

1.1 Βασικοί κανόνες ασφαλείας

Κάποιοι από τους βασικούς κανόνες ασφαλείας είναι οι εξής:

1. Αλλαγή κωδικών ανά τακτά χρονικά διαστήματα

Οι κωδικοί αποτελούν το συνηθέστερο τρόπο αυθεντικοποίησης υποκειμένων στα πληροφοριακά συστήματα. Είναι ένα μέσο διατήρησης της ακεραιότητας και εμπιστευτικότητας των δεδομένων με αποτέλεσμα να χρήζει ιδιαίτερης σημασίας η πολυπλοκότητα και η συχνότητα αλλαγής του. Προτείνεται η αλλαγή κωδικών ανά τακτά χρονικά διαστήματα πχ. ανά δύο μήνες.

2. Εγκατάσταση αντιϊκού προγράμματος (anti - virus)

Τα ιομορφικά λογισμικά είναι το συνηθέστερο μέσο παραβίασης ενός πληροφοριακού συστήματος. Παρόλο που υπάρχουν πλέον πολυμορφικά λογισμικά τα οποία μπορούν να παραβιάσουν οποιοδήποτε πληροφοριακό σύστημα, κρίνεται αναγκαία η εγκατάσταση αντιϊκών προγραμμάτων τα οποία αποτρέπουν την εκτέλεσή του ιού και ελαχιστοποιούν την εξάπλωση του σε άλλα πληροφοριακά συστήματα.

3. Ενημερώσεις προγραμμάτων

Ένα σύνηθες φαινόμενο είναι η καθυστέρηση ενημερώσεων των προγραμμάτων, το οποίο όμως αποτελεί και ευπάθεια για ένα πληροφοριακό σύστημα. Κρίνεται απαραίτητη η αυτόματη ενημέρωση των προγραμμάτων εφόσον δεν επηρεάζεται η λειτουργικότητα των εφαρμογών ενός πληροφοριακού συστήματος.

4. Αποφυγή εκτέλεσης συνημμένων μέσω μηνυμάτων ηλεκτρονικής αλληλογραφίας (E-mail attachments)

Ο συνηθέστερος τρόπος μετάδοσης των ιομορφικών λογισμικών γίνεται μέσω συνημμένων αρχείων κατά την αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας (e-mail). Προτείνεται η αποφυγή εκτέλεσης συνημμένων από άγνωστους αποστολείς ειδικά εάν το πληροφοριακό σύστημα δεν έχει εγκατεστημένο κάποιο ιομορφικό λογισμικό.

5. Διατήρηση αντιγράφων ασφαλείας (Backup)

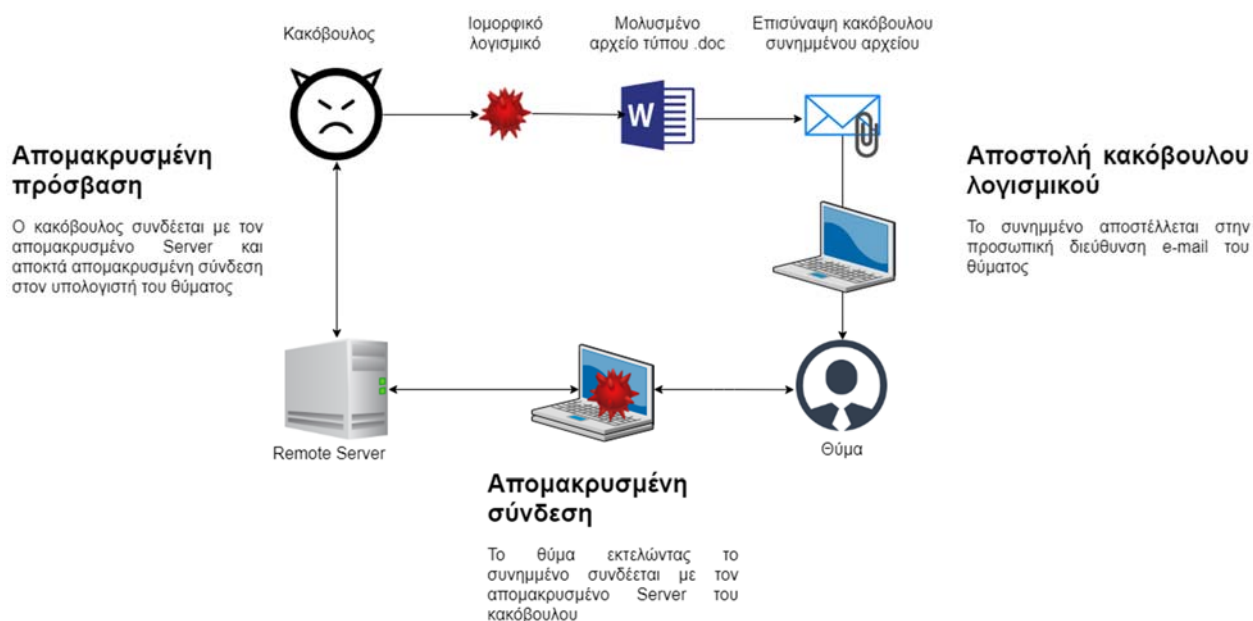
Ένα απλό μέτρο διασφάλισης της διαθεσιμότητας των δεδομένων είναι η διατήρηση αντιγράφων ασφαλείας. Η διατήρηση των δεδομένων μπορεί να γίνει είτε μέσω κάποιου φυσικού μέσου όπως ένας σκληρός εξωτερικός δίσκος ή μέσω κάποιας υπηρεσίας Cloud. Με βάση ωστόσο το γενικό κανονισμό προστασίας των προσωπικών δεδομένων, η διατήρηση των αντιγράφων ασφαλείας, εφόσον γίνεται μέσω Cloud υπηρεσίας, πρέπει να διασφαλίζεται η συμβατότητα του παρόχου με τον κανονισμό, ως εκτελών την επεξεργασία, όπως και η χώρα διατήρησης άρα και επεξεργασίας των δεδομένων.

