ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

ΝΙΚΟΛΑΟΣ Ι. ΝΙΚΟΛΟΠΟΥΛΟΣ
Βουλευτής Αχαΐας - ΝΕΑ ΔΗΜΟΚΡΑΤΙΑ

ΑΝΑΦΟΡΑ
ΠΡΟΣ ΤΟΥΣ ΥΠΟΥΡΓΟΥΣ:

- **Οικονομικών**
- **Εσωτερικών**
- **Εθνικής Αμυνας**

Θέμα: Προβληματισμοί της Ενωσης Πληροφορικών

Σχετικά με το υπόμνημα της Ενωσης Πληροφορικών Ελλάδος και τις θέσεις που εκφράζουν.

Αρ. Πρωτ.

Πάτρα

Ο αναφέρων Βουλευτής

Νίκος Ι. Νικολόπουλος

ΠΑΔ 372
21 ΟΚΤ. 2011

Μιαούλη 48, 262 22 Πάτρα, Τηλ.: 2610 344 700-2, Φαξ: 2610 344 703
Βουλής 4, 105 62 Αθήνα, Τηλ.: 210 370 6427, Φαξ: 210 325 3729
nikolopoulos@parliament.gr

ΕΝΩΣΗ
ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Ένωση Πληροφορικών Ελλάδας
Κοδριγκτώνος 33, 5ος όροφος
ΤΚ 10434, Αθήνα
http://www.epe.org.gr
e-mail: info@epe.org.gr

ΠΡΟΣ: α) Πολιτική ηγεσία Υπουργείου Οικονομικών

β) Πολιτική ηγεσία Υπουργείου Εσωτερικών

γ) Πολιτική ηγεσία Υπουργείου Εθνικής Άμυνας

δ) Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ)

ε) Αρχή Προστασίας Προσωπικών Δεδομένων (ΑΠΠΔ)

ς) Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)

ΚΟΙΝ: α) Γραφείο Πρωθυπουργού

β) Βουλευτές Ελληνικού Κοινοβουλίου

γ) Τμήματα Πληροφορικής Πανεπιστημιακού και Τεχνολογικού Τομέα των ΑΕΙ (βλ. πίνακα που συνοδεύει την παρούσα επιστολή)

δ) Μέσα ενημέρωσης

ΘΕΜΑ: "Παρέμβαση για το ζήτημα της Πολιτικής Ασφάλειας σε δημόσιες υπηρεσίες και οργανισμούς"

Αθήνα, 13 Οκτωβρίου 2011

Αξιότιμες Κυρίες / Αξιότιμοι Κύριοι,

Η ΕΠΕ (Ένωση Πληροφορικών Ελλάδας), ως φορέας έκφρασης και επίσημης αντιπροσώπευσης των δεκάδων χιλιάδων επιστημόνων και επαγγελματιών Πληροφορικής και νέων Τεχνολογιών, αποφοίτων Πληροφορικής των ιδρυμάτων του Πανεπιστημιακού και του Τεχνολογικού τομέα της Ανώτατης

Εκπαίδευσης της χώρας μας, μεταξύ των άλλων, έχει επισημάνει πολλές φορές στο παρελθόν τα πολύ σοβαρά προβλήματα στη λειτουργία κρατικών φορέων και οργανισμών, σε ότι αφορά τον τρόπο μελέτης, ανάθεσης, προμήθειας και χρήσης υλικού (hardware) και λογισμικού (software) υποδομής.

Η ΕΠΕ έχει επίσης επισημάνει την επισταμένη ανάγκη ιδιαίτερης προσοχής σε ζητήματα Πολιτικής Ασφάλειας (Security Policy) σε σχέση με τις υποδομές αυτές, τόσο σε επίπεδο δεδομένων προσωπικού χαρακτήρα, όσο και σε επίπεδο διοικητικών πληροφοριών και διαδικασιών γενικότερα, καθώς οι Τεχνολογίες Πληροφορικής και Τηλεπικοινωνιών (ΤΠΕ)απαιτούν εξειδικευμένες γνώσεις και πρακτικές, από προσωπικό που συχνά δεν τις κατέχει ή δεν είναι αρμόδιο για αυτά τα ζητήματα.

