Ενότητα 7-Δ - Οργάνωση διαδικασιών για τη διασφάλιση της κυβερνοασφάλειας της επιχείρησης και του περιβάλλοντός της

Ενότητα 7- D2 Διαχείριση της εσωτερικής και εξωτερικής επικοινωνίας με τους συνεργάτες, τους προμηθευτές και τους πελάτες

Επικοινωνία

- Υπενθυμίσεις, πρόληψη , Κίνδυνος, σχέδιο δράσης
- Οι παράγοντες της κρίσης
- Επικοινωνία κρίσης

ΕΞΑΜΗΝΟ 10					
Ενότητα 7 - Εφαρμογή μιας αποτελεσματικής πολιτικής για την ασφάλεια στον κυβερνοχώρο		**BC 3**	**45**	*6*	**6**
Ενότητα 7-Α - Ορισμοί των εννοιών ασφάλειας και προστασίας			**15**	**2**	**2**
ΕΕ7-Α-1	Ασφάλεια και προστασία, δύο ξεχωριστοί τομείς αλλά ίσης σημασίας				
UE7-A-2	Κυβερνοασφάλεια: μια κοινή όραση μεταξύ χρηστών, σχεδιαστών εξοπλισμού, δίκτυα μετάδοσης, υπηρεσίες διαχείρισης δεδομένων				
UE7-C - Διαχείριση του κινδύνου που συνδέεται με τις κυβερνοεπιθέσεις			**15**	*2*	**2**
UE7-C-1	Προσδιορισμός λειτουργικών τομέων, χαρτογράφησή τους, εξασφάλιση ασφαλή διαλειτουργικότητα - Ανάγκες, διαπιστώσεις, ανάλυση				
UE7-C-2	Ασφάλιση για την κάλυψη των δαπανών που προκύπτουν από κυβερνοεπιθέσεις συστημάτων πληροφοριών				
UE7-D - Οργάνωση των διαδικασιών για τη διασφάλιση της κυβερνοασφάλειας της επιχείρησης και του περιβάλλοντός της			**15**	*2*	**2**
UE7-D-1	Οι φάσεις της δράσης: πρόβλεψη και παρακολούθηση, αντίδραση και καταπολέμηση, αποκατάσταση				
UE7-D-2	Διαχείριση της εσωτερικής και εξωτερικής επικοινωνίας με τους συνεργάτες, τους προμηθευτές, πελάτες				

Υπενθυμίσεις

- Κίνδυνος
- Πρόληψη
- Σχέδιο δράσης

Επικοινωνία

Κίνδυνος στον κυβερνοχώρο

(υπενθύμιση)

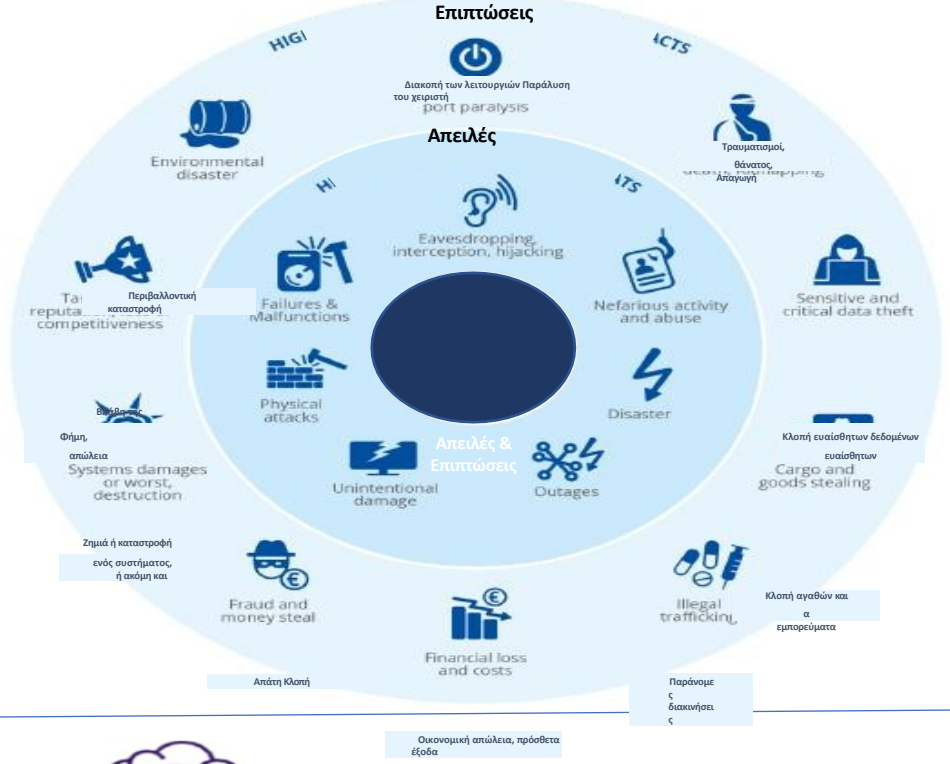
Εμπιστευτικότητα

Ακεραιότητα

Διαθεσιμότητα

Μη άρνηση

Επίπεδο	Κανονισμοί	Λιμάνια	Πλοία	Υπεράκτιες δραστηριότητες	Απειλές
OIV 	**ECI Dir** (2008) **LPM** (2007)	Μεγάλα ασφαλή λιμάνια	Σπάνια είναι OIV	Πετρέλαιο και φυσικό αέριο	Κυβερνοεπίθεση Τρομοκρατία Καταστροφή
OSE 	**Οδηγία NIS** (2020)	Ορισμένα λιμάνια που δεν είναι OIV	Σε ορισμένες χώρες	EMR και υποβρύχια καλώδια	Τρομοκρατία Εγκληματικές δραστηριότητες (συμπεριλαμβανομένου του κυβερνοχώρου)
Χρήστης 	**RGPD** (2018	Η ανάγκη για αύξηση του PPCM στον τομέα της κυβερνοασφάλειας είναι αναπόφευκτη σε έναν τομέα που είναι σε μεγάλο βαθμό ψηφιοποιημένος και συνδεδεμένος.			Εγκληματικές δραστηριότητες Επιρροή



Τι Πού Πώς

Ποιος

Κακόβουλο λογισμικό Script kiddy

Κακόβουλος υπάλληλος

Τρομοκρατική ομάδα

Εγκληματική οργάνωση

Κράτος

Ασφάλεια / Προστασία
Πρόληψη / Κίνδυνος

Παράδειγμα σχεδίου δράσης

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ – ΣΧΕΔΙΟ ΔΡΑΣΗΣ

I	Ευαισθητοποίηση και εκπαίδευση	ΠΡΟΤΥΠΟ	ΕΝΙΣΧΥΜΕΝΟ
1	Εκπαίδευση των επιχειρησιακών ομάδων στην ασφάλεια των συστημάτων πληροφοριών		
2	Ευαισθητοποίηση των χρηστών σχετικά με τις βασικές ορθές πρακτικές ασφάλειας πληροφορικής		
3	Διαχείριση των κινδύνων της διαχείρισης πληροφορικής		
II	Γνωρίστε το σύστημα πληροφοριών		
4	Προσδιορισμός των πιο ευαίσθητων πληροφοριών και διακομιστών και διατήρηση ενός διαγράμματος του δικτύου		
5	Διαθέτει έναν πλήρη κατάλογο των προνομιακών λογαριασμών και τον διατηρεί ενημερωμένο		
6	Οργάνωση των διαδικασιών άφιξης, αναχώρησης και αλλαγής θέσης των χρηστών		
7	Να επιτρέπεται η σύνδεση στο δίκτυο της οντότητας μόνο σε ελεγχόμενο εξοπλισμό		
III	Αυθεντικοποίηση και έλεγχος πρόσβασης		
8	Ταυτοποίηση κάθε ατόμου που έχει πρόσβαση στο σύστημα και διάκριση μεταξύ ρόλων χρήστη/διαχειριστή.		
9	Ανάθεση των κατάλληλων δικαιωμάτων πρόσβασης σε ευαίσθητους πόρους του συστήματος πληροφοριών		
10	Ορίστε και ελέγξτε τους κανόνες επιλογής και μεγέθους των κωδικών πρόσβασης		
11	Προστασία των κωδικών πρόσβασης που είναι αποθηκευμένοι στα συστήματα		
12	Αλλαγή των προεπιλεγμένων στοιχείων ελέγχου ταυτότητας σε εξοπλισμό και υπηρεσίες		
13	Προτιμήστε, όποτε είναι δυνατόν, ισχυρή πιστοποίηση		