1.2 Συνήθειες κυβερνοεπιθέσεις

1.2.1 Κακόβουλο λογισμικό (malicious software - malware)

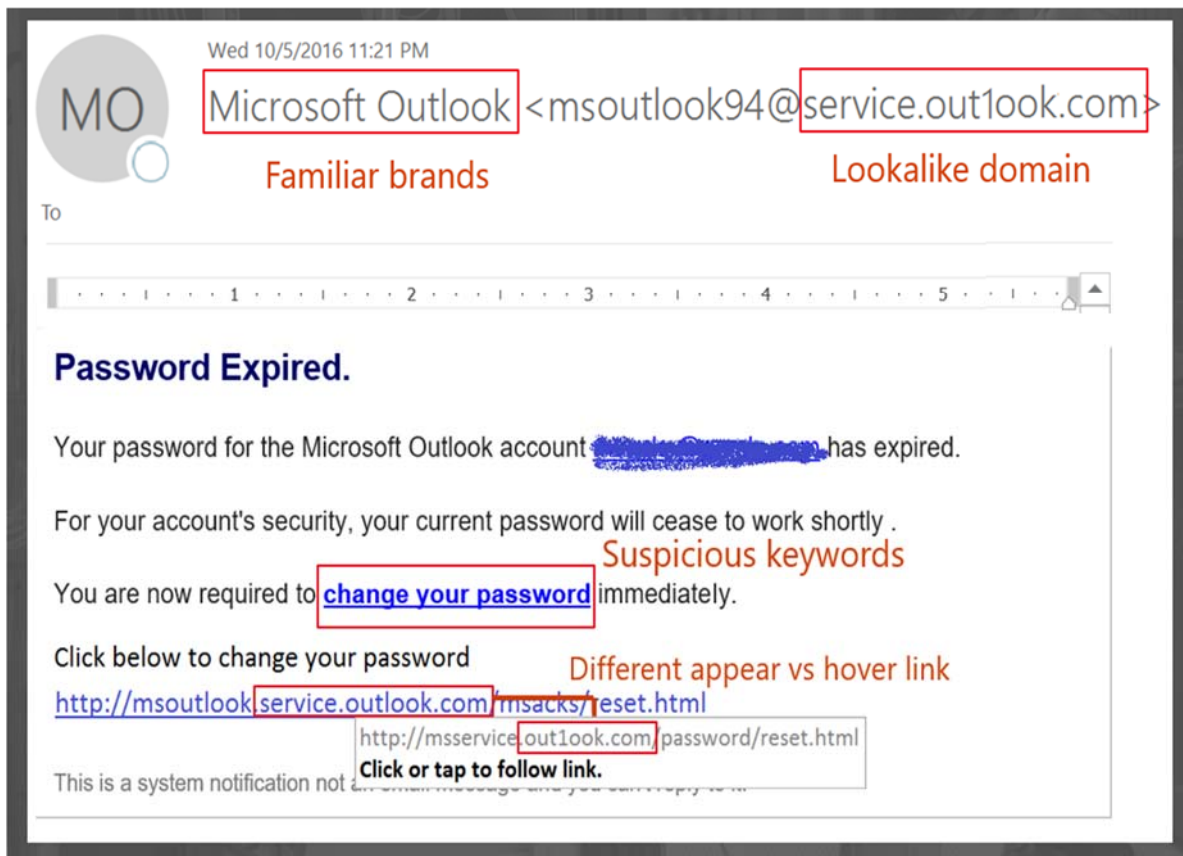
Οι τύποι των συνηθέστερων κακόβουλων λογισμικών περιγράφονται παρακάτω:

- **Ιός (virus)** - Λογισμικό το οποίο μεταδίδεται μεταξύ των πληροφοριακών συστημάτων. Μπορεί να αλλοιώσει, να κλέψει ή να διαγράψει τα δεδομένα του χρήστη.
- **Worm** – Κακόβουλο λογισμικό το οποίο αντιγράφει τον εαυτό του από τον έναν υπολογιστή στον άλλον χωρίς την ανθρώπινη παρέμβαση.
- **Δούρειος Ίππος (Trojan horse)** – Κακόβουλο λογισμικό το οποίο μπορεί να αποθηκεύσει κωδικούς μέσω την καταγραφή της κίνησης του πληκτρολογίου ακόμη και να καταγράψει βίντεο μέσω της κάμερας.
- **Rootkits** – Κακόβουλο λογισμικό το οποίο επιτρέπει την πρόσβαση σε ένα υπολογιστικό σύστημα με δικαιώματα υπερχρήστη ενώ κρύβει την παρουσία του καθώς ενσωματώνεται σε βασικά αρχεία του λειτουργικού συστήματος ή άλλων εφαρμογών.