Ως αποτέλεσμα, ακόμα και βασικές διαδικασίες και πρακτικές ασφάλειας, όπως ο έλεγχος πρόσβασης σε ψηφιακά αρχεία και ηλεκτρονική αλληλογραφία κρατικών οργανισμών και δημόσιων φορέων, όχι απλώς να μην διασφαλίζεται, αλλά συχνά να τίθεται σε άμεσο κίνδυνο, με άγνωστες εν γένει συνέπειες, βραχυπρόθεσμα ή μακροπρόθεσμα, σε ότι αφορά την προστασία προσωπικών δεδομένων ατόμων αλλά και ζωτικές πληροφορίες για το σύνολο της κρατικής υποδομής.

Εδώ και αρκετούς μήνες, ήδη από τις αρχές του 2010, η χώρα μας βρίσκεται υπό αυστηρή δημοσιοοικονομική επιτήρηση από την Ευρωπαϊκή Ένωση, μέσω των αρμόδιων οργάνων της. Εκπρόσωποι του Eurogroup, της Ευρωπαϊκής Κεντρικής Τράπεζας (ΕΚΤ) και του Διεθνούς Νομισματικού Ταμείου (ΔΝΤ), βρίσκονται εκ περιτροπής στην Ελλάδα, με αποστολή κάθε φορά τον λεπτομερή έλεγχο μιας τεράστιας πληθώρας στοιχείων που αφορούν το δημοσιοοικονομικό έλεγχο και την αξιολόγηση των αποτελεσμάτων εφαρμογής των αντίστοιχων νόμων που έχουν ψηφιστεί έκτοτε και αφορούν ακριβώς σε αυτή τη δημοσιονομική προσαρμογή της χώρας μας.

Οι αρμοδιότητες αυτών των προσώπων, των οποίων ο συνολικός αριθμός και ο ρόλος του καθενός ξεχωριστά δεν είναι απόλυτα ξεκάθαρα ακόμα και τώρα, δίνει εκ των πραγμάτων μοναδική δυνατότητα πρόσβασης σε υπουργεία, δημόσιους φορείς, κρατικές υπηρεσίες και οργανισμούς. Υπό κανονικές συνθήκες, παρόμοιο επίπεδο πρόσβασης, τόσο σε ευρύτητα όσο και σε βάθος πληροφόρησης, έχουν μόνο διορισμένοι ορκισμένοι δημόσιοι υπάλληλοι κάθε βαθμίδας, οι οποίοι όμως και πάλι εργάζονται σε συγκεκριμένα τμήματα οργανισμών και φορέων, δηλαδή ποτέ δεν έχουν τόσο μαζική ελεύθερη πρόσβαση σε λεπτομερή στοιχεία π.χ. άλλου υπουργείου.

Αντίθετα, στην περίπτωση των λεγόμενων «ελεγκτών» που επισκέπτονται τακτικά πλέον τη χώρα μας, μπορούν να εντοπιστούν ορισμένα εξαιρετικά ζητήματα ασφάλειας:

1. Δεν είναι απόλυτα γνωστός (δημόσια) ο ακριβής αριθμός τους, καθώς και η ιδιότητα, η αρμοδιότητα και η εν γένει βαθμίδα του καθενός, ως μέλος της κάθε «αποστολής».
2. Δεν πρόκειται για διορισμένους ορκισμένους δημόσιους υπαλλήλους, αλλά για αλλοδαπούς, υπαλλήλους διαφόρων φορέων και οργανισμών (Eurogroup, ΕΚΤ, ΔΝΤ), πράγμα που σημαίνει ότι

Καδρυγκτώνος 33, (3ος όροφος), ΤΚ 10673, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

δεν δεσμεύονται απαραιτήτως από κανένα απόρρητο, ούτε και διοικητική διαδικασία ελέγχου, σε ότι αφορά το χειρισμό ευαίσθητων δεδομένων του εκάστοτε κρατικού οργανισμού τον οποίο επισκέπτονται.

3. Η παραμονή τους στην Ελλάδα είναι συνήθως εξαιρετικά μικρή, μερικά 24ωρα ή μερικές ημέρες, πράγμα που σημαίνει ότι οποιαδήποτε διαδικασία δεν ελεγχθεί επιτόπου τη στιγμή που πραγματοποιείται, είναι εξαιρετικά δύσκολο ως απίθανο να μπορεί να ελεγχθεί εκ των υστέρων - πολύ περισσότερο να επιβληθούν οποιαδήποτε μορφής «κυρώσεις» αν διαπιστωθούν παραβιάσεις διοικητικών κανονισμών ως προς το απόρρητο.

