Θεματική ενότητα ΔΕΟ 45

ΜΑΘΗΜΑ
#11
[10/3/22]

Τόμος Β’

ΚΕΦΑΛΑΙΟ 4-5-8

ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ ΔΙΟΙΚΗΣΗΣ

Eclass4U

The best Choice for you

ΘΕΡΜΟΠΥΛΩΝ 17
ΠΕΡΙΣΤΕΡΙ
100Μ ΑΠΟ ΤΗ ΣΤΑΣΗ
ΜΕΤΡΟ «ΠΕΡΙΣΤΕΡΙ»

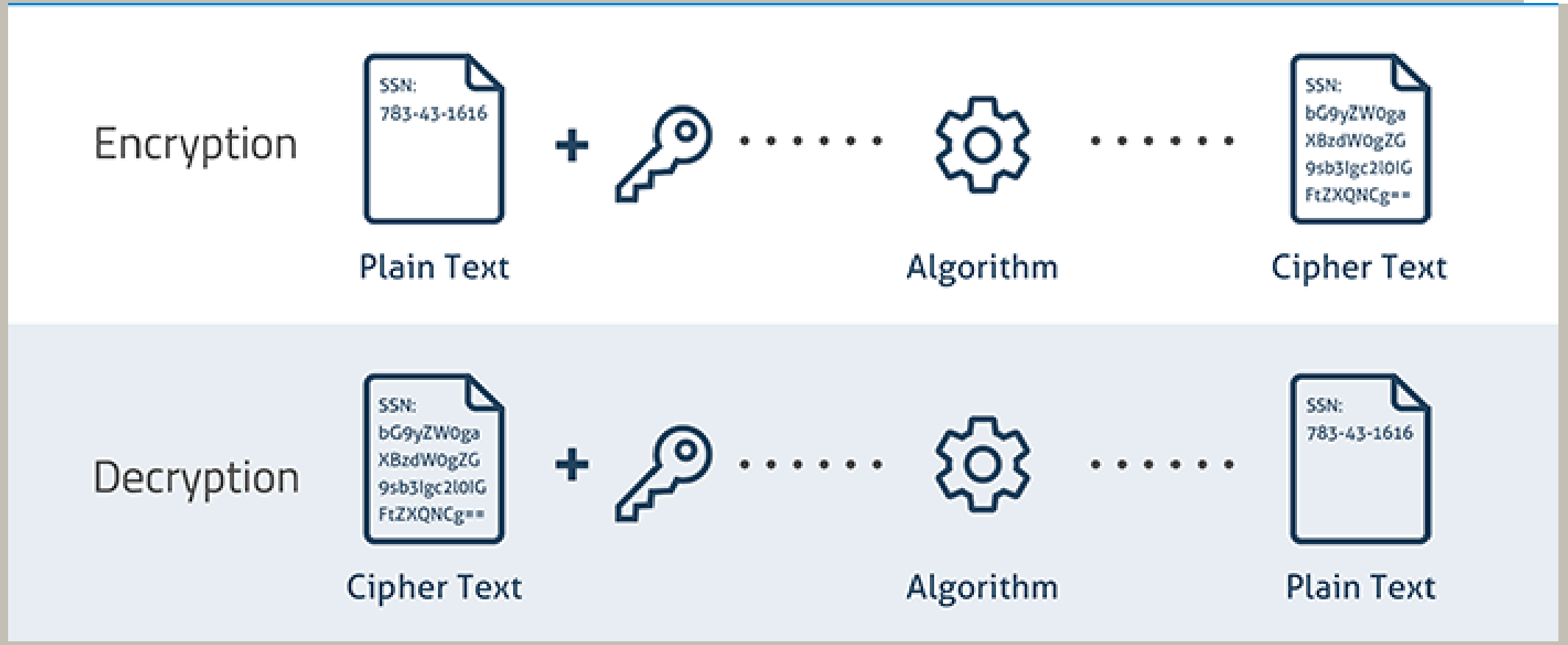
ΤΗΛΕΦΩΝΟ: 210-5711484
ΚΙΝΗΤΟ: 6970401981
EMAIL:grammateia.eclass4u@gmail.com
ΤΟΠΟΘΕΣΙΑ WEB : www.eclass4u.gr
SOCIAL MEDIA:

