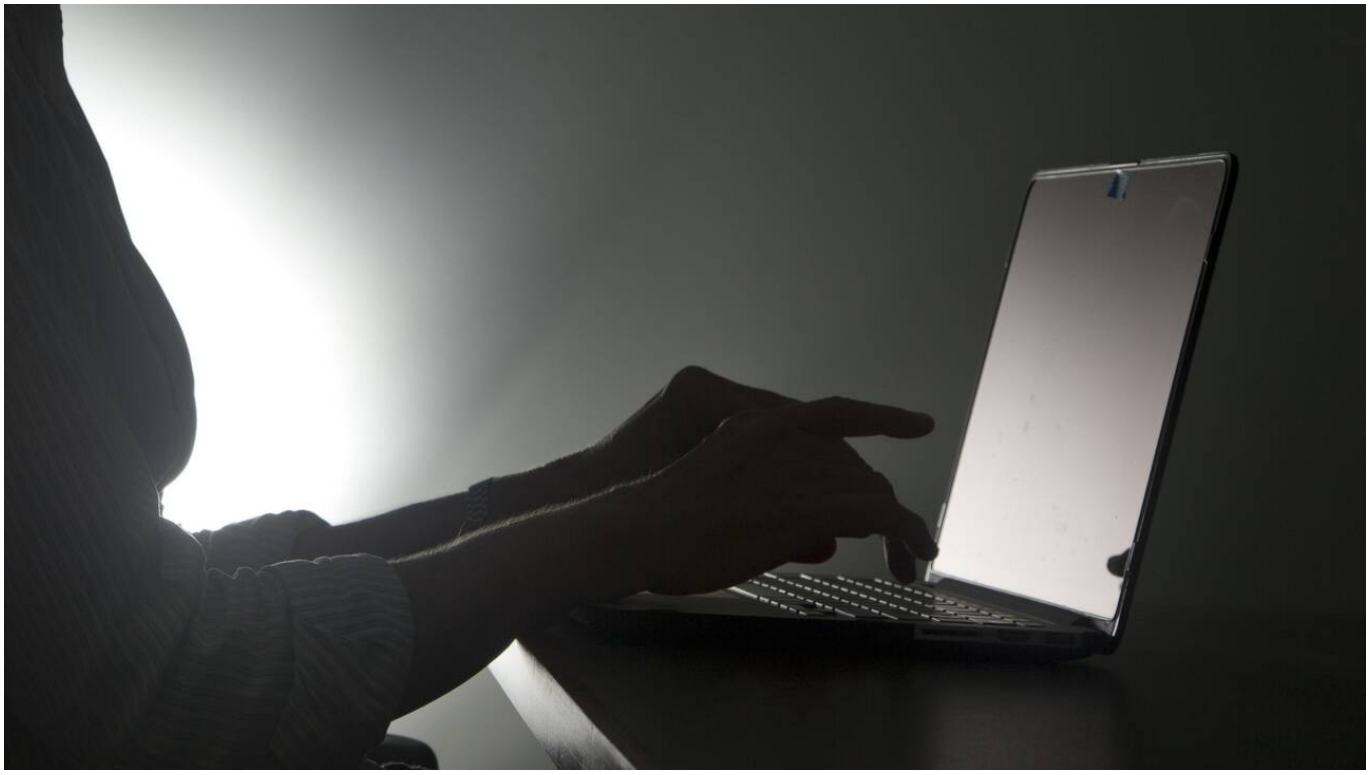
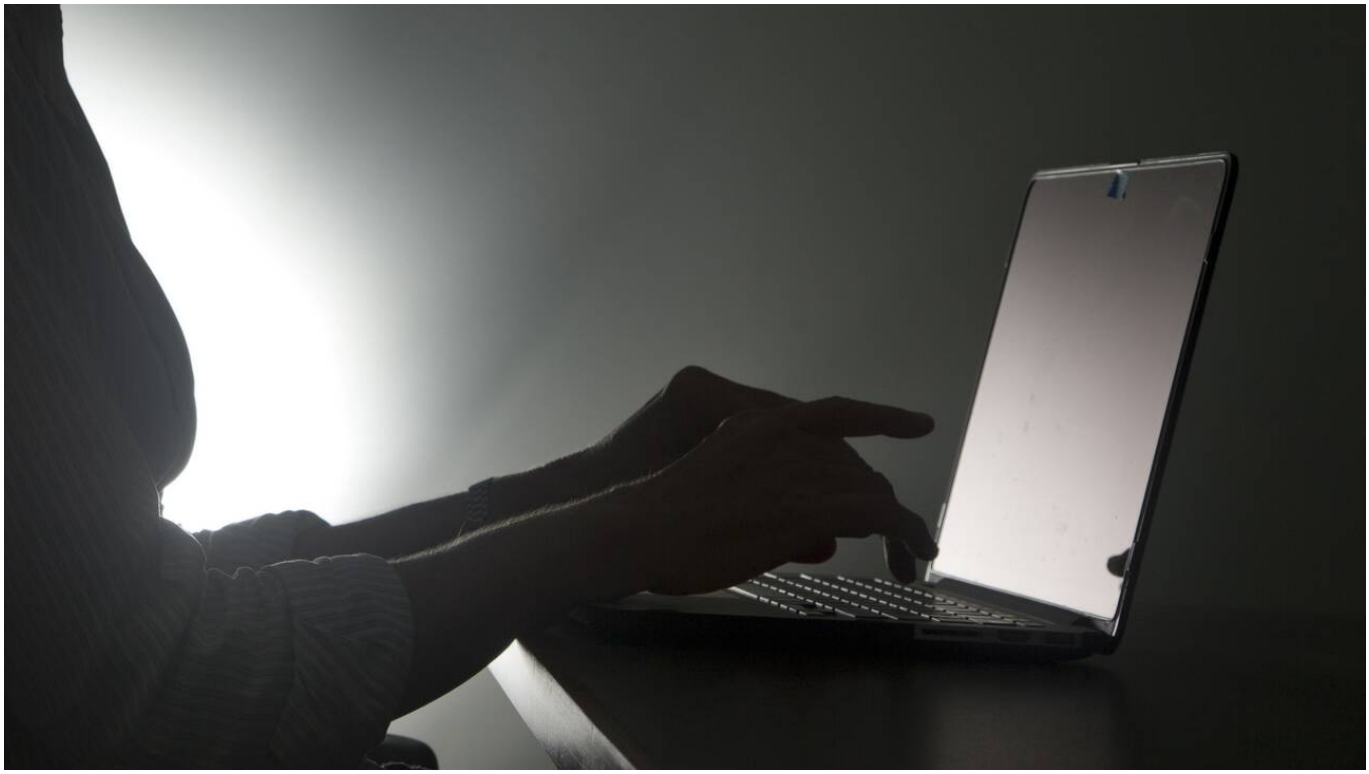
17 Σεπτεμβρίου 2020