4. Αντίθετα με τη διοικητική οργάνωση και το σαφή διαχωρισμό αρμοδιοτήτων, ανά υπουργείο ευθύνης, ανά οργανισμό, ή ακόμα και ανά υπηρεσία ή τμήμα μέσα σε έναν οργανισμό, όπου η πρόσβαση σε αρχεία και δεδομένα από υπαλλήλους γίνεται αναγκαστικά «διαμερισματοποιημένα» (compartmentalized), στην περίπτωση των «ελεγκτών» ο διαχωρισμός αυτός φαίνεται να εξαφανίζεται εντελώς ή τουλάχιστον σε πολύ μεγάλο βαθμό. Πρακτικά, πολύ λίγοι άνθρωποι, πέραν και εκτός των ίδιων των κρατικών φορέων, αποκτούν ξαφνικά πρόσβαση σε τεράστιας ευρύτητας πληροφορίες.

5. Επιπλέον, ο τρόπος και οι συνθήκες των ελέγχων που γίνονται στα πλαίσια των παραπάνω «αποστολών» είναι τέτοιες, ώστε η πληροφόρηση που λαμβάνουν οι «ελεγκτές» είναι καθολική, λεπτομερέστατη και απόλυτα έγκυρη, εφόσον προέρχεται από τις πιο επίσημες και αρμόδιες πηγές. Αυτό σημαίνει πρακτικά ότι το επίπεδο ασφάλειας (εμπιστευτικότητας) των πληροφοριών αυτών είναι το ανώτερο δυνατό, εννοείται τουλάχιστονγια τον εκάστοτε φορέα. Κάποιοι κρατικοί φορείς διαχειρίζονται πληροφορίες χαμηλού επιπέδου εμπιστευτικότητας (π.χ. διαχειριστικά έξοδα μιας γραμματείας ενός δημόσιου οργανισμού), ενώ άλλοι θέματα εξαιρετικής κρισιμότητας σε επίπεδο εθνικής ασφάλειας (π.χ. αγορές και αποθέματα καυσίμων Σωμάτων Στρατού, στο υπουργείο Άμυνας).

6. Είναι φυσικό εκ των πραγμάτων, οι παραπάνω έλεγχοι να βασίζονται κατά κανόνα σε ψηφιακά αρχεία και ηλεκτρονική αλληλογραφία, μεταξύ των «ελεγκτών» και των αρμόδιων υπαλλήλων του κάθε οργανισμού, τόσο κατά τη διάρκεια των συναντήσεων, όσο και πριν και μετά από τις επισκέψεις των «αποστολών» στη χώρα μας. Ως εκ τούτου, δεδομένα σε ψηφιακή μορφή αποθηκεύονται, αντιγράφονται, τυπώνονται, μεταδίδονται, κατά το δοκούν, στα πλαίσια των τυπικών (κανονικών) διαδικασιών. Αυτό σημαίνει ότι ο βαθμός έκθεσής τους, σε ότι αφορά την εμπιστευτικότητα και τον έλεγχο πρόσβασης σε αυτά, να είναι εξαιρετικά μεγάλος και να μην μπορεί εν γένει να περιοριστεί στα πλαίσια μιας συγκεκριμένης συνάντησης, σε συγκεκριμένο τόπο και χρόνο.

7. Σημειώνεται ότι, ενώ από την πλευρά της εκάστοτε αρμόδιας υπηρεσίας ή φορέα ο έλεγχος της

Καδρυγκτώνος 33, (5ος όροφος), ΤΚ 10434, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

ασφάλειας πρόσβασης μπορεί εν γένει να ελεγχθεί (εσωτερικό δίκτυο, υποδομή Η/Υ, διαδικασίες προσωπικού), αντίθετα στην πλευρά του «αποδέκτη», δηλαδή των μελών των «αποστολών» αυτών, αντίστοιχοι έλεγχοι είναι μάλλον αδύνατοι. Πρακτικά, οτιδήποτε καταλήγει στους Η/Υ, στους λογαριασμούς ηλεκτρονικής αλληλογραφίας ή στους φακέλους με τα εκτυπωμένα αντίγραφα των «ελεγκτών», δηλαδή οτιδήποτε παραλαμβάνουν ως δεδομένα για τους ελέγχους, δεν μπορεί να ελεγχθεί ως προς την εξουσιοδότηση πρόσβασης σε αυτά (ή ασφαλούς διαγραφής τους), παρά μόνο από τους ίδιους του «ελεγκτές», στο βαθμό και την έκταση που οι ίδιοι το επιθυμούν και το επιτρέπουν.