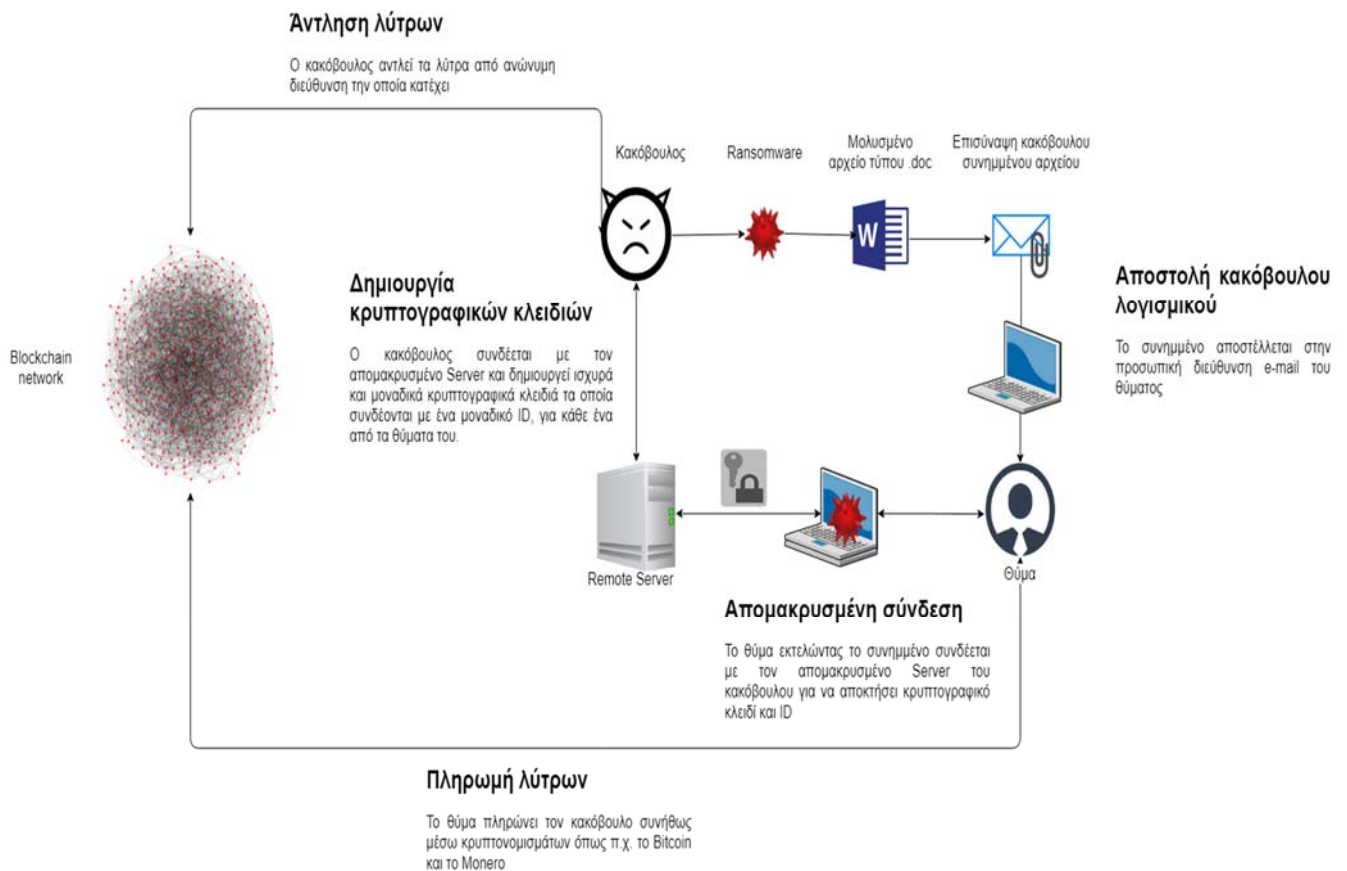
1.2.2 Επιθέσεις phishing μέσω κοινωνικής μηχανικής (Social engineering attack)

Οι επιθέσεις κοινωνικής μηχανικής αποτελούν τον κύριο τρόπο εξάπλωσης ιομορφικών λογισμικών. Ο επιτιθέμενος χρησιμοποιώντας συνήθως μηνύματα μέσω e-mail ξεγελά το υποκείμενο με τελικό σκοπό την εκτέλεση ιομορφικού λογισμικού το οποίο είτε επισυνάπτει είτε φιλοξενεί σε ιστοσελίδα. Συνήθως ο κακόβουλος χρήστης γνωρίζει λεπτομέρειες για τον παραλήπτη του μηνύματος μέσω των κοινωνικών δικτύων ή άλλων ευρέως διαθέσιμων ανοιχτών πηγών πληροφοριών (Open Source Intelligence - OSINT).



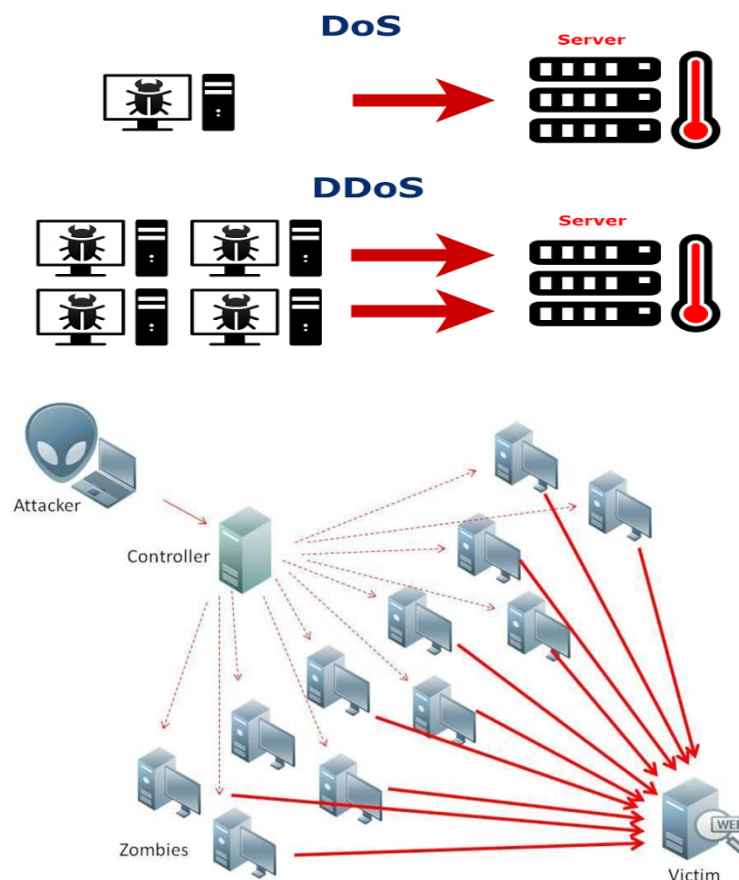
1.2.3 Ransomware

Το ransomware είναι κακόβουλο λογισμικό που εγκαθίσταται κρυφά στο πληροφοριακό σύστημα, κρυπτογραφεί τα δεδομένα του θύματος και απαιτεί την καταβολή λύτρων για να τα αποκρυπτογραφήσει. Η καταβολή των λύτρων γίνεται κυρίως μέσω κρυπτονομισμάτων και η μετάδοση του συνήθως μέσω e-mail. Μια από τις μαζικότερες κυβερνοεπιθέσεις παγκοσμίως, η οποία αφορούσε στο ransomware WannaCry, διήρκεσε 4 ημέρες, μόλυνε περίπου 300,000 υπολογιστές παγκοσμίως και κόστισε συνολικά 130,634.77 δολάρια.