Καθηγήτρια Κατερίνα Μαργαριτοπούλου
Katerinam.eclass4u@gmail.com

Κρυπτογράφηση και Αποκρυπτογράφηση

- Η κρυπτογράφηση (encryption) είναι η διαδικασία κατά την οποία ο αποστολέ μετατρέπει την αρχική πληροφορία σε άλλη μορφή και μεταδίδει το προκύπτον ακατανόητο μήνυμα μέσω ενός ανοικτού δικτύου.
- Ο αποστολέας χρησιμοποιεί έναν αλγόριθμο κρυπτογράφησης και ένα κλειδί για τη μετατροπή του απλού κειμένου (αρχικού μηνύματος) σε κρυπτοκείμενο (κρυπτογραφημένο μήνυμα).
- Το απλό κείμενο (plaintext) είναι τα δεδομένα που πρέπει να προστατευθούν κατά τη διάρκεια της μετάδοσης.
- Το κρυπτοκείμενο (cipher text) είναι το κωδικοποιημένο κείμενο που παράγεται ως αποτέλεσμα του αλγόριθμου κρυπτογράφησης για τον οποίο χρησιμοποιείται ένα συγκεκριμένο κλειδί.
- Ο αλγόριθμος κρυπτογράφησης είναι ένας κρυπτογραφικός αλγόριθμος στον οποίο εισάγεται ένα απλό κείμενο και ένα κλειδί κρυπτογράφησης και παράγει ένα κρυπτογραφημένο κείμενο.