8. Σημειώνεται επίσης ότι κάποιες τεχνολογίες και κάποιες ευρύτατα διαδεδομένες πρακτικές χρήσης αυτών εμπεριέχουν αποδεδειγμένα αυξημένο κίνδυνο σε ότι αφορά την ασφάλεια των εμπλεκόμενων δεδομένων. Για παράδειγμα, είναι γνωστό ότι συγκεκριμένα πρωτόκολλα ασύρματης σύνδεσης σε τοπικό δίκτυο (WiFi) εμπεριέχουν σαφή κίνδυνο παραβίασης του απορρήτου, λόγω προβλημάτων στη σχεδίαση ή στην υλοποίησή τους. Και μπορεί αυτό να εντάσσεται εν μέρει στους αντίστοιχους μηχανισμούς ασφάλειας του συγκεκριμένου φορέα/τοποθεσίας (ασφάλεια τοπικού δικτύου WiFi, αν χρησιμοποιήθηκε κατά τη συνάντηση), αλλά η χρήση του εκ των υστέρων, σε άλλο τόπο και χρόνο, από τον «παραλήπτη», δημιουργεί εν γένει έκθεση αντίστοιχης σοβαρότητας, σε όποια δεδομένα αποθήκευσε και πήρε μαζί του (ετεροχρονισμένη παραβίαση, μέσω του ίδιου αδύναμου κρίκου).

9. Ανάλογοι κίνδυνοι υπάρχουν στην αποστολή χωρίς ισχυρή κρυπτογράφηση, μηνυμάτων, συνημμένων εγγράφων και αρχείων, μέσω ηλεκτρονικού ταχυδρομείου, καθώς στην περίπτωση αυτή τα δεδομένα συχνά διαχέονται στο διαδίκτυο με ακαθόριστο τρόπο (ανάλογα τα πρωτόκολλα δρομολόγησης και την τεχνολογία πρόσβασης) και παραμένουν σε προσωρινές μνήμες (caches) ενδιάμεσων κόμβων για πολλές ώρες ή και ημέρες, των οποίων η ασφάλεια είναι μη ελέγξιμη και συχνά εντελώς άγνωστη στον αποστολέα και στον παραλήπτη.

10. Ειδικά για την πολύ διαδεδομένη τεχνολογία αποθήκευσης τύπου SSD(Solid-StateDisk), που συχνά βλέπουμε ως πολύ μικρές φορητές συσκευές τύπου «USBstick» ή «thumbdrive», είναι φυσικό να δίνεται ιδιαίτερη προσοχή σε επίπεδο ελέγχου πρόσβασης σε ευαίσθητα δεδομένα, καθώς επιτρέπει την αποθήκευση μαζικού όγκου δεδομένων γρήγορα, σε πολύ μικρό χώρο και χωρίς ιδιαίτερο εξοπλισμό (όπως π.χ. στην περίπτωση CD ή DVD εγγραφής). Επίσης, είναι γνωστό ότι ακόμα και όταν προβλέπονται συγκεκριμένες διαδικασίες ασφαλούς διαγραφής, οι συσκευές SSD είναι εν γένει εξαιρετικά δύσκολο ως αδύνατο να διαγραφούν εντελώς (securewipe) λόγω της συγκεκριμένης τεχνολογίας και της κατασκευής τους, με αποτέλεσμα να χρειάζονται ειδικό χειρισμό όταν τα απαιτούμενα επίπεδα ασφάλειας είναι αυξημένα.

Τα παραπάνω είναι μερικά μόνο ενδεικτικά σημεία σχετικά με το γενικότερο ζήτημα της ασφάλειας,

Καβαφάκτωνος 33, (5ος όροφος), ΤΚ 10434, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

σε ότι αφορά τις «αποστολές» εκπροσώπων των οργανισμών που εμπλέκονται εδώ και σχεδόν 2 χρόνια με τη δημοσιονομική επιτήρηση της Ελλάδας. Αφορούν πρακτικά ζητήματα, χειρισμού τεχνολογιών και συσκευών καθημερινής χρήσης, τα οποία ενδέχεται να εμπεριέχουν σημαντικό κίνδυνο έκθεσης ευαίσθητων δεδομένων κρατικών φορέων, δημόσιων οργανισμών, υπουργείων και υποδομών.