1.2.4 Επιθέσεις άρνησης υπηρεσιών (Denial of Service)

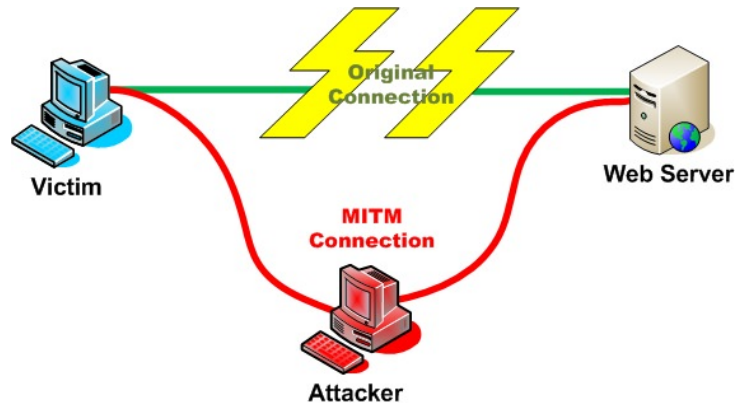
Επίθεση άρνησης υπηρεσιών ονομάζεται η επίθεση εναντίον ενός υπολογιστή ή υπηρεσίας, με σκοπό ο επιτιθέμενος να καταστήσει την πληροφοριακή υποδομή ανίκανη να εξυπηρετήσει άλλες συνδέσεις. Η κυριότερη μορφή των επιθέσεων αυτών είναι η καταναεμημένη επίθεση άρνησης εξυπηρέτησης κατά την οποία ο κακόβουλος χρήστης χρησιμοποιεί πολλαπλές συνδέσεις μέσω άλλων θυμάτων ή και θυτών (Distributed Denial of Service - DDoS). Παρόλα αυτά, η συγκεκριμένη επίθεση μπορεί να γίνει και χωρίς την κακόβουλη πρόθεση των χρηστών, όταν για παράδειγμα αρκετοί χρήστες συνδεθούν ταυτόχρονα σε μια ιστοσελίδα. Παρόλα αυτά η παραβιάζεται διαθεσιμότητα της υπηρεσίας και εν τέλει η ασφάλεια των δεδομένων.



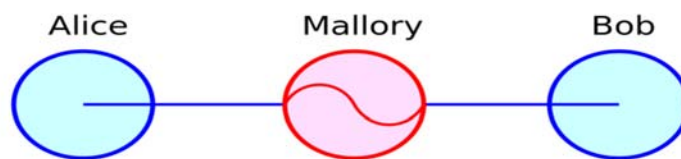
1.2.5 Επίθεση Man-in-the-Middle

Κατά την επίθεση Man-in-the-Middle (MITM) ο κακόβουλος χρήστης παρεμποδίζει την επικοινωνία δύο μερών, ελέγχοντας τη ροή της επικοινωνίας με σκοπό την απόσπαση των διαβιβαζόμενων πληροφοριών. Η επίθεση MITM γίνεται συνήθως με δύο, τρόπους:

- την υποκλοπή των δεδομένων (eavesdropping attack) και



- την αλλοίωση του μηνύματος από τον αποστολέα στον παραλήπτη και αντίστροφα.



1.2.6 Επαναχρησιμοποίηση κωδικών

Μια από τις συνηθέστερες κυβερνοεπιθέσεις είναι η εξαντλητική επίθεση εναντίων κωδικών (brute – force attack). Κατά την επίθεση, ο κακόβουλος χρησιμοποιεί γνωστές λίστες με τους συνηθέστερους κωδικούς παγκοσμίως, με σκοπό την προσπέλαση των δεδομένων ενός αυθεντικοποιημένου χρήστη. Η ευπάθεια πηγάζει από τη χρήση αδύναμων κωδικών και την επαναχρησιμοποίηση τους σε διάφορα πληροφοριακά συστήματα.

1.2.7 Προηγμένη επίμονη απειλή (Advanced Persistent Threat – APT)

Κατά την προηγμένη επίμονη απειλή, ο κακόβουλος χρήστης συνήθως καταρτίζεται από υψηλού επιπέδου τεχνικές ικανότητες, οργάνωση και κίνητρα, πραγματοποιεί μακροχρόνιες επιθέσεις στοχεύοντας στην αποκάλυψη πληροφοριών υψηλής σημασίας και πολλές φορές εθνικής ασφαλείας. Μια από τις γνωστότερες κυβερνοεπιθέσεις που εντάσσονται στα πλαίσια του κυβερνοπολέμου, είναι η επίθεση APT μέσω του ιού, τύπου Worm, Stuxnet το 2010. Βασικός στόχος του Stuxnet ήταν οι εγκαταστάσεις εμπλουτισμού ουρανίου του Ιράν. Ο ιός μόλυνε τα πληροφοριακά συστήματα μέσω USB, αποσκοπούσε στο σύστημα μετάδοσης εντολών των φυγόκεντρων που αξιοποιούνται για τον εμπλουτισμό ουρανίου, αλλάζοντας την ταχύτητα τους και εν τέλει καταστρέφοντας τους.

1.2.8 Μη εξουσιοδοτημένη πρόσβαση μέσω προεπιλεγμένων κωδικών πρόσβασης (Default Passwords)

Οι περισσότεροι πάροχοι εξοπλισμών πληροφοριακών συστημάτων, χρησιμοποιούν προεπιλεγμένους κωδικούς, ώστε οι τελικοί χρήστες να μπορούν με ευκολία να παραμετροποιούν τις εργοστασιακές ρυθμίσεις. Ωστόσο, τις περισσότερες φορές οι τελικοί χρήστες δεν γνωρίζουν τη συγκεκριμένη ιδιότητα με αποτέλεσμα η εργοστασιακή ρύθμιση από χαρακτηριστικό να γίνεται ευπάθεια.

