ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ, ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΠΟΚΕΝΤΡΩΣΗΣ
ΓΕΝΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ
ΥΠΗΡΕΣΙΑ ΑΝΑΠΤΥΞΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΔΙΕΥΘΥΝΣΗ ΛΕΙΤΟΥΡΓΙΚΗΣ ΥΠΟΔΟΜΗΣ

Αθήνα, 13 / 2 / 1998

Αριθ. Πρωτ.
ΥΑΠ/Φ.06.11/3633

Ταχ. Δ/νση : Β. Σοφίας 15
Ταχ. Κωδ. : 106 74 ΑΘΗΝΑ
FAX : 3393290

ΠΡΟΣ: Όλα τα Υπουργεία,
Αυτοτελείς Γεν. Γραμματείες,
Γεν. Γραμματείες Περιφερειών
και Νομαρχιακές Αυτοδιοικήσεις
α) Δ/νσεις Διοικητικού
β) Μονάδες Πληροφορικής

ΚΟΙΝ: α) Γραφεία Υπουργών
β) Γραφεία Υφυπουργών
γ) Γεν. Γραμματείς Υπουργείων
δ) Γεν. Γραμματείς Αυτοτελών Γεν. Γραμματειών
ε) Γεν. Γραμματείς Περιφερειών
στ) Νομάρχες

ΘΕΜΑ : «Ασφάλεια Πληροφοριακών Συστημάτων Δημοσίου Τομέα»

1. Τα τελευταία έτη, η λειτουργία των φορέων του Δημοσίου Τομέα, τόσο στη χώρα μας όσο και διεθνώς, στηρίζεται όλο και περισσότερο στη χρήση πληροφοριακών συστημάτων. Μεγάλος όγκος κρίσιμων στοιχείων, που αφορούν ιδιαίτερα σημαντικές κρατικές λειτουργίες, αποθηκεύονται ηλεκτρονικά, υφίστανται όλες τις αναγκαίες επεξεργασίες και διακινούνται με τη βοήθεια πληροφοριακών συστημάτων.

Οι σπουδαιότεροι λόγοι οι οποίοι καθιστούν το Θέμα της ασφάλειας των πληροφοριακών συστημάτων του Δημόσιου Τομέα υψίστης σημασίας είναι:

α) Η επέκταση της χρήσης των πληροφοριακών συστημάτων στο Δημόσιο Τομέα.

β) Η συγκέντρωση και η ηλεκτρονική αποθήκευση σε αυτά μεγάλου όγκου κρίσιμων για την αποτελεσματικότητα του κάθε φορέα στοιχείων.

γ) Η ανάγκη προστασίας του απορρήτου των στοιχείων αυτών.

δ) Η ανάγκη υψηλής διαθεσιμότητας των παραπάνω στοιχείων, η οποία σε πολλούς φορείς αποτελεί προϋπόθεση για τη στοιχειώδη λειτουργία ακόμα και για την επιβίωση τους.

ε) Η ανάγκη εξασφάλισης της ακεραιότητας και της αξιοπιστίας των παραπάνω στοιχείων.
στ) Η συνεχώς αυξανόμενη πολυπλοκότητα των χρησιμοποιουμένων νέων τεχνολογιών της πληροφορικής και των τηλεπικοινωνιών.
ζ) Η σπουδαιότητα και το μέγεθος των πραγματοποιουμένων επενδύσεων για τη δημιουργία, συντήρηση και εκμετάλλευση πληροφοριακών συστημάτων στους φορείς του Δημόσιου Τομέα.
η) Η παρατηρούμενη αύξηση του ηλεκτρονικού εγκλήματος.

2. Σημαντικός παράγοντας για την ασφάλεια των πληροφοριακών συστημάτων των φορέων του Δημοσίου Τομέα είναι **η *προστασία του απορρήτου*** των στοιχείων τα οποία είναι ηλεκτρονικά αποθηκευμένα σ' αυτά.

