράφηση / Αποκρυπτογράφηση ενός μηνύματος

Δίνετε το δημόσιο κλειδί σας στον υπόλοιπο κόσμο. Όταν κάποιος θέλει να σας στείλει ένα κρυπτογραφημένο μήνυμα, χρησιμοποιεί το δημόσιο κλειδί σας - που όλοι γνωρίζουν- για την κρυπτογράφηση. Μόνο το ιδιωτικό σας κλειδί (που δεν πρέπει ποτέ να κοινοποιηθεί σε κανέναν) θα επιτρέψει την αποκρυπτογράφηση και την ανάγνωση του μηνύματος. Ένα ψηφιακό πιστοποιητικό σας επιτρέπει να λαμβάνετε, αλλά όχι να στέλνετε κρυπτογραφημένα email.

Η ασφαλής αμφίδρομη επικοινωνία επιτυγχάνεται όταν και τα δύο μέρη της επικοινωνίας έχουν στην κατοχή τους ένα ψηφιακό πιστοποιητικό και το καθένα απο αυτά γνωρίζει το δημόσιο κλειδί του άλλου. Αυτά τα δύο άτομα έχουν πλέον την ίδια ικανότητα και μπορούν να στέλνουν κρυπτογραφημένα μηνύματα μεταξύ τους χρησιμοποιώντας ο ένας το δημόσιο κλειδί του άλλου και να τα αποκρυπτογραφούν με το ιδιωτικό τους κλειδί.

Εάν διαθέτετε ένα ψηφιακό πιστοποιητικό από τη χώρα σας (ενσωματωμένο στην ταυτότητα σας) ή από το ίδρυμά σας, προσπαθήστε να το χρησιμοποιήσετε για να υπογράψετε τα email σας και να τα κρυπτογραφήσετε για να κατανοήσετε τη διαφορά μεταξύ αυτών των δύο προσεγγίσεων.