Κρυπτογράφηση και Αποκρυπτογράφηση



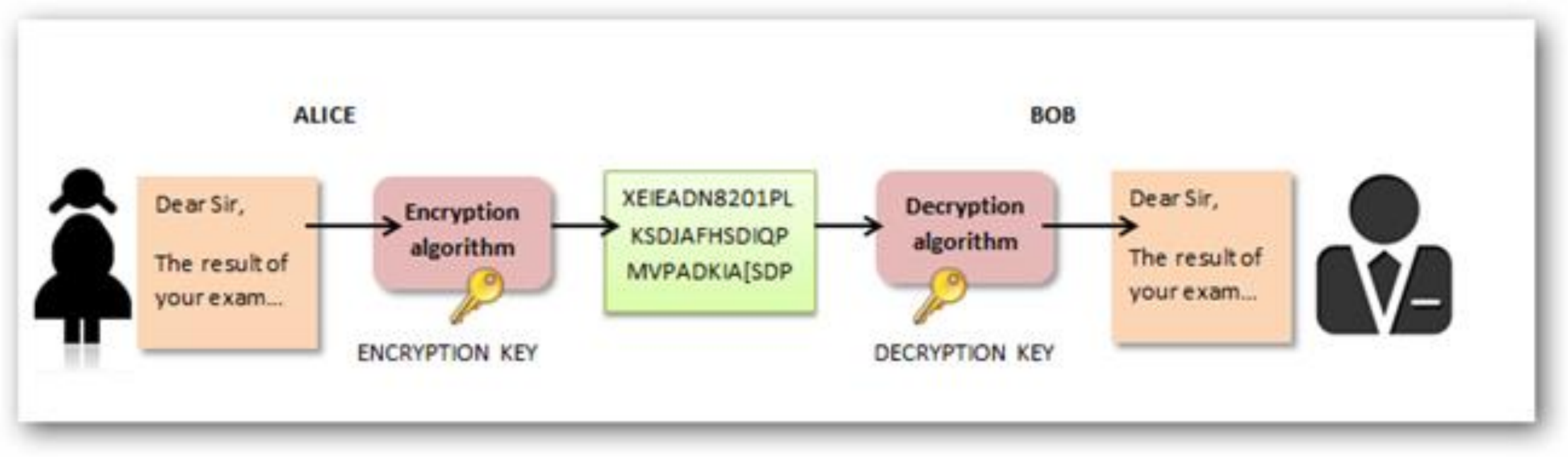
Κρυπτογράφηση και Αποκρυπτογράφηση

- Η **αποκρυπτογράφηση (decryption)** αναστρέφει τη διαδικασία της κρυπτογράφησης για να μετατρέψει το μήνυμα στην αρχική του μορφή.
- Ο δέκτης χρησιμοποιεί έναν **αλγόριθμο αποκρυπτογράφησης** και ένα κλειδί για να μετατρέψει το κρυπτοκείμενο στο αρχικό, απλό κείμενο.
- Ο **αλγόριθμος αποκρυπτογράφησης** είναι μια μαθηματική διαδικασία που χρησιμοποιείται για την αποκρυπτογράφηση και παράγει το αρχικό απλό κείμενο ως αποτέλεσμα οποιουδήποτε δεδομένου κρυπτογραφημένου κειμένου και του κλειδιού αποκρυπτογράφησης.
- Είναι η αντίστροφη διαδικασία του αλγόριθμου κρυπτογράφησης.

Κλειδιά κρυπτογράφησης και αποκρυπτογράφησης

- είναι τυχαία σειρά δυαδικών ψηφίων (bits) που δημιουργούνται ειδικά για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων.
- Τα κλειδιά που χρησιμοποιούνται για κρυπτογράφηση και αποκρυπτογράφηση μπορεί να είναι είτε παρόμοια είτε ανόμοια, ανάλογα με τον τύπο των κρυπτοσυστημάτων που χρησιμοποιούνται (κρυπτογράφηση συμμετρικού κλειδιού ή κρυπτογράφηση ασύμμετρου ή δημόσιου κλειδιού).
- Κάθε κλειδί είναι μοναδικό και δημιουργείται μέσω ενός αλγορίθμου ώστε να εξασφαλιστεί ότι δεν είναι προβλέψιμο. Τα κλειδιά παράγονται συνήθως με γεννήτριες τυχαίων αριθμών ή με αλγορίθμους υπολογιστών που μιμούνται γεννήτριες τυχαίων αριθμών.
- Η **κρυπτογράφηση συμμετρικού κλειδιού (symmetric key encryption)** αναφέρεται στους αλγορίθμους που χρησιμοποιούν το ίδιο μυστικό κλειδί τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση.