Τι πρέπει να κάνουν οι επιχειρήσεις για την ασφάλεια τους από κυβερνοεπιθέσεις

/ Επιστήμες, Τέχνες & Πολιτισμός



Μία σειρά από προτεινόμενες ενέργειες και βασικές κατευθύνσεις για την αποτελεσματική προστασία των πληροφοριακών συστημάτων των ελληνικών επιχειρήσεων από κυβερνοεπιθέσεις, έδωσε στη δημοσιότητα η Εθνική Αρχή Κυβερνοασφάλειας.



Όπως επισημαίνεται στη σχετική ανακοίνωση, τα μέτρα αυτά ένα σύνολο ενεργειών που ονομάζεται ψηφιακή «άμυνα-σε-βάθος» (defense-in-depth) και περιλαμβάνουν καλές πρακτικές για τον περιορισμό και την αντιμετώπιση των πιο κοινών τύπων επιθέσεων στα συστήματα, τις εφαρμογές και το δίκτυο.

Όσον αφορά τις προτεινόμενες οδηγίες είναι οι εξής:

1- Αναπτύξτε πολιτικές ασφάλειας, κατευθυντήριες οδηγίες και διαδικασίες για την προστασία των πληροφοριακών αγαθών και των σχετικών συστημάτων, οι οποίες να επεκτείνονται και σε προμηθευτές υπηρεσιών και αγαθών, καθώς και σε παρόχους υπηρεσιών νέφους (cloud).

2- Χρησιμοποιείτε κατάλληλα παραμετροποιημένο και ενημερωμένο λογισμικό προστασίας από κακόβουλο κώδικα (anti-malware software) με κεντρική διαχείριση. Επίσης, να υφίσταται σχέδιο (patch management) για την προγραμματισμένη εγκατάσταση των ενημερώσεων ασφάλειας (security updates) στα λειτουργικά συστήματα και τις εφαρμογές.