Οι πρόσφατες τεχνολογικές εξελίξεις παρέχουν τη δυνατότητα αποθήκευσης μεγάλου όγκου στοιχείων σε μικρού μεγέθους μέσα ηλεκτρονικής αποθήκευσης, με αποτέλεσμα να διευκολύνεται η διαρροή τους. Το πρόβλημα αυτό επιδεινώνεται από τη συνεχώς διευρυνόμενη δικτυακή διασύνδεση ηλεκτρονικών υπολογιστών διαφόρων μεγεθών, με τη βοήθεια τόσο τοπικών όσο και ευρείας περιοχής δικτύων. Πολλά από τα στοιχεία αυτά είναι ιδιαίτερα κρίσιμα και ευαίσθητα και συνεπώς η διαρροή τους, πέραν των αρμοδίων και εξουσιοδοτημένων για το χειρισμό τους υπαλλήλων, μπορεί να προκαλέσει σημαντικές ηθικές και υλικές βλάβες σε πλήθος πολιτών και επιχειρήσεων, ενώ παράλληλα μπορεί να προσφέρει σε άλλους πολίτες και επιχειρήσεις ανεπίτρεπτα ηθικά και υλικά οφέλη.

Ο φυσικός και ο ηλεκτρονικός έλεγχος της πρόσβασης στα πληροφοριακά συστήματα των φορέων του Δημοσίου Τομέα, μπορεί να συμβάλει σημαντικά στην προστασία του απορρήτου των παραπάνω ηλεκτρονικά τηρουμένων στοιχείων.

3. Ένας επιπλέον σημαντικός παράγοντας για την ασφάλεια των πληροφοριακών συστημάτων των φορέων του Δημοσίου Τομέα είναι η εξασφάλιση της ***ακεραιότητας*** των στοιχείων τα οποία τηρούνται ηλεκτρονικά σε αυτά.

Με τον όρο ακεραιότητα εννοούμε την προστασία των στοιχείων αυτών, από λανθασμένες (τυχαία ή εσκεμμένα) τροποποιήσεις και διαγραφές, οι οποίες μειώνουν την αξιοπιστία των και δημιουργούν κινδύνους λανθασμένων διοικητικών ενεργειών και αποφάσεων σε βάρος πολιτών και επιχειρήσεων.

Η καλή οργάνωση της λειτουργίας και εκμετάλλευσης των πληροφοριακών συστημάτων και η ορθολογική ανάπτυξη, δοκιμή και τεκμηρίωση του χρησιμοποιουμένου λογισμικού εφαρμογών, μπορούν να συμβάλουν σημαντικά στην εξασφάλιση της ακεραιότητας, της ορθότητας και της αξιοπιστίας των παραπάνω στοιχείων, σε συνδυασμό πάντα με το φυσικό και τον ηλεκτρονικό έλεγχο της πρόσβασης σε αυτά.

4. Σπουδαίος, τέλος, παράγοντας για την ασφάλεια των πληροφοριακών συστημάτων του Δημοσίου Τομέα είναι η εξασφάλιση της ***διαθεσιμότητάς*** τους.

Σε πολλούς φορείς του Δημοσίου Τομέα η μη διαθεσιμότητα των πληροφοριακών τους συστημάτων όποτε τα χρειάζονται, είτε λόγω φυσικών καταστροφών (π.χ. πυρκαγιάς, πλημμύρας, δολιοφθοράς, κλπ) είτε λόγω διαφόρων βλαβών (π.χ. διακοπής παροχής ηλεκτρικού ρεύματος, βλαβών διαφόρων συνιστωσών του υλικού, κλπ), μπορεί να προκαλέσει σημαντικά λειτουργικά προβλήματα, με ιδιαίτερα δυσάρεστες συνέπειες.

Η κατάλληλη χωροθέτηση, η διαμόρφωση των χώρων και ο εξοπλισμός των Μηχανογραφικών Κέντρων με την αναγκαία υποδομή σε συνδυασμό με τις κατάλληλες πολιτικές για:

α) τη συντήρηση του υλικού και του λογισμικού τους,

β) τον εφεδρικό εξοπλισμό και

γ) τα εφεδρικά αντίγράφα των ηλεκτρονικών στοιχείων

μπορούν να συμβάλουν στην εξασφάλιση του επιθυμητού υψηλού επιπέδου διαθεσιμότητας και στην αποφυγή όλων των σχετικών λειτουργικών προβλημάτων.