Κλειδιά κρυπτογράφησης και αποκρυπτογράφησης



Κρυπτογράφηση με Δημόσιο Κλειδί

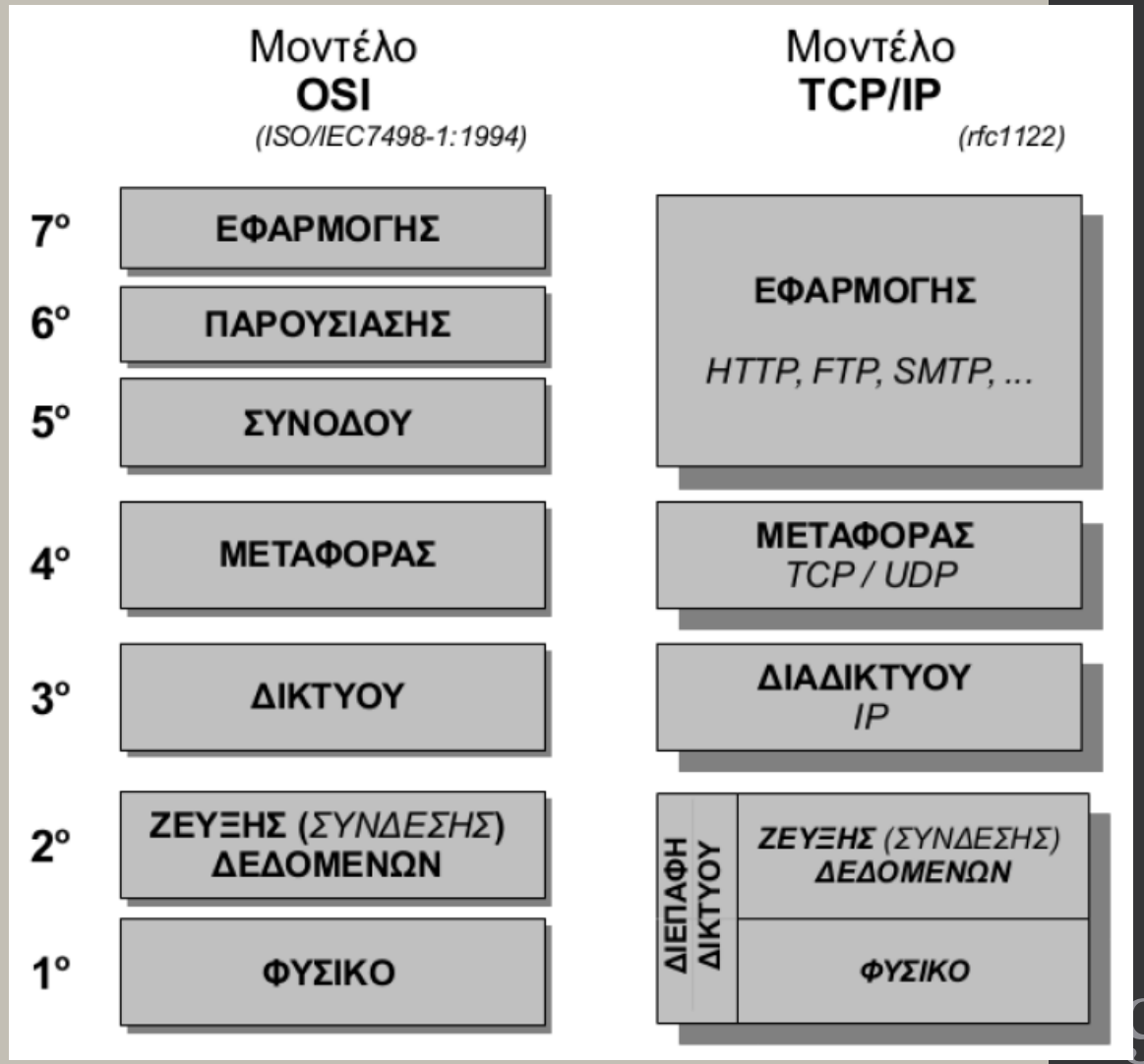
Ένα σύστημα κρυπτογράφησης με δημόσιο κλειδί μπορεί να θεωρηθεί ως μία σειρά δημόσιων και ιδιωτικών κλειδιών, τα οποία κλειδώνουν τα δεδομένα όταν αυτά μεταδίδονται και τα ξεκλειδώνουν κατά την παραλαβή τους. Ο αποστολέας εντοπίζει το δημόσιο κλειδί του παραλήπτη σε έναν κατάλογο και το χρησιμοποιεί για να κρυπτογραφήσει ένα μήνυμα. Το μήνυμα στέλνεται κρυπτογραφημένο μέσω του Διαδικτύου ή ενός ιδιωτικού δικτύου. Όταν φτάσει στον προορισμό του, ο παραλήπτης αποκρυπτογραφεί τα δεδομένα με το δικό του ιδιωτικό κλειδί και διαβάζει το μήνυμα.