Συχνά, το ζήτημα της ασφάλειας δεδομένων και υποδομών ΤΠΕ παρερμηνεύεται και θεωρείται θέμα αποκλειστικά και μόνο στρατιωτικής φύσεως. Αυτό είναι σοβαρότατο λάθος, ιδιαίτερα στη συγκεκριμένη περίπτωση. Η βαθιά γνώση, με λεπτομέρεια και σαφήνεια, πληροφοριών για σημαντικές κρατικές υποδομές, διαθέσιμα και υπηρεσίες της χώρας μας, ειδικά σε αυτή τη χρονική στιγμή και υπό τις σημερινές διεθνείς συνθήκες, δυνητικά αποτελεί από μόνο του ένα εξαιρετικό στρατηγικό πλεονέκτημα, σε πολιτικό, οικονομικό ακόμα και σε στρατιωτικό επίπεδο.

Ενδεικτικά αναφέρονται μερικά παραδείγματα:

1. Η γνώση της λεπτομερούς οικονομικής αποτίμησης μιας δημόσιας υπηρεσίας ή οργανισμού, η οποία πρόκειται βάσει επίσημων εξαγγελιών να αποκρατικοποιηθεί στο αμέσως επόμενο χρονικό διάστημα, αποτελεί πληροφορία εξαιρετικά μεγάλης αξίας για χρηματοπιστωτικούς οργανισμούς που πρόκειται να αποτιμήσουν ή και να εξαγοράσουν οι ίδιοι τον οργανισμό αυτό.
2. Η γνώση της λεπτομερούς οικονομικής αποτίμησης μιας δημόσιας υποδομής (π.χ. αυτοκινητόδρομος διοδίων), η οποία πρόκειται βάσει επίσημων εξαγγελιών να εκποιηθεί στο αμέσως επόμενο χρονικό διάστημα, αποτελεί εξίσου αξιοποιήσιμη πληροφορία υψηλής αποτίμησης, που από μόνη της είναι «εμπορεύσιμη» σε επίπεδο διεθνών χρηματοπιστωτικών συμφωνιών.
3. Η γνώση της λεπτομερούς οικονομικής αποτίμησης ενός δημόσιου οργανισμού, υπηρεσίας ή υποδομής, που ακόμα **δεν** έχει ανακοινωθεί ότι πρόκειται να αποκρατικοποιηθεί, αποτελεί πληροφορία ακόμα μεγαλύτερης αξίας, που εντάσσεται στην κατηγορία της «εσωτερικής πληροφόρησης» (insidetrading).
4. Η προσωρινή ή μόνιμη παραχώρηση μεγάλου όγκου δεδομένων φορολογικής ή εμπορικής φύσεως, πολιτών και ιδιωτικών επιχειρήσεων, εκθέτει τα δεδομένα αυτά με τρόπο και χρόνο που δεν μπορεί να προβλεφθεί. Για παράδειγμα, μαζικά δεδομένα φορολογικού μητρώου ή ιατρικού ιστορικού εμπεριέχουν εν γένει τον κίνδυνο διαρροής προσωπικών πληροφοριών πολιτών και επιχειρήσεων σε τρίτους, που στη συγκεκριμένη περίπτωση ίσως να βρίσκονται εντελώς εκτός της χώρας και άρα εκτός κάθε ανάλογου περιορισμού ή κύρωσης (ΑΠΠΔ, ΑΔΑΕ, κτλ).
5. Τα δημοσιοοικονομικά στοιχεία που συνδέονται έμμεσα ή άμεσα με τη διοικητική υποστήριξη (logistics), σωμάτων ασφαλείας και στρατιωτικών μονάδων, εκθέτουν πληροφορίες πολύ μεγαλύτερης ευρύτητας και κρισιμότητας. Τακτικά έξοδα για καύσιμα, διατροφή, έξοδα

Καδρανητώνος 33, (5ος όροφος), ΤΚ 10431, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

μετακίνησης προσωπικού, εξοπλιστικά προγράμματα, αποστολές εξωτερικού, πρεσβείες και προξενεία, αποτελούν εξαιρετικά σημαντικές πληροφορίες που τυπικά προστατεύονται σε επίπεδο εθνικής ασφάλειας και κατατίθενται μόνο στο Κοινοβούλιο, σε έκταση και λεπτομέρεια που δεν θέτει σε κίνδυνο άλλες πιο κρίσιμες πληροφορίες.