1.2.9 Επίθεση SQL Injection (SQLi)

Η επίθεση SQL Injection αφορά στην παραβίαση βάσεων δεδομένων μέσω διαδικτυακών διεπαφών (Web Interfaces). Η βάση δεδομένων είναι ένα εργαλείο για τη συλλογή και την οργάνωση πληροφοριών. Σε αυτές τις πληροφορίες οργανώνονται κυρίως πληροφορίες αυθεντικοποίησης όπως το όνομα και ο κωδικός του χρήστη, ωστόσο υπάρχει η πιθανότητα αποθήκευσης και προσωπικών δεδομένων του χρήστη. Με την επίθεση SQLi παραβιάζεται η ασφάλεια των πληροφοριακών συστημάτων εφόσον χάνεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των δεδομένων.

```
[02:44:24] [INFO] postprocessing table dump
Database: dvwa
Table: users
[5 entries]
+-----+-----+
| user   | password                                     |
+-----+-----+
| 1337   | 8d3533d75ae2c3966d7e0d4fcc69216b (charley) |
| admin  | 5f4dcc3b5aa765d61d8327deb882cf99 (password)|
| gordonb| e99a18c428cb38d5f260853678922e03 (abc123)  |
| pablo  | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)|
| smithy | 5f4dcc3b5aa765d61d8327deb882cf99 (password)|
+-----+-----+
```

1.2.10 Μη εξουσιοδοτημένη πρόσβαση λόγω αδύναμων ή μη σωστών παραμετροποιημένων κανόνων ελέγχου προσπέλασης (Access control lists - ACL)

Ο επιτιθέμενος μπορεί να προσπελάσει προσωπικά δεδομένα χρηστών, λόγω της μη σωστής παραμετροποίησης των κανόνων ελέγχου προσπέλασης από το διαχειριστή του πληροφοριακού συστήματος. Σε αυτή την περίπτωση, ο επιτιθέμενος μπορεί να επαυξήσει τα δικαιώματά του, είτε οριζόντια σε δικαιώματα άλλου χρήστη, είτε κάθετα σε δικαιώματα υπερχρήστη.

1.3 Μέτρα ασφαλείας με σκοπό τον περιορισμό των κινδύνων παραβίασης και διαρροής πληροφοριών και δεδομένων

1.3.1 Αποφυγή πολιτικής Bring your own device (BYOD)

Η ραγδαία αύξηση της τεχνολογίας, έχει δημιουργήσει την ανάγκη προσπέλασης των δεδομένων, εταιρικών και προσωπικών, μέσω απομακρυσμένης πρόσβασης. Για παράδειγμα η πρόσβαση στα εταιρικά emails ή έγγραφα μπορεί να γίνει από το προσωπικό κινητό, υπολογιστή ή tablet. Τα τελευταία χρόνια αρκετές επιχειρήσεις υιοθετούν την πολιτική της χορήγησης εταιρικών συσκευών στους υπαλλήλους χωρίς να τους επιτρέπουν την πρόσβαση στις προσωπικές τους συσκευές. Με αυτό τον τρόπο περιορίζεται το περιθώριο διαρροής εταιρικών και προσωπικών δεδομένων καθώς και η μόλυνση του εσωτερικού δικτύου της εταιρείας από ιομορφικό λογισμικό.

1.3.2 Διαμόρφωση διαχειριστικών δικαιωμάτων

Αναγκαία κρίνεται η διαμόρφωση των δικαιωμάτων των χρηστών, με σκοπό τον περιορισμό των επιπτώσεων από μια παραβίαση πληροφοριακού συστημάτων. Η δημιουργία πίνακα προσπέλασης (access matrix), ο οποίος ορίζει τα δικαιώματα εκτέλεσης, ανάγνωσης και εγγραφής αρχείων ελαχιστοποιεί την κάθετη και οριζόντια επαύξηση δικαιωμάτων (vertical & horizontal privilege escalation).

1.3.3 Διεξαγωγή τακτικών ελέγχων ασφαλείας

Με βάση τα διεθνή πρότυπα ασφαλείας και τον Γενικό Κανονισμό Προστασίας των προσωπικών δεδομένων κρίνεται απαραίτητη η τακτική διεξαγωγή ελέγχων ασφαλείας όπως ο έλεγχος διείσδυσης, η προσομοίωση κυβερνοεπίθεσης και η αποτίμηση κινδύνων. Σκοπός των ελέγχων είναι η αποτίμηση των πληροφοριακών συστημάτων, η ανίχνευση κινδύνων και ευπαθειών και τέλος η πρόταση τεχνικών και οργανωτικών μέτρων για τη διασφάλιση της πληροφοριακής υποδομής.

1.3.4 Εγκατάσταση τοίχους προστασίας (Firewall)

Το firewall είναι μια τεχνολογία λογισμικού ή υλικού με σκοπό τον έλεγχο της εισερχόμενης ή εξερχόμενης διαδικτυακής κίνησης μέσω της ανάλυσης των διερχόμενων πακέτων και ανάλογα με την πολιτική, τα απορρίπτει ή τα αποδέχεται. Επίσης προτείνεται η εγκατάσταση τοίχους προστασίας στο επίπεδο εφαρμογής (application layer) π.χ. στο πρωτόκολλο HTTP όπου υπάρχει το τοίχος προστασίας διαδικτυακών εφαρμογών (Web Application Firewall - WAF).

1.3.5 Εγκατάσταση συστήματος ανίχνευσης εισβολών (IDS)

Το σύστημα ανίχνευσης εισβολών, είναι υλοποίηση υλικού ή λογισμικού με σκοπό την συνεχή ενημέρωση της κίνησης του δικτύου για τον εντοπισμό κακόβουλων δραστηριοτήτων και περιστατικών ασφαλείας καθώς και την ενημέρωση των διαχειριστών σε πραγματικό χρόνο ώστε να δράσουν αναλόγως.