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ – ΣΧΕΔΙΟ ΔΡΑΣΗΣ

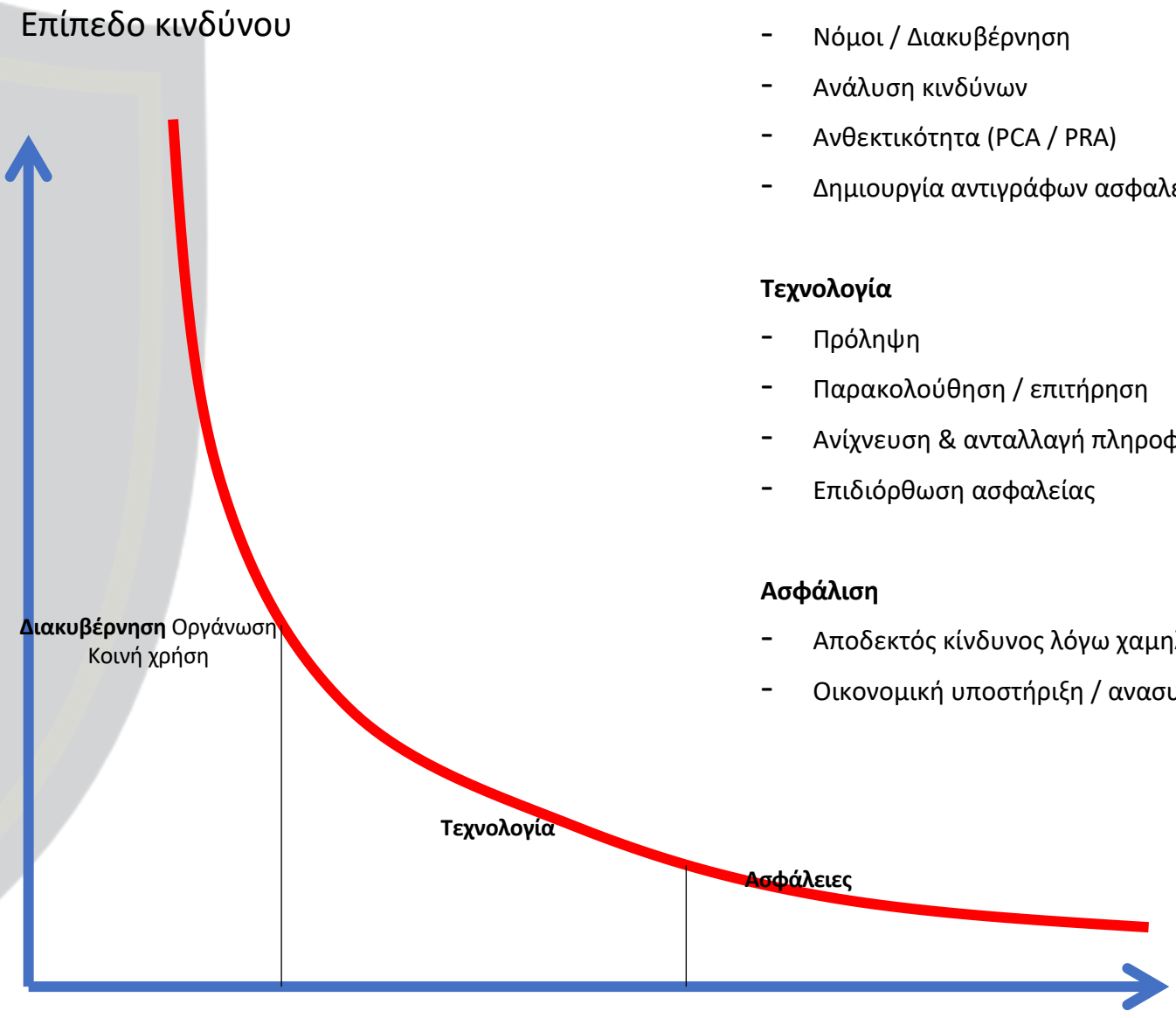
IV	Ασφάλεια των θέσεων εργασίας		
14	Εφαρμογή ενός ελάχιστου επιπέδου ασφάλειας σε όλο το δίκτυο υπολογιστών		
15	Προστασία από απειλές που σχετίζονται με τη χρήση αφαιρούμενων μέσων αποθήκευσης		
16	Χρησιμοποιήστε ένα κεντρικό εργαλείο διαχείρισης για να ομογενοποιήσετε τις πολιτικές ασφαλείας		
17	Ενεργοποιήστε και διαμορφώστε το τοπικό τείχος προστασίας των σταθμών εργασίας		
18	Κρυπτογράφησε τα ευαίσθητα δεδομένα που μεταδίδονται μέσω του Διαδικτύου		
V	Ασφάλεια του δικτύου		
19	Τμηματοποίηση του δικτύου και δημιουργία διαχωριστικών μεταξύ των ζωνών		
20	Διασφάλιση της ασφάλειας των δικτύων Wi-Fi και του διαχωρισμού των χρήσεων		
21	Χρησιμοποιήστε ασφαλή πρωτόκολλα, εφόσον υπάρχουν.		
22	Εγκατάσταση ασφαλούς πύλης πρόσβασης στο Διαδίκτυο		
23	Διαχωρισμός των υπηρεσιών που είναι ορατές από το Διαδίκτυο από το υπόλοιπο σύστημα πληροφοριών		
24	Προστασία του επαγγελματικού ηλεκτρονικού ταχυδρομείου		
25	Ασφάλιση των αποκλειστικών διασυνδέσεων δικτύου με τους συνεργάτες		
26	Έλεγχος και προστασία της πρόσβασης στους χώρους των διακομιστών και στα τεχνικά δωμάτια		

ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ – ΣΧΕΔΙΟ ΔΡΑΣΗΣ

VI	Ασφάλεια της διοίκησης		
27	Απαγόρευση πρόσβασης στο Διαδίκτυο από τους σταθμούς εργασίας/διακομιστές διαχείρισης του συστήματος πληροφοριών		
28	Χρήση ενός αποκλειστικού και διαχωρισμένου δικτύου για τη διαχείριση του συστήματος πληροφοριών		
29	Περιορίστε τα δικαιώματα διαχείρισης των σταθμών εργασίας στις απολύτως απαραίτητες λειτουργικές ανάγκες		
VII	Διαχείριση της κινητικότητας		
30	Λήψη μέτρων για τη φυσική ασφάλεια των κινητών τερματικών		
31	Κρυπτογράφηση ευαίσθητων δεδομένων, ιδίως σε εξοπλισμό που ενδέχεται να χαθεί		
32	Ασφάλιση της σύνδεσης δικτύου των τερματικών που χρησιμοποιούνται σε κινητές εφαρμογές.		
33	Υιοθέτηση πολιτικών ασφαλείας ειδικά για κινητές συσκευές		
VIII	Διατήρηση του συστήματος πληροφοριών σε καλή κατάσταση		
34	Καθορισμός πολιτικής ενημέρωσης των στοιχείων του συστήματος πληροφοριών		
35	Προβλέψτε τη λήξη της συντήρησης του λογισμικού και των συστημάτων και περιορίστε τις προσκολλήσεις λογισμικού		
IX	Εποπτεία, έλεγχος, αντίδραση		
36	Ενεργοποίηση και διαμόρφωση των αρχείων καταγραφής των πιο σημαντικών στοιχείων		
37	Ορισμός και εφαρμογή πολιτικής δημιουργίας αντιγράφων ασφαλείας για κρίσιμα στοιχεία		
38	Διενέργεια τακτικών ελέγχων και επιθεωρήσεων ασφαλείας και εφαρμογή των σχετικών διορθωτικών μέτρων		
39	Ορίστε έναν υπεύθυνο για την ασφάλεια των συστημάτων πληροφοριών και ενημερώστε το προσωπικό σχετικά.		
40	Καθορισμός διαδικασίας διαχείρισης περιστατικών ασφάλειας		
X	Για να προχωρήσετε περαιτέρω		
41	Διενέργεια επίσημης ανάλυσης κινδύνων		
42	Προτίμηση στη χρήση προϊόντων και υπηρεσιών που έχουν πιστοποιηθεί από την ANSSI		