Οι παραπάνω παρατηρήσεις αποτελούν μια ενδεικτική και μόνο αναφορά των ζητημάτων ασφάλειας ΤΠΕ που συνδέονται, άμεσα ή έμμεσα, με το έργο των «ελεγκτών» των οργάνων του Eurogroup, της ΕΚΤ και του ΔΝΤ στη χώρα.

Είναι φανερό ότι οι κίνδυνοι ασφάλειας σε επίπεδο ελέγχου πρόσβασης και μεταφοράς ευαίσθητων δεδομένων εθνικού χαρακτήρα υπάρχουν, είναι ευρέως γνωστοί σε τεχνικό επίπεδο και είναι υπαρκτοί σε καθημερινή βάση. Είναι επίσης βέβαιο ότι τέτοιες κρίσιμες πληροφορίες σίγουρα αποτελούν μέρος των ελέγχων και των συναντήσεων αυτών, καθώς και επικοινωνιών πριν και μετά τις συναντήσεις, ως μέρος της φυσιολογικής διαδικασίας και συνεργασίας. Τέλος, είναι απόλυτα σαφές ότι κάποιες από τις πληροφορίες αυτές έχουν χαρακτήρα εθνικού απορρήτου, η έκθεσή τους σε μη προβλεπόμενους αποδέκτες αποφέρει σημαντικότατη βλάβη στη χώρα και επιπλέον αποτελούν εμπορεύσιμο προϊόν εξαιρετικά υψηλής χρηματιστηριακής αξίας σε παγκόσμιο επίπεδο.

Ας μην ξεχνάμε ότι είναι πολύ πρόσφατη η περίπτωση των τηλεφωνικών υποκλοπών πριν μερικά χρόνια μέσω εταιρίας κινητής τηλεφωνίας, η οποία άγγιξε τα πιο υψηλά ιστάμενα πρόσωπα της επίσημης Πολιτείας και που ποτέ δεν διαλευκάνθηκε πλήρως μέχρι και σήμερα, ούτε ως προς την έκτασής της, ούτε ως προς τις επιπτώσεις της σε κάθε επίπεδο.

Βάσει των παραπάνω, **η ΕΠΕ καλεί τους αρμόδιους κρατικούς φορείς, τις αρμόδιες δημόσιες υπηρεσίες και τα συναρμόδια υπουργεία, να απαντήσουν δημοσίως, μέσω δελτίου τύπου ή στο Κοινοβούλιο, και να ενημερώσουν την Ελληνική Κοινωνία για τα ακόλουθα:**

1. Να απαντήσουν σχετικά με τα ζητήματα που αναφέρονται παραπάνω (σημεία 1-10), δηλαδή για τις **προβλέψεις διασφάλισης** της ασφάλειας δεδομένων και γενικότερα την εφαρμοζόμενη Πολιτική Ασφάλειας, κατά τους ελέγχους και τις συναντήσεις των «αποστολών» στην Ελλάδα.
2. Να απαντήσουν σχετικά με τη διασφάλιση της εμπιστευτικότητας των ευαίσθητων πληροφοριών, προσωπικού ή εθνικού απορρήτου, σε επίπεδο **περιορισμού του κινδύνου** σε πιθανή έκθεση, δηλαδή σε περιπτώσεις όπως τα παραδείγματα που αναφέρονται παραπάνω (σημεία 1-5).
3. Να δεσμευτούν **επίσημα** και να διαβεβαιώσουν **δημόσια** ότι οι παραπάνω προβλέψεις υπάρχουν, εφαρμόζονται και αναθεωρούνται όταν πρέπει, έτσι ώστε να διασφαλιστεί πλήρως το απόρρητο ευαίσθητων πληροφοριών προσωπικού ή εθνικού χαρακτήρα.