1.3.6 Εγκατάσταση συστήματος αποτροπής εισβολών (IPS)

Το σύστημα αποτροπής εισβολών μοιάζει αρκετά με το IDS αλλά διαφοροποιείται ως προς τη διαχείριση των συμβάντων παραβίασης πληροφοριακών συστημάτων. Κατά την αναγνώριση κακόβουλων πακέτων στη δικτυακή επικοινωνία το IPS απορρίπτει τα πακέτα και φράσσει την κίνηση από τη διεύθυνση της πηγής επαναφέροντας τη σύνδεση όταν αυτή απαιτείται.

1.3.7 Τμηματοποίηση και απομόνωση δικτύου

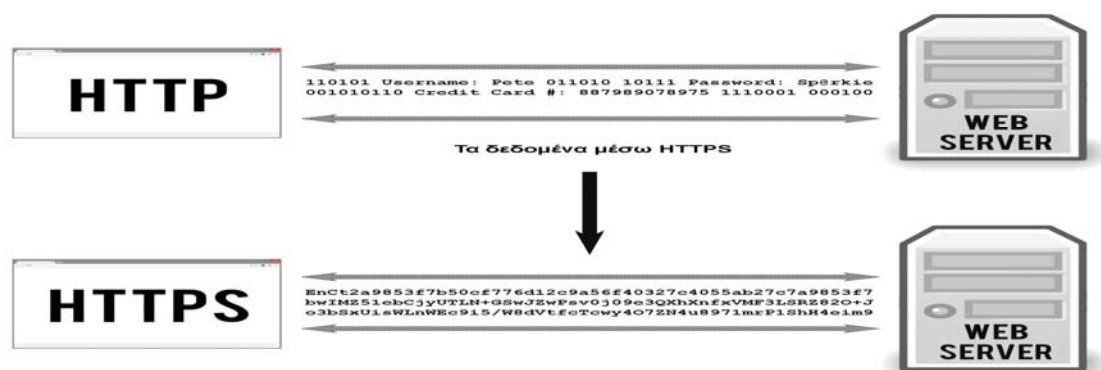
Η τμηματοποίηση δικτύου περιλαμβάνει τον διαχωρισμό του δικτύου σε μικρότερα δίκτυα και η απομόνωση καθορίζει μέσω των κανόνων ποιες συσκευές επιτρέπεται να επικοινωνούν με άλλες συσκευές στο δίκτυο. Ελαχιστοποιείται με αυτό τον τρόπο η προσπέλαση δεδομένων από χρήστες που δεν την χρειάζονται. Συνήθως επιτυγχάνεται μέσω του firewall ή τη δημιουργία εικονικών υποδικτύων (Virtual Lan - Vlan).

1.3.8 Αποτροπή διαρροής δεδομένων (Data leak prevention - DLP)

Η αποτροπή διαρροής δεδομένων είναι μια τεχνολογία η οποία αναγνωρίζει και αποτρέπει πιθανά τρωτά σημεία στην ασφάλεια των πληροφοριακών συστημάτων που αφορούν στη μεταφορά απόρρητων πληροφοριών εκτός του δικτύου ενός οργανισμού. Χρησιμοποιεί κυρίως λέξεις κλειδιά, μεταδεδομένα και στατιστικές αναλύσεις για να εντοπίσει εμπιστευτικές ή απόρρητες πληροφορίες στην εξερχόμενη κίνηση.

1.3.9 Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση των δεδομένων μέσω έγκυρων κρυπτογραφικών αλγορίθμων ενισχύει την εμπιστευτικότητα των δεδομένων. Μπορεί να υλοποιηθεί μέσω διαφόρων πρωτοκόλλων όπως τις VPN συνδέσεις που υλοποιούνται με IPsec ή μέσω της κρυπτογράφησης των δεδομένων που μεταφέρονται μέσω του ιστού με τη χρησιμοποίηση πιστοποιητικού SSL/TLS.



1.3.10 Επιμόρφωση προσωπικού

Η επιμόρφωση του προσωπικού είναι το μοναδικό μη τεχνικό μέσο περιορισμού των κινδύνων παραβίασης αλλά ίσως και το πιο σημαντικό. Κρίνεται απαραίτητη η επιμόρφωση του προσωπικού σε θέματα ασφαλείας προσωπικών δεδομένων, στη γνωστοποίηση των νέων επιθέσεων και τεχνολογιών και ο έλεγχος ετοιμότητας σε πραγματικά γεγονότα.

1.4 Κρυπτογραφία

Με τον όρο κρυπτογραφία εννοούμε τη μελέτη μαθηματικών αλγορίθμων που στοχεύουν στην εξασφάλιση της εμπιστευτικότητας και ακεραιότητας των δεδομένων, πιστοποιώντας την ασφαλή μετάδοση και διασφάλιση της πληροφορίας και της ταυτότητας του αποστολέα της.

1.4.1 Ορολογία

Κρυπτογράφηση (encryption): ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.

Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται **αποκρυπτογράφηση (decryption)**.

Κρυπτογραφικός αλγόριθμος (cipher): είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

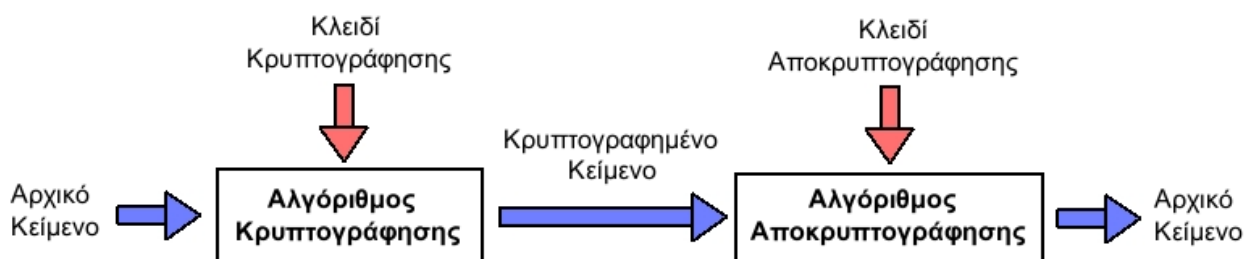
Αρχικό κείμενο (plaintext): είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (key): είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (ciphertext): είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (cryptanalysis): είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί.