Μείωση του κινδύνου / δράση

Μείωση του κινδύνου στον κυβερνοχώρο



Διακυβέρνηση / οργάνωση

- Νόμοι / Διακυβέρνηση
- Ανάλυση κινδύνων
- Ανθεκτικότητα (PCA / PRA)
- Δημιουργία αντιγράφων ασφαλείας

Τεχνολογία

- Πρόληψη
- Παρακολούθηση / επιτήρηση
- Ανίχνευση & ανταλλαγή πληροφοριών για περιστατικά
- Επιδιόρθωση ασφαλείας

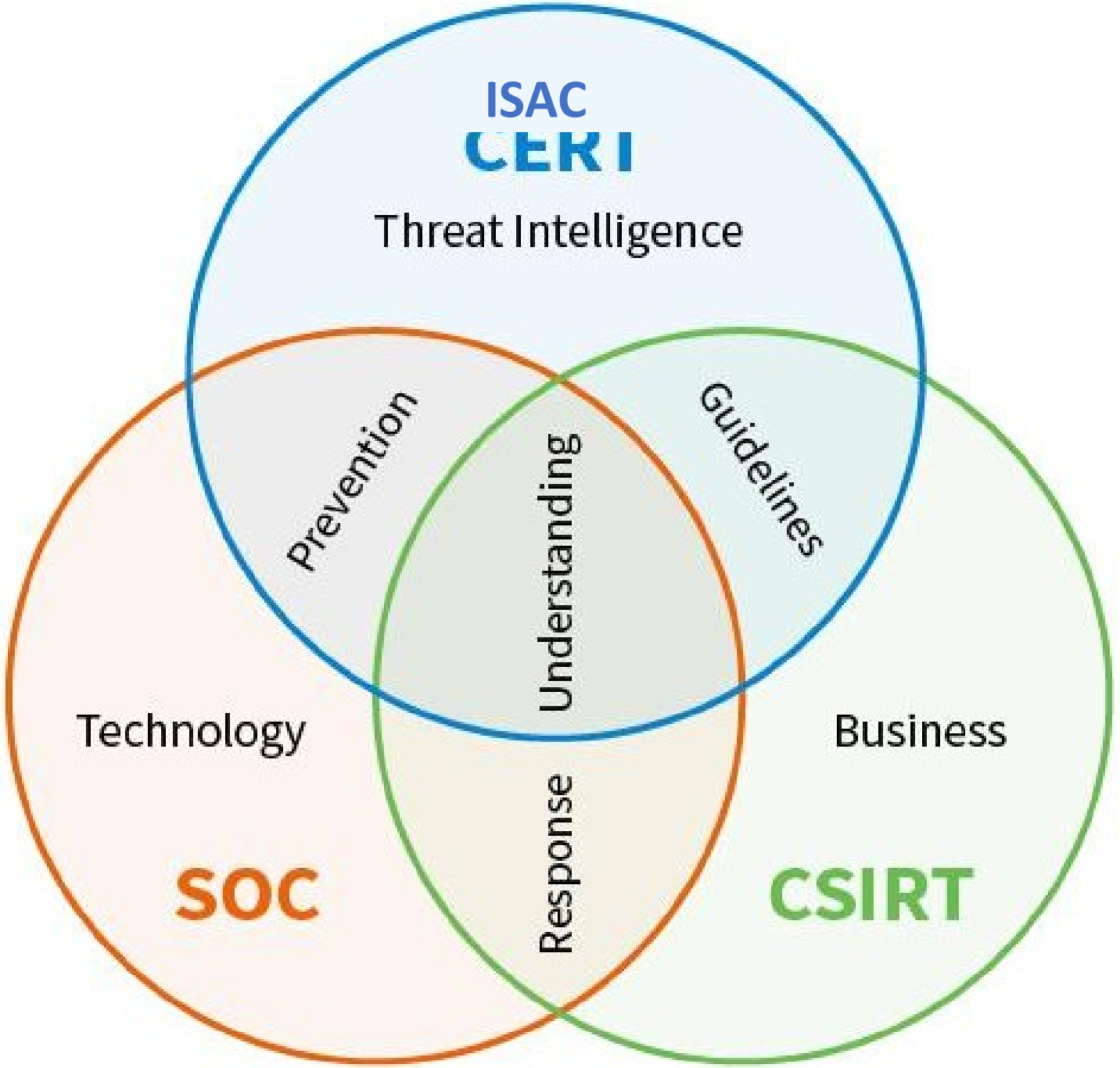
Ασφάλιση

- Αποδεκτός κίνδυνος λόγω χαμηλής συχνότητας εμφάνισης
- Οικονομική υποστήριξη / ανασυγκρότηση

Ερώτηση

-

Πώς να οργανωθείτε για την αντιμετώπιση απειλών στον κυβερνοχώρο ;



Οι 10 βασικοί κανόνες για τον περιορισμό των κινδύνων από κυβερνοεπιθέσεις (1/2)

Διεξαγωγή ανάλυσης κινδύνων

- Προσδιορίστε τα βασικά επιχειρηματικά περιουσιακά στοιχεία, την κρισιμότητά τους και τις επιπτώσεις σε περίπτωση συμβάντος.
- χαρτογράφηση των ενδιαφερόμενων μερών του οργανισμού
- να προσδιορίσετε τις ισχύουσες νομικές και κανονιστικές απαιτήσεις
- να καθορίσετε τα σενάρια απειλών και τους επιχειρησιακούς κινδύνους.

Σύνταξη μιας εξαντλητικής περιγραφής των αναγκών από λειτουργική και ασφαλιστική άποψη

Απαιτήσεις σχετικά με το σχεδιασμό, την ανάπτυξη, το MCO / MCS, καθώς και την αναστρεψιμότητα.

Απαιτήσεις προστασίας από νόμους με εξωεδαφική εμβέλεια (RGPD, SecNumCloud, νόμος περί αποκλεισμού κ.λπ.).

Λάβετε υπόψη τον οδηγό σχετικά με τις «γενικές ρήτρες ασφάλειας στις συμβάσεις» της ANSSI και της Διεύθυνσης Προμηθειών του Κράτους (DAE).

Στηριχθείτε σε έναν αξιόπιστο πάροχο φιλοξενίας για τις πιο ευαίσθητες επεξεργασίες και δεδομένα

Για τις τεχνολογίες Cloud, η πιστοποίηση SecNumCloud εγγυάται ένα επίπεδο εμπιστοσύνης και προστασία από εξωεδαφικές νομοθεσίες.

Στο πλαίσιο της υποδομής φιλοξενίας, πρέπει να δοθεί ιδιαίτερη προσοχή στις αρχές διαχωρισμού, ιδίως:

- μεταξύ των πόρων των διαφόρων πελατών της υποδομής
- μεταξύ των διαφόρων περιβαλλόντων ανάπτυξης, προπαραγωγής και παραγωγής αντίστοιχα
- μεταξύ των πόρων της επιχείρησης και εκείνων που προορίζονται για τη διαχείριση και τη διοίκηση.