3- Διαχείριση λογαριασμών και έλεγχος πρόσβασης:

i) Η πρόσβαση σε πληροφορίες και συστήματα θα πρέπει να γίνεται βάσει ρόλων και καθηκόντων, σύμφωνα με την προσέγγιση “need-to-know-basis” και “least privilege”.

ii) Η χρήση των λογαριασμών διαχείρισης θα πρέπει να γίνεται αποκλειστικά για διαχειριστικές εργασίες. Ανάλογα με την κρισιμότητα των δεδομένων και των συστημάτων, συστήνονται επιπλέον μέτρα, όπως π.χ. η χρήση υπολογιστών αποκλειστικά για διαχείριση, καθώς και η αυθεντικοποίηση δύο παραγόντων (two-factor-authentication).

iii) Χρησιμοποιείστε ισχυρούς κωδικούς πρόσβασης (strong passwords). Συνιστάται οι κωδικοί πρέπει να έχουν μήκος τουλάχιστον 10 χαρακτήρων με συνδυασμό κεφαλαίων, μικρών, ειδικών χαρακτήρων και αριθμών.

iv) Τηρείτε αρχεία καταγραφής (log files) στο δίκτυο, στους servers, στα λειτουργικά συστήματα και τις εφαρμογές, τα οποία θα ελέγχονται τακτικά για ανίχνευση επιθέσεων και προσπαθειών παραβίασης των συστημάτων.

4- Υλοποιήστε πολυεπίπεδη άμυνα:

i) Στην εξωτερική περίμετρο με τη χρήση firewalls, IDS (Intrusion Detection Systems), IPS (Intrusion Prevention Systems), access control lists κ.α..

ii) Εσωτερικά με την τμηματοποίση του δικτύου (είτε με φυσικό τρόπο είτε με εικονικό τρόπο [virtual lans]) και την υλοποίηση κανόνων πρόσβασης (σε χρήστες και συσκευές) και περιορισμού δικαιωμάτων, καθώς και τη δημιουργία DMZ.

5- Υλοποιήστε σε τακτική βάση προγράμματα ευαισθητοποίησης του προσωπικού και διαμόρφωσης κουλτούρας ασφάλειας (security awareness training). Η συντριπτική πλειοψηφία των σύγχρονων κυβερνοεπιθέσεων ξεκινά με επιθέσεις κοινωνικής μηχανικής (π.χ. phishing email, spam).

6- Η απομακρυσμένη πρόσβαση (remote access) στα συστήματα του Οργανισμού θα πρέπει να γίνεται με τη χρήση VPN με ισχυρή κρυπτογράφηση, καθώς και χρήση αυθεντικοποίησης 2 παραγόντων (two-factor-authentication).

7- Αναπτύξτε ένα σχέδιο αντιμετώπισης περιστατικών (incidence response plan), το οποίο θα περιλαμβάνει σαφείς ρόλους και ενέργειες και θα δοκιμάζεται σε περιοδική βάση.

8- Θα πρέπει να τηρείτε τακτικά αντίγραφα ασφαλείας (backup) των δεδομένων σας, διασφαλίζοντας την αποτελεσματική ανάκτησή τους (recovery) σε περίπτωση απώλειας. Επίσης, τα αντίγραφα ασφαλείας των κρίσιμων και ευαίσθητων δεδομένων θα πρέπει να αποθηκεύονται με ασφαλή τρόπο και περιορισμό πρόσβασης.

9- Εφαρμόζετε μηχανισμούς κρυπτογράφησης στα κρίσιμα και προσωπικά δεδομένα που τηρούνται στον Οργανισμό, προκειμένου να εξασφαλίζεται η εμπιστευτικότητα και η ιδιωτικότητά τους σε όλα τα στάδια του κύκλου ζωής τους.

10- Εφαρμόζετε μέτρα προστασίας και ανάκαμψης από φυσικές και περιβαλλοντικές απειλές (διαταραχή ηλεκτροδότησης, πλημμύρες, πυρκαγιές κ.λπ.).

Η Εθνική Αρχή Κυβερνοασφάλειας επισημαίνει ακόμη ότι η ασφάλεια των πληροφοριακών και τηλεπικοινωνιακών υποδομών είναι μια διαρκής διαδικασία και καλεί τόσο τις επιχειρήσεις όσο και τους πολίτες να διατηρούν ενημερωμένο τον εξοπλισμό τους (υπολογιστές, smartphones, tablets, routers κ.τ.λ.) με βάση τις οδηγίες των κατασκευαστών και να εμπιστεύονται μόνο αξιόπιστες πηγές πληροφόρησης για την ενημέρωσή τους σε θέματα προστασίας.

Πηγή: cnn.gr