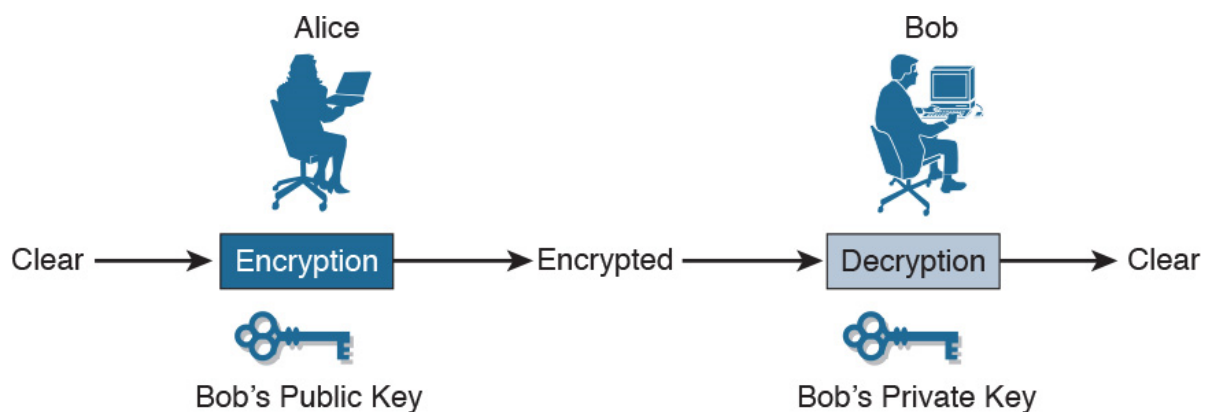
Η διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης φαίνεται στο παρακάτω σχήμα.



1.4.2 Ασύμμετρη κρυπτογραφία

Οι ασύμμετροι αλγόριθμοι ή αλγόριθμοι δημοσίου κλειδιού είναι σχεδιασμένοι έτσι ώστε το κλειδί που χρησιμοποιείται για την κρυπτογράφηση να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση. Πέρα από αυτό, το κλειδί αποκρυπτογράφησης δεν μπορεί να υπολογιστεί από το κλειδί κρυπτογράφησης. Οι αλγόριθμοι αυτοί καλούνται και "δημοσίου κλειδιού" γιατί το κλειδί κρυπτογράφησης μπορεί να δημοσιοποιηθεί. Ο καθένας μπορεί να κρυπτογραφήσει ένα μήνυμα με το δημόσιο κλειδί αλλά μόνο αυτός που διαθέτει το αντίστοιχο ιδιωτικό κλειδί μπορεί να το αποκρυπτογραφήσει.

Παραδείγματα ασύμμετρων αλγορίθμων είναι οι RSA, ElGamal και DSA.

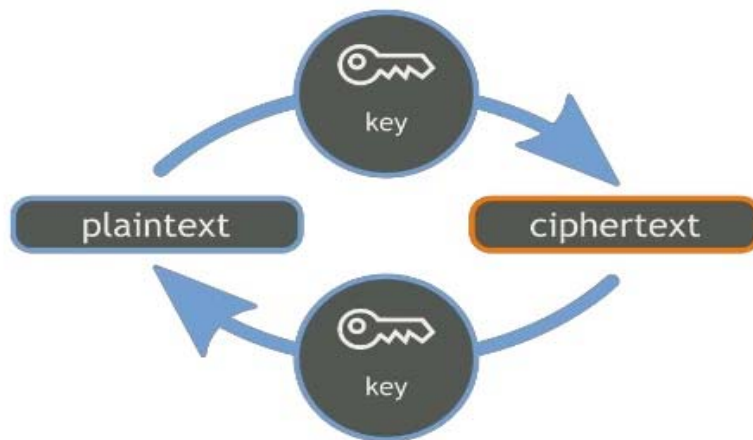


1.4.3 Συμμετρική κρυπτογραφία

Στους συμμετρικούς αλγόριθμους το κλειδί κρυπτογράφησης μπορεί να υπολογιστεί από το κλειδί που χρησιμοποιείται για την αποκρυπτογράφηση και το ανάποδο. Μάλιστα στις περισσότερες περιπτώσεις τα κλειδιά κρυπτογράφησης και αποκρυπτογράφησης είναι τα ίδια. Αυτοί οι αλγόριθμοι χρειάζονται την συμφωνία μεταξύ του αποστολέα και του παραλήπτη για το κλειδί που θα χρησιμοποιηθεί, για να μπορέσουν να επικοινωνήσουν με ασφάλεια. Η ασφάλεια των αλγορίθμων βασίζεται στην μυστικότητα αυτού του κλειδιού. Για όσο καιρό επιθυμούμε η επικοινωνία να παραμείνει μυστική, για τον ίδιο καιρό πρέπει και το κλειδί να παραμείνει μυστικό.

Παραδείγματα συμμετρικών αλγορίθμων είναι οι DES, IDEA, RC5 και SAFER.