Διασφάλιση ορθών πρακτικών ανάπτυξης/σχεδιασμού (συμπεριλαμβανομένων τακτικών ελέγχων)

Ασφάλεια υποδομών, εφαρμογών και τερματικών διαχειριστών και χρηστών, εσωτερικών ή εξωτερικών.

Έλεγχος και προστασία των διασυνδέσεων

Οι διασυνδέσεις μεταξύ συστημάτων με τρίτα συστήματα πληροφορικής και/ή παρόχους είναι σημαντικά σημεία προσοχής. Αυτές καθορίζουν την έκταση έκθεσης σε απειλές και επιθέσεις. Είναι σκόπιμο:

- να χαρτογραφηθούν
- να αξιολογείται και να διατηρείται το επίπεδο ασφάλειας
- να διασφαλιστεί η ανίχνευση περιστατικών ασφάλειας.

Ιδιαίτερα, πρέπει να ληφθούν υπόψη και οι εσωτερικές διασυνδέσεις της οντότητας, ιδίως για την πρόσβαση σε κινητές συσκευές.

Οι 10 βασικοί κανόνες για τον περιορισμό των κινδύνων από κυβερνοεπιθέσεις (2/2)

Ασφάλεια στη διαχείριση ταυτοτήτων, στους μηχανισμούς αυθεντικοποίησης και στους ελέγχους πρόσβασης

Διαχείριση ταυτοτήτων και μηχανισμοί αυθεντικοποίησης.

Η ANSSI παρέχει οδηγούς με συστάσεις για την ενίσχυση της ασφάλειας ενός πληροφοριακού συστήματος:

- *Συστάσεις σχετικά με την πολυπαραγοντική αυθεντικοποίηση και τους κωδικούς πρόσβασης.*
- *Οδηγός για την υγιεινή των υπολογιστών: ενίσχυση της ασφάλειας του πληροφοριακού σας συστήματος με 42 μέτρα*.
- *Συστάσεις ασφάλειας σχετικά με ένα σύστημα GNU/Linux*.

Προστασία των πόρων διαχείρισης των πληροφοριακών συστημάτων

Αυτοί οι πόροι αποτελούν ιδιαίτερο στόχο των επιτιθέμενων, καθώς τους επιτρέπουν να αναλάβουν γρήγορα τον έλεγχο ολόκληρου του πληροφοριακού συστήματος.

Ο οδηγός *«Συστάσεις για την ασφαλή διαχείριση των συστημάτων πληροφοριών»* της ANSSI παρέχει καθοδήγηση στους φορείς.

Διασφάλιση της ασφάλειας των πληροφοριακών συστημάτων

Διορθωτικά μέτρα ασφαλείας για τις τεχνικές βάσεις που χρησιμοποιούνται.

Ο ιστότοπος του CERT-FR δημοσιεύει σε πραγματικό χρόνο τις προειδοποιήσεις ασφαλείας.

Διασφάλιση και προστασία των αντιγράφων ασφαλείας των δεδομένων και της υποδομής

Η αποθήκευση εκτός σύνδεσης και εκτός του χώρου εργασίας, καθώς και οι διαδικασίες αποκατάστασης, είναι καθοριστικής σημασίας για την αντιμετώπιση μιας κρίσιμης κατάστασης, είτε αυτή προέρχεται από κυβερνοεπίθεση είτε όχι.

Εφαρμογή ενός συστήματος ανίχνευσης περιστατικών ασφαλείας (συμπεριλαμβανομένης της καταγραφής) και διαχείρισης κρίσεων

Επιτρέπει την ταχεία αναγνώριση μιας απειλής και τη λήψη των απαραίτητων προληπτικών και διορθωτικών μέτρων πριν φτάσουμε σε μια κατάσταση παραβίασης.
Αυτά τα συστήματα βασίζονται αναγκαστικά σε μια υποδομή συλλογής και συγκέντρωσης αρχείων καταγραφής συμβάντων ασφαλείας, τα οποία τροφοδοτούν τις υπηρεσίες ανίχνευσης (βλ. τους οδηγούς *«Συστάσεις ασφαλείας για την αρχιτεκτονική ενός συστήματος καταγραφής»* και *«Συστάσεις ασφαλείας για την καταγραφή συστημάτων Microsoft Windows σε περιβάλλον Active Directory*»).

Καθορισμός διαδικασιών και διαδικασιών διαχείρισης κρίσεων στον κυβερνοχώρο

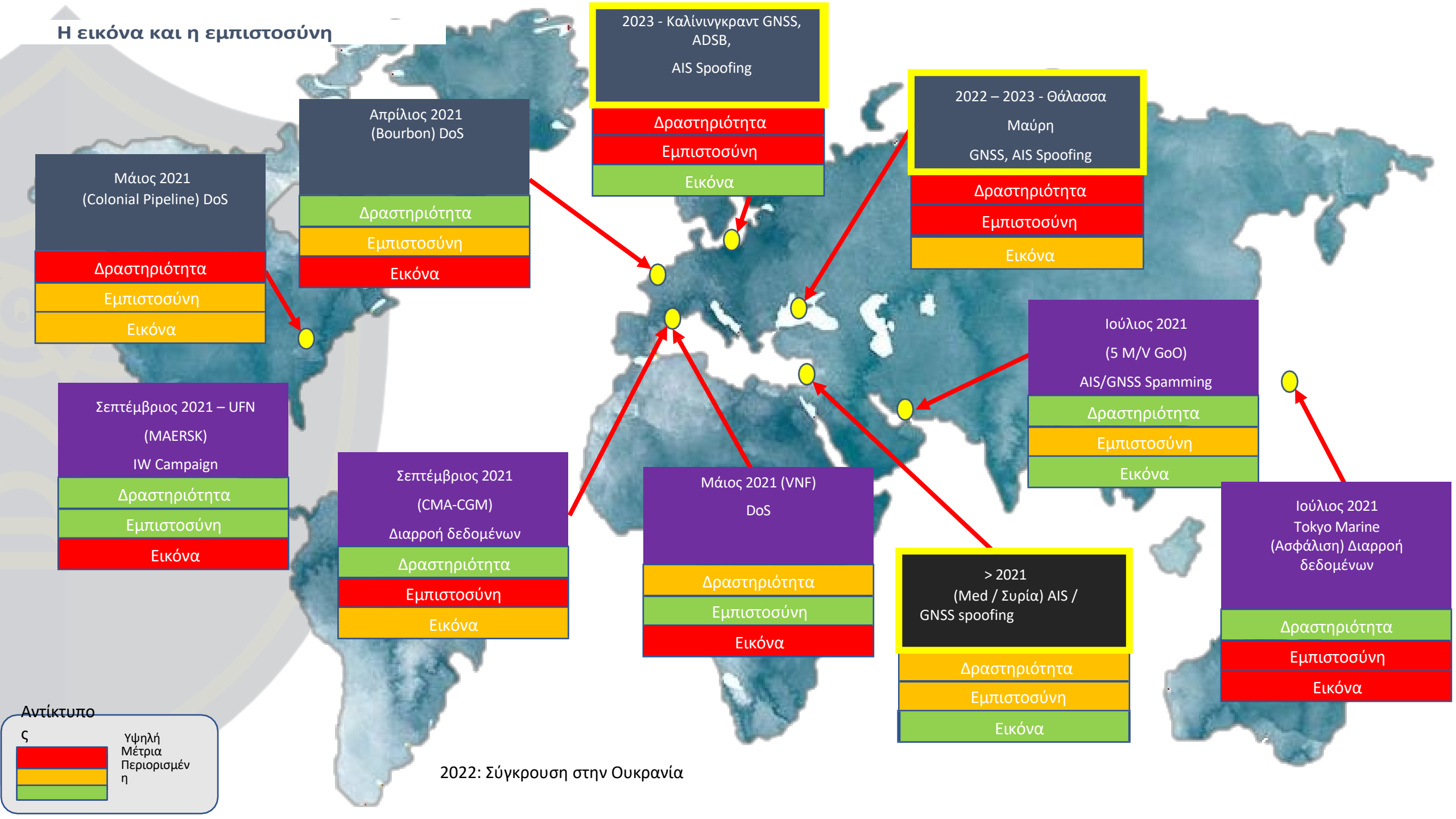
Όσον αφορά την αντιμετώπιση περιστατικών, βασιστείτε σε παρόχους που είναι εξειδικευμένοι στην αντιμετώπιση περιστατικών ασφάλειας (PRIS).