5. Οι ενέργειες που πρέπει να γίνουν για την ασφάλεια των πληροφοριακών συστημάτων ενός φορέα εξαρτώνται, γενικά, σε μεγάλο βαθμό από τα χαρακτηριστικά και τις ιδιαιτερότητές του. Σύμφωνα με τη διεθνή εμπειρία, *ένα* ολοκληρωμένο πρόγραμμα ασφάλειας πληροφοριακών συστημάτων είναι απαραίτητο να περιλαμβάνει ενέργειες σε πέντε (5) επίπεδα:

α) Νομοθεσίας

β) Εσωτερικού Κανονισμού

γ) Φυσικής Προστασίας

δ) Οργάνωσης και Διαδικασιών

ε) Ηλεκτρονικής Προστασίας (στο υλικό και στο λογισμικό)

Ορισμένα πρακτικά βήματα τα οποία κάθε φορέας του Δημοσίου Τομέα ενδείκνυται να πραγματοποιήσει για την ασφάλεια των πληροφοριακών συστημάτων του είναι :

- Ο εντοπισμός των βασικών κινδύνων και προβλημάτων όσον αφορά στην ασφάλεια των πληροφοριακών συστημάτων του, λαμβάνοντας υπόψη όλες τις ιδιαιτερότητές του, και κατηγοριοποίησή τους σε επίπεδα προτεραιότητας.

- Ο προσδιορισμός όλων των αναγκαίων ενεργειών, οι οποίες πρέπει να γίνουν στα πέντε παραπάνω επίπεδα, για την αντιμετώπιση των προαναφερθέντων κινδύνων και προβλημάτων ασφάλειας (κυρίως αυτών με την υψηλότερη προτεραιότητα).

- Η κατάρτιση χρονοδιαγράμματος της υλοποίησης των ενεργειών αυτών

- Η μέριμνα, ώστε, σε όλες τις μελέτες και τα έργα πληροφοριακών συστημάτων, τα οποία πρόκειται ο φορέας να υλοποιήσει, να δίνεται ιδιαίτερη έμφαση στα θέματα της ασφάλειάς τους.

Για τον αποτελεσματικότερο συντονισμό των φορέων του Δημοσίου Τομέα σε θέματα ασφάλειας πληροφοριακών συστημάτων και δικτύων παρακαλούνται

α. Όλες οι Μονάδες Πληροφορικής να επιστρέψουν συμπληρωμένο το επισυναπτόμενο ερωτηματολόγιο στην Υπηρεσία Ανάπτυξης Πληροφορικής το αργότερο μέχρι τις 20 Μαρτίου 1998, και

β. Όλες οι Διευθύνσεις Διοικητικού να ενημερώσουν το ταχύτερο δυνατό τους εποπτευόμενους από την Υπηρεσία τους φορείς.

6. Διευκρινίσεις σχετικά με το περιεχόμενο της εγκυκλίου παρέχονται από τους, κ. Αλέξανδρο Λεβεντίδη, Προϊστάμενο της Διεύθυνσης Λειτουργικής Υποδομής, και κ. Ευριπίδη Λουκή, Ειδικό Επιστήμονα (τηλ. 3393254, 3393276).

Ο Υπουργός

Αλέξανδρος Παπαδόπουλος

ΑΚΡΙΒΕΣ ΑΝΤΙΓΡΑΦΟΝ
ΑΠΟ ΤΟ ΓΡΑΦΕΙΟ ΤΗΣ ΓΡΑΜΜΑΤΕΙΑΣ

<u>Εσωτερική Διανομή :</u>

1. Γραφείο κ. Υπουργού
2. Γραφείο κ. Υφυπουργού
3. Γραφείο κ. Γεν. Γραμματέα
4. Γραφεία κ.κ. Γεν Διευθυντών
5. Γραμματεία της Επιτροπής Παρακολούθησης του Ε.Π. «ΚΛΕΙΣΘΕΝΗΣ»

ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ

ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Α. Γενικά

Α.1. Ποιες είναι οι κυριότερες κατηγορίες στοιχείων τα οποία αποθηκεύετε στο πληροφοριακό σας σύστημα;

Πόσο σημαντικά είναι αυτά για τη συνολική λειτουργία του φορέα σας;

Α.2. Ποια προβλήματα θα υπάρξουν για το φορέα σας, εάν τα παραπάνω στοιχεία:

- Χαθούν
- Δεν είναι διαθέσιμα για ένα μικρό χρονικό διάστημα
- Δεν είναι διαθέσιμα για ένα μεγαλύτερο χρονικό διάστημα