Κρυπτογράφηση

- Οι εφαρμογές μηνυμάτων, όπως το Signal ή το Whatsapp, χρησιμοποιούν κρυπτογράφηση από άκρο σε άκρο για την προστασία της εμπιστευτικότητας και της ιδιωτικότητας των επικοινωνιών των χρηστών και για την εξακρίβωση της ταυτότητας των χρηστών.
- Στην κρυπτογράφηση από άκρο σε άκρο, κρυπτογραφούνται μόνο τα δεδομένα. Η βάση για την κρυπτογράφηση από άκρο σε άκρο είναι ένα πρωτόκολλο (Signal Protocol), το οποίο έχει αναπτυχθεί από την εταιρεία Open Whisper Systems. Αυτό το πρωτόκολλο κρυπτογράφησης από άκρο σε άκρο έχει σχεδιαστεί για να εμποδίζει τα τρίτα μέρη και την εταιρεία παραγωγής της εφαρμογής να έχουν ελεύθερη πρόσβαση σε μηνύματα ή κλήσεις.
- Επιπλέον, ακόμη και αν τα κλειδιά κρυπτογράφησης από τη συσκευή ενός χρήστη έχουν παραβιαστεί, δεν μπορούν να χρησιμοποιηθούν για την αποκρυπτογράφηση μηνυμάτων που έχουν σταλεί στο παρελθόν.
- Η κρυπτογράφηση των μηνυμάτων υλοποιείται χρησιμοποιώντας ασύμμετρη και συμμετρική κρυπτογράφηση. Η ασύμμετρη κρυπτογράφηση χρησιμοποιείται για την προετοιμασία της κρυπτογραφημένης συνομιλίας μεταξύ δύο χρηστών, ενώ η συμμετρική κρυπτογράφηση χρησιμοποιείται κατά τη διάρκεια της επικοινωνίας.

Χρήση ασύμμετρης και συμμετρικής κρυπτογράφησης: HTTPS

- Ενώ η κρυπτογράφηση στις εφαρμογές μηνυμάτων χρησιμοποιείται για την ταυτοποίηση των χρηστών – ανθρώπων – το HTTPS χρησιμοποιείται για την ταυτοποίηση μηχανών. Σε έναν εξαιρετικά συνδεδεμένο κόσμο, όπου καθημερινά μεταφέρονται εκατομμύρια ευαίσθητα δεδομένα μέσω του διαδικτύου, η ανάγκη διασφάλισης των διαύλων επικοινωνίας μεταξύ πελατών / browsers και διακομιστών (servers) είναι υψίστης σημασίας.
- Το HTTPS είναι ένα πρωτόκολλο του μοντέλου TCP/IP, το οποίο είναι ο συνδυασμός του πρωτοκόλλου ασφαλείας SSL/TLS (Secure Sockets Layer / Transport Layer Security) πάνω στο πρωτόκολλο HTTP (Hyper Text Transmission Protocol). Ουσιαστικά το HTTPS είναι η πράσινη κλειδαριά που βλέπουμε αριστερά από τη διεύθυνση της ιστοσελίδας που επισκεπτόμαστε.



η κυβερνοεπίθεση που έπληξε τα πληροφοριακά συστήματα των ΕΛΤΑ

η κυβερνοεπίθεση που έπληξε τα πληροφοριακά συστήματα των ΕΛΤΑ

- στόχος ήταν η κρυπτογράφηση των κρίσιμων συστημάτων για την επιχειρησιακή λειτουργία των ΕΛΤΑ. Η επίθεση ξεκίνησε από κακόβουλο λογισμικό μηδενικού χρόνου, το οποίο εγκαταστάθηκε σε σταθμό εργασίας και με την τεχνική https reverse shell συνδέθηκε σε υπολογιστικό σύστημα το οποίο ελεγχόταν από ομάδα κυβερνοεγκληματιών.
- Για την επίλυση του τεχνικά δύσκολου αυτού έργου εξετάζονται ένα προς ένα περισσότερα από 2500 τερματικά συστήματα για λόγους IT ασφαλείας, ενώ ταυτόχρονα εγκαθίστανται και προγράμματα agents.
- Στόχος αποτελεί κατά την εταιρεία η άμεση επαναλειτουργία του εμπορικού πληροφοριακού συστήματος, η ασφάλεια όλων των δεδομένων και η ταχύτερη εξομάλυνση στην λειτουργία των καταστημάτων. Όπως τονίζεται, οι αρμόδιες υπηρεσίες Πληροφορικής, σε σύμπραξη με τους ειδικούς στο IT Security συνεργάτες, εργάζονται σε 24ωρη βάση για την πλήρη αποκατάσταση των πληροφοριακών συστημάτων και την επαναφορά της ασφαλούς λειτουργίας του δικτύου.

Ευχαριστώ πολύ