Επικοινωνία σε καταστάσεις κρίσης

Επικοινωνία και κρίση

- Πρέπει να επικοινωνήσουμε;
- Σε ποιον
- Πώς
- Πότε
- Η διαφάνεια
- Τα όρια

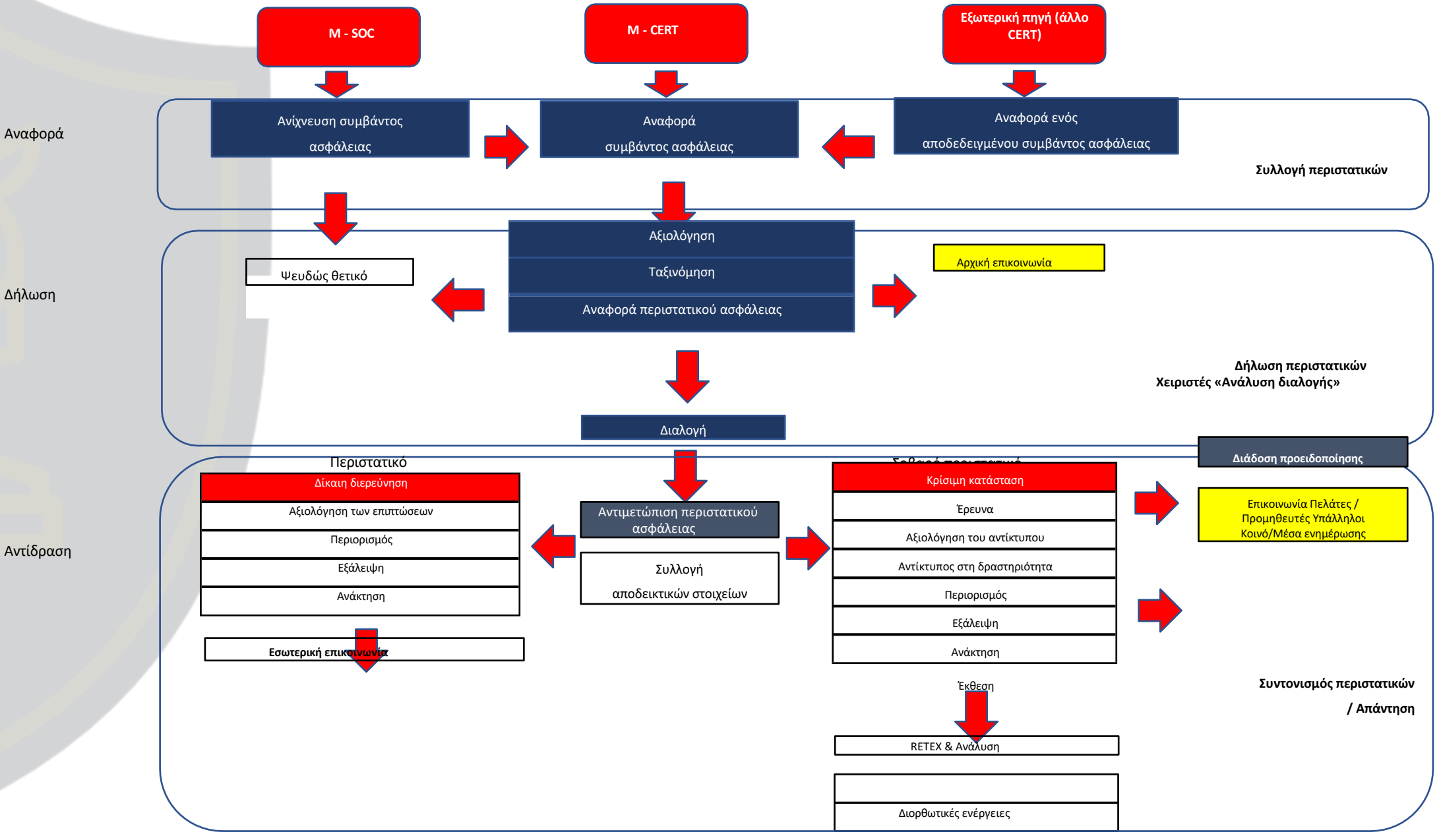
Η εικόνα και η εμπιστοσύνη



POSITIONNER UNE CRISE CYBER FACE AUX ÉVÈNEMENTS PORTANT ATTEINTE AUX ACTIVITÉS MÉTIERS D'UNE ORGANISATION

Υπενθύμιση – Διαχείριση κρίσεων

Οργανόγραμμα διαχείρισης περιστατικών



Τα στάδια της επικοινωνίας σε περίπτωση κρίσης

ΣΤΑΔΙΟ 1: έναρξη διαλόγου με τις ομάδες κυβερνοασφάλειας και πληροφορικής εκτός περιόδου κρίσης

ΒΗΜΑ 2: Προβλέψτε τα σενάρια κρίσης και τις απαντήσεις που πρέπει να δοθούν στον τομέα της επικοινωνίας ΒΗΜΑ 3: Σχεδιάστε τη στρατηγική επικοινωνίας για την αντιμετώπιση της κρίσης

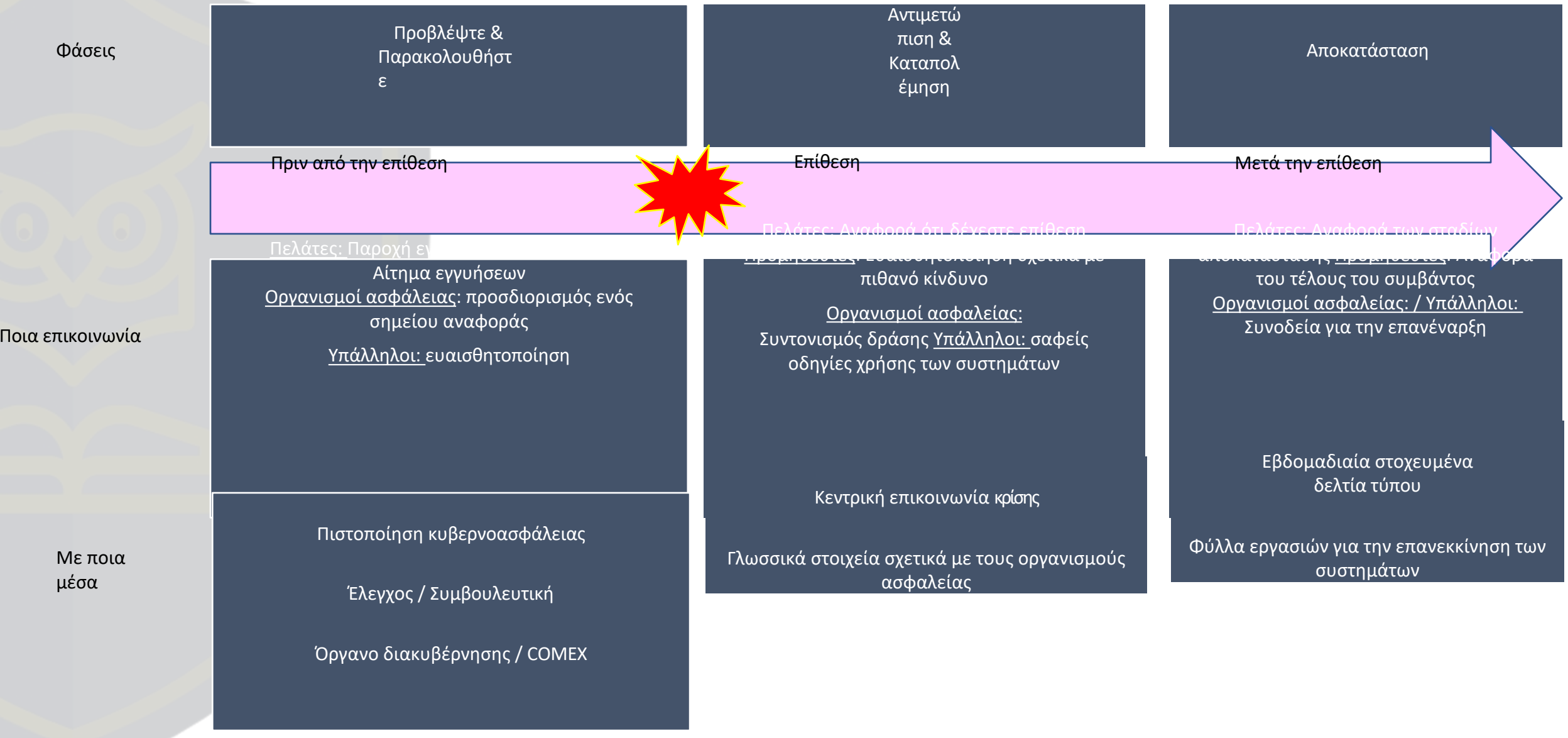
ΒΗΜΑ 4: ενσωμάτωση της επικοινωνίας στην οργάνωση της διαχείρισης κρίσεων στον κυβερνοχώρο