SYMMETRIC CRYPTOGRAPHY

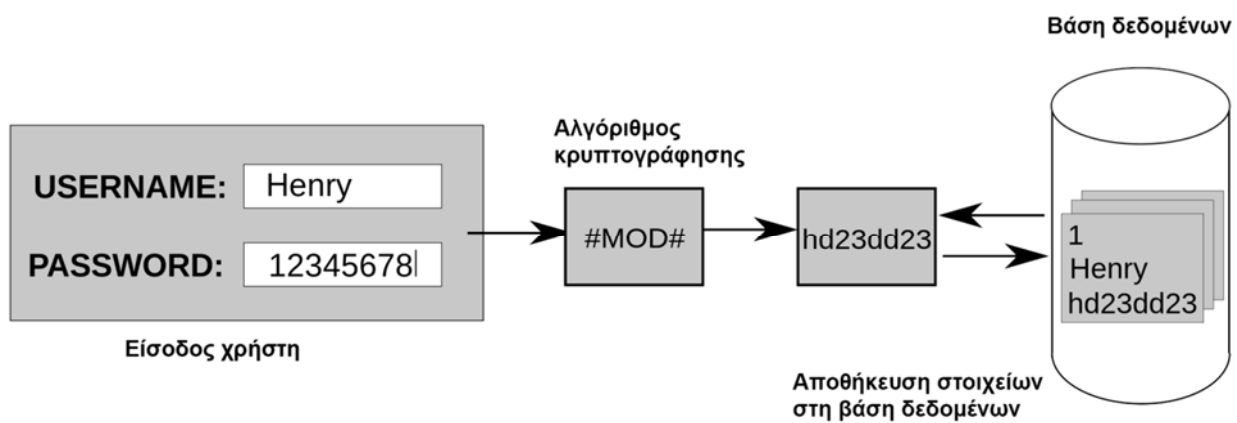


1.4.4 Μονόδρομες συναρτήσεις κατακερματισμού

Οι μονόδρομες συναρτήσεις κατακερματισμού (one-way hash functions) αποτελούν θεμελιώδη στοιχεία για την ανάπτυξη των περισσότερων πρωτοκόλλων κρυπτογράφησης. Οι συναρτήσεις κατακερματισμού είναι συναρτήσεις οι οποίες δέχονται σαν είσοδο μια ακολουθία χαρακτήρων μεταβλητού μήκους και παράγουν ένα μήνυμα σταθερού μεγέθους (γενικά μικρότερο) που ονομάζεται τιμή κατακερματισμού (hash value). Οι μονόδρομες συναρτήσεις κατακερματισμού είναι συναρτήσεις οι οποίες δουλεύουν μόνο προς την μία κατεύθυνση: είναι εύκολο να υπολογιστεί μια τιμή κατακερματισμού για κάποιο δεδομένο μήνυμα αλλά είναι αδύνατο να υπολογιστεί το μήνυμα στο οποίο αντιστοιχεί μια συγκεκριμένη τιμή σύνοψης. Μία καλά σχεδιασμένη μονόδρομη συνάρτηση κατακερματισμού είναι επίσης ελεύθερη από συγκρούσεις (collision-free) δηλαδή είναι δύσκολο να βρεθούν δύο μηνύματα που δίνουν την ίδια τιμή κατακερματισμού.

Οι μονόδρομες συναρτήσεις κατακερματισμού χρησιμοποιούνται κυρίως για εφαρμογές επαλήθευσης. Η τιμή σύνοψης αντιστοιχεί πλήρως, και αντιπροσωπεύει το αρχικό μήνυμα. Η αλλαγή έστω και ενός bit στο αρχικό μήνυμα αλλάζει κατά μέσο όρο τα μισά bits της τιμής σύνοψης.

Παραδείγματα μονόδρομων συναρτήσεων σύνοψης είναι οι MD4, MD5 και SHA.



1.5 Ψευδωνυμοποίηση

1.5.1 Ορισμός

Με βάση τον κανονισμό ως ψευδωνυμοποίηση:

«ορίζεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.»

1.5.2 Σκοπός

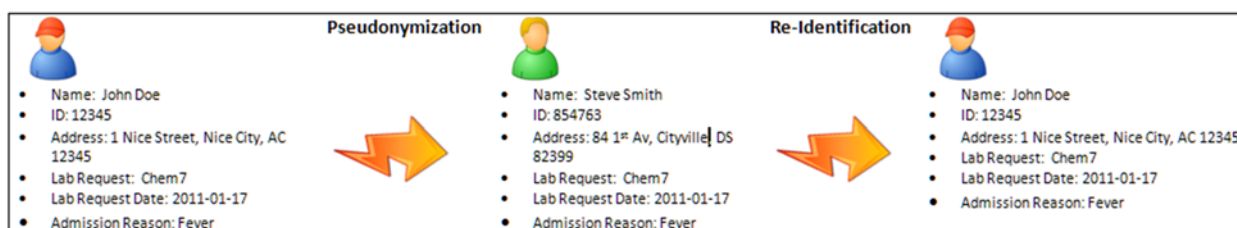
Ο σκοπός της ψευδωνυμοποίησης είναι η ευχέρεια της συλλογής δεδομένων για το υποκείμενο χωρίς η ταυτότητά του τελευταίου να γνωστοποιείται στον υπεύθυνο επεξεργασίας.

1.5.3 Υλοποίηση

Οι περαιτέρω πληροφορίες πρέπει να φυλάσσονται χωριστά και να υπόκεινται σε τεχνικά και οργανωτικά μέτρα ασφαλείας, ώστε να εξασφαλίζεται ότι το υποκείμενο των δεδομένων δεν μπορεί να αναγνωριστεί.

Οι κύριοι τρόποι ψευδωνυμοποίησης των δεδομένων είναι:

- η κρυπτογράφηση
- Αποχαρακτηρισμός δεδομένων
- ο διαχωρισμός των βάσεων δεδομένων



1.6 Ανωνυμοποίηση

1.6.1 Ορισμός και σκοπός

Ως ανωνυμοποίηση ορίζονται όλες οι ενέργειες που εκτελεί ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία πάνω σε σύνολο προσωπικών δεδομένων, με αποκλειστικό γνώμονα τη μη – αναστρέψιμη παραμόρφωση του μέρους εκείνου των δεδομένων που επιτρέπει τον προσδιορισμό ενός φυσικού προσώπου.

Η διαφορά της ανωνυμοποίησης από την ψευδωνυμοποίησης έγκειται στο ότι στην ανωνυμοποίηση δεν είναι δυνατός ο επαναπροσδιορισμός του υποκειμένου σε αντίθεση με την ψευδωνυμοποίηση.

Name	Token/Pseudonym	Anonymized
Clyde	qOerd	xxxxxx
Marco	Loqfh	xxxxxx
Les	Mcv	xxxxxx
Les	Mcv	xxxxxx
Marco	Loqfh	xxxxxx
Raul	BhQl	xxxxxx
Clyde	qOerd	xxxxxx