Α.3. Ποιους μηχανισμούς διαθέτετε για τον έλεγχο της πρόσβασης στα πληροφοριακά σας συστήματα και την αυθεντικοποίηση;

Β. Διασφάλιση Απορρήτου

Β.1. Ποια είναι τα κυριότερα απορρήτου χαρακτήρα στοιχεία τα οποία αποθηκεύονται ηλεκτρονικά στο πληροφοριακό σας σύστημα;

Β.2. Με ποιους τρόπους εξασφαλίζετε την εμπιστευτικότητα των απορρήτων αυτών στοιχείων;

Γ. Διασφάλιση Ακεραιότητας

Γ.1. Ποιους μηχανισμούς ελέγχου διαθέτετε για την εξασφάλιση της ακεραιότητας των στοιχείων τα οποία είναι αποθηκευμένα στα πληροφοριακά σας συστήματα έναντι λανθασμένων (τυχαίων ή εσκεμμένων) τροποποιήσεων και διαγραφών τους;

Γ.2. Έχετε διαμορφώσει μία συστηματική πολιτική αντιμετώπισης των ηλεκτρονικών ιών;

Δ. Προστασία από φυσικούς κινδύνους

Δ.1. Ποια μέτρα λαμβάνετε για την προστασία των πληροφοριακών σας συστημάτων από φυσικές καταστροφές (π.χ. πυρκαγιές, πλημμύρες, κ.λ.π.) ;

Δ.2. Ποια μέτρα λαμβάνετε για την προστασία των πληροφοριακών σας συστημάτων από κακόβουλες ενέργειες (π.χ. κλοπές, δολιοφθορές, βανδαλισμοί, κ.λ.π.) ;

Δ.3. Ποιους μηχανισμούς διαθέτετε για τον έλεγχο της εισόδου ατόμων στον χώρο του μηχανογραφικού σας κέντρου και την ανίχνευση λαθραίας εισόδου ;

Πως γίνεται η εξακρίβωση της ταυτότητας των εισερχομένων ατόμων σ' αυτό;

Ε. Διασφάλιση Διαθεσιμότητας

Ε.1. Με ποιους τρόπους εξασφαλίζετε τη διαθεσιμότητα των διαφόρων συνιστωσών του πληροφοριακού σας συστήματος, όπως π.χ.

- Υλικού

- Λογισμικού
- Δικτυακών συνδέσεων
- Δεδομένων

κ.λ.π.

για τις, ζωτικής σημασίας, βλαβών, προβλημάτων, κ.λ.π.

Ε.2. Ποιους μηχανισμούς διαθέτετε για την προστασία του μηχανογραφικού σας εξοπλισμού από διαταραχές της τάσεως και διακοπές του ηλεκτρικού ρεύματος;

Ε.3. Ποιους μηχανισμούς διαθέτετε για την αποκατάσταση της ομαλής λειτουργίας του πληροφοριακού σας συστήματος μετά από προβληματικές καταστάσεις;

ΣΤ. Ασφάλεια δικτύων

Ποια μέτρα λαμβάνετε για την ασφάλεια του δικτύου σας (έλεγχος πρόσβασης και αυθεντικοποίηση, εμπιστευτικότητα, ακεραιότητα, εξασφάλιση διαθεσιμότητας κ.λ.π.) ;

Ζ. Οργάνωση

Έχετε ολοκληρωμένο πρόγραμμα ασφάλειας των πληροφοριακών σας συστημάτων, το οποίο να καλύπτει όλες τις πλευρές της

- Εμπιστευτικότητα απορρήτων στοιχείων
- Ακεραιότητα στοιχείων
- Ασφάλεια από φυσικούς κινδύνους
- Διαθεσιμότητα
- Αποκατάσταση ομαλής λειτουργίας μετά από προβληματικές καταστάσεις

Η. Εμφανισθέντα Προβλήματα

Ποια συγκεκριμένα προβλήματα σχετικά με Θέματα ασφάλειας διαπιστώθηκαν στο χώρο ευθύνης σας κατά τη διάρκεια της τελευταίας πενταετίας και πως τα αντιμετωπίσατε (συνοπτική περιγραφή τους - τεχνικές και διοικητικές παρεμβάσεις που ακολούθησαν) ;