ΒΗΜΑ 5: Οργάνωση της επικοινωνίας κρίσης

ΒΗΜΑ 6: Δημιουργία ενός εργαλείου αφιερωμένου στη διαχείριση κρίσεων στον κυβερνοχώρο

ΒΗΜΑ 7: Εκπαίδευση των ομάδων στη διαχείριση της επικοινωνίας

Επικοινωνία πριν, κατά τη διάρκεια και μετά



Πρακτική περίπτωση

Σενάριο: Παραβίαση των πληροφοριακών συστημάτων σας μέσω τρίτου

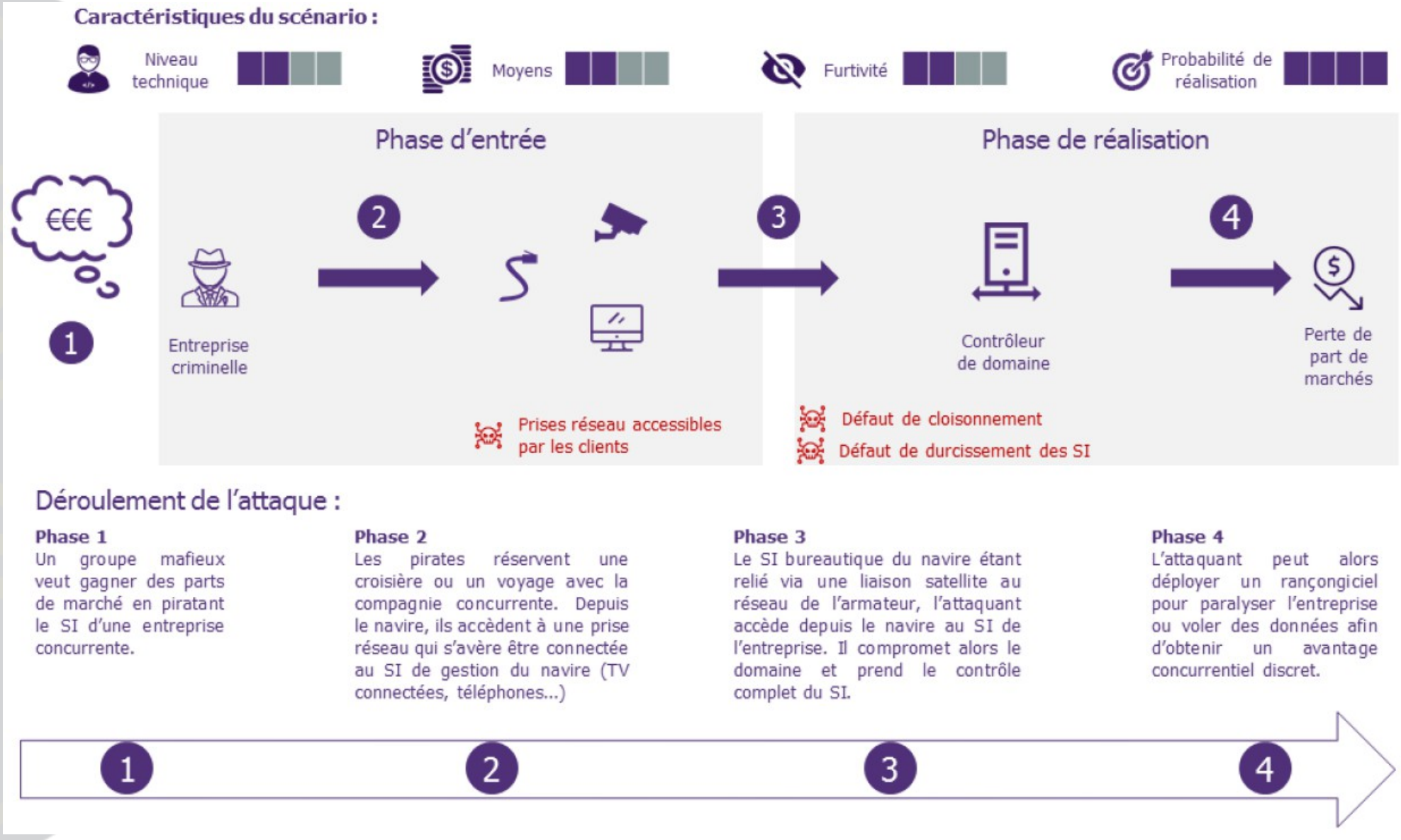
Ένας εισβολέας που επιθυμεί να αυξήσει το μερίδιο αγοράς του προκαλώντας ζημιά σε μια ανταγωνιστική εταιρεία, αποκτά πρόσβαση, μόλις εισέλθει σε έναν από τους ιστότοπους του θύματός του, σε μια πρίζα δικτύου που βρίσκεται σε μια δημόσια, μη κλειδωμένη περιοχή. Εξαπλώνεται εντός του πληροφοριακού συστήματος και, μέσω του διαδικτύου, στο δίκτυό σας για να φτάσει στα πληροφοριακά σας συστήματα.

Η διαμόρφωση του ελεγκτή τομέα παρουσιάζει ορισμένες αδυναμίες, ο εισβολέας εκμεταλλεύεται μία από αυτές και αποκτά

δικαιώματα διαχειριστή. Έτσι, αποκτά τον πλήρη έλεγχο του πληροφοριακού σας συστήματος.

Η αδύναμη ή ανύπαρκτη διαχωριστική θωράκιση, καθώς και η απουσία παρακολούθησης των δικτύων, καθιστούν τα συστήματα πληροφορικής τρίτων πιθανά σημεία εισόδου.

Φάσεις της επίθεσης



Αντιδράσεις / Μέτρα που πρέπει να ληφθούν

Επικοινωνία μετά την ανακάλυψη του συμβάντος

- ***Πελάτες***
- ***Προμηθευτές***
- ***Συνεργάτες / υπάλληλοι***
- ***Οργανισμοί ασφαλείας (σε περίπτωση κρίσης)***
- ***Μεγάλο κοινό (για μεγάλους ομίλους / φορείς εκμετάλλευσης)***

Συνιστώμενα μέτρα ασφαλείας

→ Εγκατάσταση λύσης ελέγχου πρόσβασης στο δίκτυο

Οι πρίζες δικτύου που βρίσκονται σε χώρους προσβάσιμους στο κοινό πρέπει, στο μέτρο του δυνατού, να απενεργοποιούνται. Όταν αυτές οι πρίζες

χρησιμοποιούνται για την παροχή μιας υπηρεσίας, πρέπει να εφαρμοστεί έλεγχος πρόσβασης στο δίκτυο.

Οι ντουλάπες και οι τεχνικοί χώροι πρέπει να είναι κλειδωμένοι.

→ Διαχωρισμός μεταξύ των διαφόρων δικτύων
Όταν το δίκτυο είναι «επίπεδο», χωρίς κανένα μηχανισμό διαχωρισμού, κάθε μηχανή του δικτύου μπορεί να έχει πρόσβαση σε οποιαδήποτε άλλη μηχανή. Η παραβίαση της ασφάλειας μιας από αυτές θέτει σε κίνδυνο ολόκληρο το σύστημα πληροφοριών, συμπεριλαμβανομένων των κρίσιμων διακομιστών.

Πρέπει επομένως να εφαρμοστεί κατάλληλη διαχωριστική μεμβράνη μεταξύ των διαφόρων δικτύων του πλοίου και, γενικότερα, της εταιρείας.

→ Ενίσχυση και διατήρηση της ασφάλειας των συστημάτων
Οι επιτιθέμενοι εκμεταλλεύονται ευρέως γνωστές ευπάθειες για να εισχωρήσουν και να αυξήσουν τα προνόμιά τους στα συστήματα πληροφορικής. Η ενίσχυση και η συνεχής ενημέρωση των συστημάτων επιτρέπουν την πρόληψη ή τον περιορισμό της προόδου ενός επιτιθέμενου.

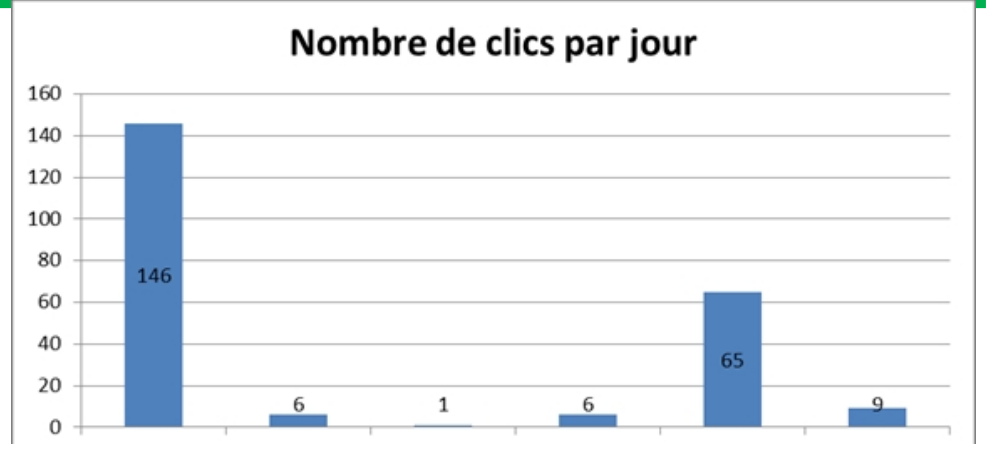
ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ - **PHISHING**

ΟΝΟΜΑ	**PHISHING – HAMECONNAGE**		
ΟΡΙΣΜΟΣ	Τεχνική που χρησιμοποιείται από απατεώνες απατεώνες για να προσωπικές προσωπικές πληροφορίες. Να κάνουν το θύμα να πιστέψει ότι επικοινωνεί με έναν αξιόπιστο τρίτο.	**ΣΤΟΧΟΣ**	Υποκλέψ την ταυτότητας.
		ΠΩΣ	Ηλεκτρονικό ταχυδρομείο.

ΠΩΣ ΑΝΤΙΔΡΑΣΗ	Για κάθε μήνυμα που λαμβάνετε,	➢ Μην ανοίγετε τα συνημμένα αρχεία ➢ Ποτέ μην κάνετε κλικ σε υπερσυνδέσμους ➢ Ελέγξτε τη διεύθυνση του αποστολέα ➢ Ελέγξτε την ώρα και την ημερομηνία αποστολής ➢ Ελέγξτε το θέμα του μηνύματος. ➢ Ελέγξτε ότι το μήνυμα δεν ζητά ασυνήθιστες/προσωπικές πληροφορίες ➢ Δώστε προσοχή στα μηνύματα προειδοποίησης που εμφανίζονται στο ηλεκτρονικό σας ταχυδρομείο

ΣΕ ΠΕΡΙΠΤΩΣΗ ΑΜΦΙΒΟΛΙΑΣ	➢ Μην ανοίγετε τα συνημμένα αρχεία	➢ Μην κάνετε κλικ σε κανέναν από τους προτεινόμενους συνδέσμους	➢ Μην απαντήσετε στο μήνυμα
	Ειδοποιήστε τον RSSI		

ΣΥΓΚΕΚΡΙΜΕΝΗ ΠΕΡΙΠΤΩΣΗ	**ΠΡΑΚΤΙΚΗ PHISHING ΣΕ ΜΕΓΑΛΟ ΟΜΙΛΟ**



Μια εκστρατεία phishing είχε ως στόχο 1000 υπαλλήλους του ομίλου.

Σε **6 ημέρες**, ο «κακόβουλος» διακομιστής συγκέντρωσε **233 κλικ**.

ΣΗΜΕΙΩΣΗ: 14 και 15 (Σαββατοκύριακο), 16 αργία.

Τελικά, **178 άτομα (18%) έκαναν κλικ** σε έναν από τους συνδέσμους του ηλεκτρονικού μηνύματος-παγίδα.

Σε περίπτωση πραγματικής επίθεσης, ένα μόνο κλικ θα μπορούσε να θέσει σε κίνδυνο ολόκληρη την εταιρεία.

13 14 15 16 17 18

Ευαισθητοποίηση SSI - Λογισμικό εκβιασμού «LOCKY»

ΟΝΟΜΑ	**LOCKY**	**ΤΥΠΟΣ**	RANSOMWARE	**ΗΜΕΡΟΜΗΝΙΑ ΕΜΦΑΝΙΣΗΣ**	ΦΕΒ 2016
		ΣΥΣΤΗΜΑ ΠΟΥ ΕΠΗΡΕΑΖΕΤΑΙ	ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ WINDOWS	**ΤΟΠΟΘΕΣΙΑ**	ΕΥΡΩΠΗ

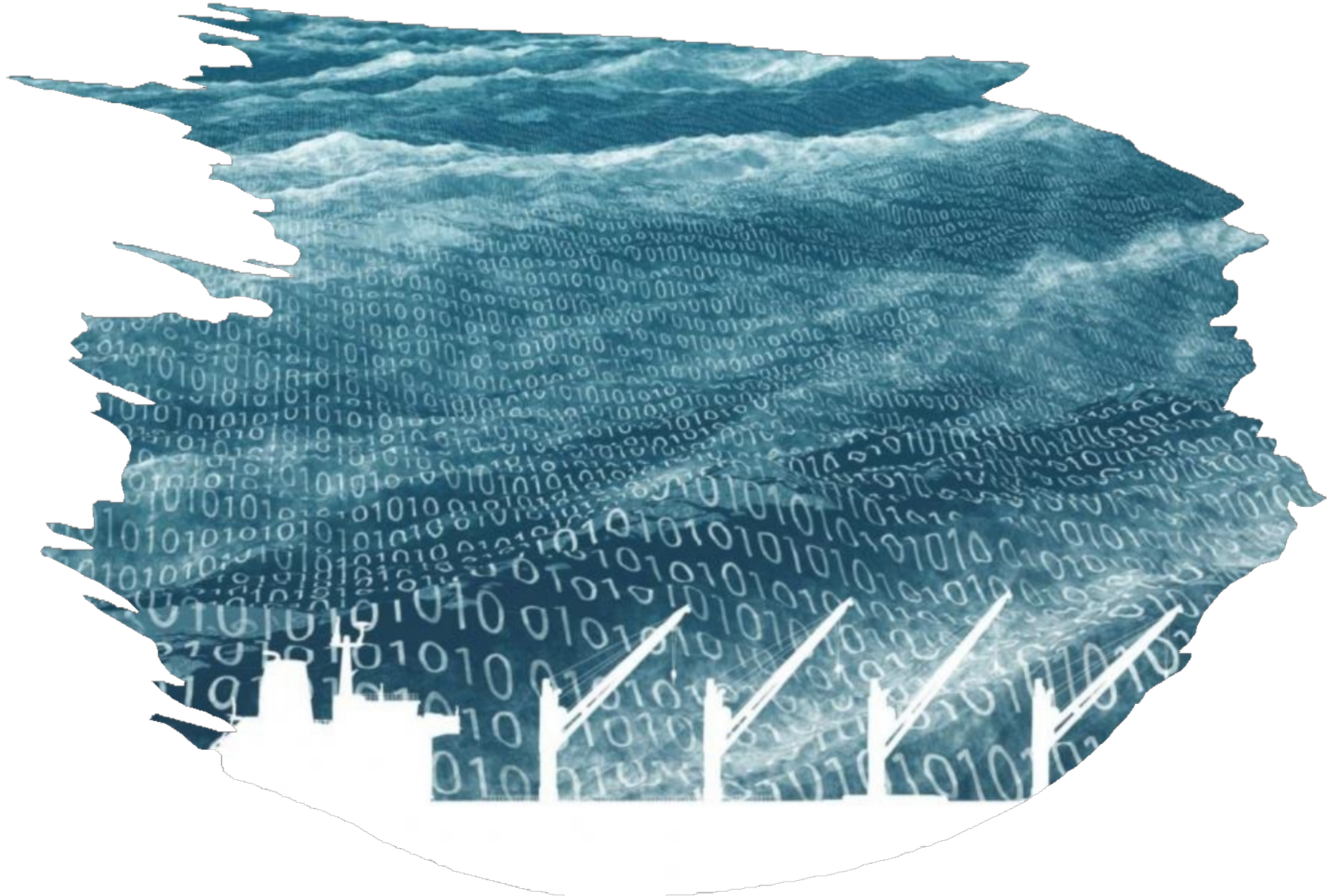
ΕΠΙΠΤΩΣΗ	ΟΜΗΡΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΣΑΣ ΔΕΔΟΜΕΝΩΝ ΜΕΣΩ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ	
ΣΤΟΧΟΣ	ΑΙΤΗΣΗ ΛΥΤΡΩΝ ΓΙΑ ΤΗΝ ΑΝΑΚΤΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ	
ΔΙΑΔΟΣΗ	ΔΙΑΔΙΔΕΤΑΙ ΜΕΣΩ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΑΠΟ **BOTNET** (Βλ. ορισμό)	
	ΜΕΣΩ ΜΗΧΑΝΗΜΑΤΟΣ	
ΜΕΘΟΔΟΣ ΕΠΙΘΕΣΗΣ	ΛΗΨΗ E-MAIL ΜΕ ΜΟΛΥΝΜΕΝΟ ΣΥΝΗΜΜΕΝΟ:	ΘΕΜΑ (προς το παρόν): ΠΡΟΣ: Τιμολόγιο J-XXXXXXX
		ΚΥΡΙΑ ΚΕΙΜΕΝΟ: ΣΩΣΤΗ ΣΥΝΤΑΞΗ, ΣΥΝΗΜΜΕΝΟ ΣΕ ΜΟΡΦΗ .DOC (ΣΥΝΗΘΩΣ, ΑΛΛΑ ΟΧΙ ΠΑΝΤΑ…)
		ΑΠΟΣΤΟΛΕΑΣ: ΠΟΤΕ Ο ΙΔΙΟΣ
	ΚΑΤΑ ΤΗΝ ΑΝΟΙΓΜΑ ΤΗΣ ΣΥΝΗΜΜΕΝΗΣ ΤΑ ΕΓΓΡΑΦΑ ΤΗΣ ΘΕΣΗΣ ΚΡΥΠΤΟΓΡΑΦΟΥΝΤΑΙ (ΜΟΡΦΗ .LOCKY)	
	ΤΟ ΣΗΜΕΙΩΜΑΤΑΡΙΟ ΑΝΟΙΓΕΙ ΓΙΑ ΝΑ ΕΜΦΑΝΙΣΕΙ ΜΙΑ ΑΙΤΗΣΗ ΛΥΤΡΩΝ	
	ΟΙ ΣΥΝΔΕΣΜΟΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΘΑ ΔΕΙΧΝΟΥΝ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ΓΙΑ ΤΗΝ ΑΝΑΚΤΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕ ΤΗ ΒΟΗΘΕΙΑ ΕΝΟΣ ΑΠΟΚΡΥΠΤΟΓΡΑΦΟΥ (ΟΝΟΜΑΖΟΜΕΝΟΥ LOCKY DECRYPTOR PRO, Η ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ ΟΠΟΙΟΥ ΔΕΝ ΕΧΕΙ ΑΠΟΔΕΙΧΘΕΙ)	
ΛΥΣΗ	**ΚΑΜΙΑ ΜΈΧΡΙ ΣΗΜΕΡΑ – ΠΛΉΡΗΣ ΑΠΩΛΕΙΑ ΤΩΝ ΔΕΔΟΜΈΝΩΝ**	
ΣΥΣΤΑΣΕΙΣ	ΜΗΝ ΠΛΗΡΩΝΕΤΕ ΤΟ ΛΥΤΡΑ ΣΤΟΥΣ ΑΠΑΓΩΓΟΥΣ ΕΠΕΙΔΗ:	Η ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΔΕΝ ΕΧΕΙ ΑΠΟΔΕΙΧΘΕΙ
		ΧΑΜΗΛΟΣ ΚΟΣΤΟΣ
		ΕΝΘΑΡΡΥΝΕΙ ΤΟΥΣ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΙΕΣ ΝΑ ΣΥΝΕΧΙΣΟΥΝ
ΤΡΕΧΟΥΣΑ ΠΡΟΛΗΠΤΙΚΗ ΜΕΘΟΔΟΣ	ΠΡΟΣΘΗΚΗ ΣΤΟ ΑΡΧΕΙΟ ΕΓΓΡΑΦΩΝ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ WINDOWS ΕΝΟΣ ΑΡΧΕΙΟΥ .LOCKY ΧΩΡΙΣ ΔΙΚΑΙΩΜΑ ΤΡΟΠΟΠΟΙΗΣΗΣ ΑΥΤΗ Η ΜΕΘΟΔΟΣ, ΣΕ ΠΕΡΙΠΤΩΣΗ ΑΝΟΙΓΜΑΤΟΣ ΕΝΟΣ ΜΟΛΥΝΘΕΝΤΟΣ ΠΑΡΑΡΤΗΜΑΤΟΣ, ΕΜΠΟΔΙΖΕΙ ΤΗΝ ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ LOCKY ΚΑΙ, ΣΥΝΕΠΩΣ, ΤΗΝ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ	

ΟΡΙΣΜΟΣ BOTNET	ΈΝΑ **BOTNET** (ΑΠΟ ΤΗΝ ΑΓΓΛΙΚΗ ΣΥΝΘΕΣΗ ΤΩΝ ΛΕΞΕΩΝ «ROBOT» ΚΑΙ «NETWORK») ΕΙΝΑΙ ΕΝΑ ΔΙΚΤΥΟ ΠΡΟΓΡΑΜΜΑΤΩΝ ΣΥΝΔΕΔΕΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΠΟΥ ΕΠΙΚΟΙΝΩΝΟΥΝ ΜΕ ΑΛΛΑ ΠΑΡΟΜΟΙΑ ΠΡΟΓΡΑΜΜΑΤΑ ΓΙΑ ΤΗΝ ΕΚΤΕΛΕΣΗ ΟΡΙΣΜΕΝΩΝ ΕΡΓΑΣΙΩΝ.

ΕΡΩΤΗΣΕΙΣ;

-

ΔΙΑΛΕΙΜΜΑ



**"I'm applying for the Information Security position.
Here is a copy of my resumé, encoded, encrypted and shredded."**