Η Ένωση Πληροφορικών Ελλάδας (ΕΠΕ), με αίσθημα ευθύνης, επισημαίνει και πάλι την ανάγκη

Καδρακτώνος 33, (5ος όροφος), ΤΚ 10434, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

διαχείρισης του συγκεκριμένου ζητήματος από την Πολιτεία, **άμεσα**, καθώς τα ζητήματα ασφάλειας σε σχέση με τις δημόσιες υπηρεσίες και υποδομές αποτελούν εν γένει έναν από τους πιο σημαντικούς παράγοντες διαχείρισης της σημερινής κρίσης, που εξελίσσεται και διαφοροποιείται καθημερινά, σε πολιτικό, οικονομικό και κοινωνικό επίπεδο.

Περιμένουμε εναγωνίως τις θέσεις και απαντήσεις σας,

Εκ μέρους του Διοικητικού Συμβουλίου
της Ένωσης Πληροφορικών Ελλάδας

Ο Πρόεδρος
Μαυροφίδης Θωμάς
(τηλ. 6944246558)

Ο Γενικός Γραμματέας
Μουμουτζής Νεκτάριος
(τηλ. 6948044562)

Καβαφάκη 33, (5ος όροφος), ΤΚ 10434, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

Πίνακας τμημάτων Πληροφορικής

1. Βιομηχανικής Πληροφορικής, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Καβάλας
2. Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών, Πανεπιστήμιο Πελοποννήσου
3. Επιστήμης και Τεχνολογίας Υπολογιστών, Πανεπιστήμιο Πελοποννήσου
4. Επιστήμης Υπολογιστών, Πανεπιστήμιο Κρήτης
5. Εφαρμοσμένης Πληροφορικής, Πανεπιστήμιο Μακεδονίας
6. Εφαρμοσμένης Πληροφορικής και Πολυμέσων, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Κρήτης
7. Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, (μόνο) Κατεύθυνση Ηλεκτρονικής και Ηλεκτρονικών Υπολογιστών, ΑΠΘ
8. Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, (μόνο) Κατεύθυνση Πληροφορικής, ΕΜΠ
9. Ηλεκτρονικών Μηχανικών και Μηχανικών Υπολογιστών, Πολυτεχνείο Κρήτης
10. Ηλεκτρονικών Υπολογιστικών Συστημάτων, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Πειραιά
11. Μηχανικών Η/Υ και Πληροφορικής, Πανεπιστήμιο Πατρών
12. Μηχανικών Η/Υ Τηλεπικοινωνιών και Δικτύων, Πανεπιστήμιο Θεσσαλίας
13. Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου
14. Μηχανικών Πληροφορικής και Τηλεπικοινωνιών, Πανεπιστήμιο Δυτικής Μακεδονίας
15. Πληροφορικής, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
16. Πληροφορικής, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Αθήνας
17. Πληροφορικής, Αλεξάνδρειο Τεχνολογικό Εκπαιδευτικό Ίδρυμα Θεσσαλονίκης
18. Πληροφορικής, Ελληνικό Ανοικτό Πανεπιστήμιο
19. Πληροφορικής, Ιόνιο Πανεπιστήμιο
20. Πληροφορικής, Οικονομικό Πανεπιστήμιο Αθηνών
21. Πληροφορικής, Πανεπιστήμιο Ιωαννίνων
22. Πληροφορικής, Πανεπιστήμιο Πειραιά
23. Πληροφορικής και Επικοινωνιών, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Σερρών

Καβουγιάννου 33, (5ος όροφος), ΤΚ 10434, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

24. Πληροφορικής και Τεχνολογίας Υπολογιστών, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Λαμίας
25. Πληροφορικής και Τεχνολογίας Υπολογιστών, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Δυτικής Μακεδονίας
26. Πληροφορικής και Τηλεματικής, Χαροκόπειο Πανεπιστήμιο
27. Πληροφορικής και Τηλεπικοινωνιών, Πανεπιστήμιο Αθηνών
28. Πληροφορικής με εφαρμογές στη Βιοϊατρική, Πανεπιστήμιο Στερεάς Ελλάδας
29. Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Ηπείρου
30. Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Καλαμάτας
31. Τεχνολογίας Πληροφορικής και Τηλεπικοινωνιών, Τεχνολογικό Εκπαιδευτικό Ίδρυμα Λάρισας
32. Τηλεπικοινωνιακών Συστημάτων και Δικτύων (Ναυπάκτου), Τεχνολογικό Εκπαιδευτικό Ίδρυμα Μεσολογγίου
33. Ψηφιακών Συστημάτων, Πανεπιστήμιο Πειραιά

Καδρηγκτώνος 33, (5ος όροφος), ΤΚ 10434, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr