Άρθρο
27-01-2022 - 15:13
20211111ST017184

Ευρωπαϊκό Κοινοβούλιο

Πώς θέλει το ΕΚ να ενισχύσει την κυβερνοασφάλεια στην ΕΕ; (συνέντευξη)

Συνέντευξη με τον ευρωβουλευτή Μπαρτ Γκρότχαϊς

Οι ευρωβουλευτές θέλουν να προστατεύσουν τους πολίτες και τις επιχειρήσεις από τις αυξανόμενες κυβερνοαπειλές. Μάθετε περισσότερα στη συνέντευξη με τον ευρωβουλευτή Μπαρτ Γκρότχαϊς.

Τα δίκτυα και τα πληροφοριακά συστήματα αποκτούν όλο και πιο κεντρικό ρόλο στην καθημερινότητά μας, με αποτέλεσμα να αυξάνονται οι απειλές στον κυβερνοχώρο. Οι απειλές αυτές μπορούν να προκαλέσουν οικονομικές καταστροφές, ακόμα και να διαταράξουν τα δίκτυα παροχής νερού και ηλεκτρικού ρεύματος ή τη λειτουργία των νοσοκομείων. Η αποτελεσματική κυβερνοασφάλεια είναι σημαντική για την προστασία των πολιτών, την υλοποίηση του ψηφιακού μετασχηματισμού και την πλήρη αξιοποίηση

Γενική Διεύθυνση Επικοινωνίας
Ευρωπαϊκό Κοινοβούλιο - Εκπρόσωπος Τύπου: Jaume Duch Guillot
Επικοινωνία: webmaster@europarl.eu

των οικονομικών, κοινωνικών και βιώσιμων οφελών της ψηφιοποίησης.

Μάθετε περισσότερα για τη σημασία της κυβερνοασφάλειας στην ΕΕ.

Στις 11 Νοεμβρίου, το Κοινοβούλιο υιοθέτησε τη διαπραγματευτική του θέση για την αναθεώρηση της Οδηγίας για την ασφάλεια δικτύου και πληροφοριών. Ο εισηγητής εξηγεί τις θέσεις του Κοινοβουλίου στη συνέντευξη που ακολουθεί.

Τι είναι το ransomware;

- Είδος κακόβουλου λογισμικού που μολύνει τα πληροφοριακά συστήματα, εμποδίζοντας το θύμα να χρησιμοποιήσει το σύστημα και τα δεδομένα που έχει αποθηκεύσει.
- Ο χρήστης συνήθως λαμβάνει ένα εκβιαστικό μήνυμα που του ζητάει να πληρώσει λύτρα για να ανακτήσει τη δυνατότητα πρόσβασης.

Ποιες είναι οι σημαντικότερες απειλές για την ασφάλεια στον κυβερνοχώρο;

Το ransomware είναι οπωσδήποτε η μεγαλύτερη απειλή. Τα περιστατικά ransomware τριπλασιάστηκαν παγκοσμίως το 2020 και φέτος αναμένουμε ακόμα περισσότερα. Πριν από δέκα χρόνια τα λογισμικά ransomware στόχευαν μεμονωμένα άτομα. Κάποιος έπρεπε να πληρώσει 100 ευρώ ή 200 ευρώ στον χάκερ. Σήμερα, η μέση πληρωμή ανέρχεται στα 140.000 ευρώ. Επίθεση δέχονται όχι μόνο οι μεγάλες εταιρείες αλλά και οι μικρές επιχειρήσεις που αναγκάζονται να πληρώσουν τα λύτρα γιατί αλλιώς δεν μπορούν να λειτουργήσουν. Αποτελεί επίσης εργαλείο εξωτερικής πολιτικής για κακοποιά καθεστώτα.

Διαβάστε περισσότερα για τις κύριες και αναδυόμενες απειλές κατά της κυβερνοασφάλειας.

Πώς η πανδημία του ransomware επηρεάζει τη ζωή ενός πολίτη ή μιας εταιρείας;

Παρατηρούμε ότι το ransomware στοχεύει σχεδόν οτιδήποτε προσφέρει υπηρεσίες στους πολίτες. Μπορεί αυτό να είναι ένας δήμος, ένα νοσοκομείο, ένας τοπικός παραγωγός. Το Κοινοβούλιο και το Συμβούλιο επεξεργάζονται νομοθεσία για την κυβερνοασφάλεια με στόχο την καλύτερη προστασία από τους χάκερ. Οι ευρωπαϊκές εταιρείες που παρέχουν βασικές ή σημαντικές υπηρεσίες θα πρέπει να λάβουν μέτρα για την ασφάλεια στον κυβερνοχώρο και οι κυβερνήσεις θα πρέπει να βοηθήσουν αυτές τις εταιρείες και να ανταλλάσσουν πληροφορίες, τόσο με τις εν λόγω εταιρείες όσο και με άλλες κυβερνήσεις.

Τι ζητά το Κοινοβούλιο ;

Το Κοινοβούλιο επιθυμεί τη θέσπιση μιας πιο φιλόδοξης νομοθεσίας. Το πεδίο εφαρμογής πρέπει να είναι ευρύτερο, να προστατεύει και να βοηθά τις εταιρείες που παρέχουν υπηρεσίες ζωτικής σημασίας. Η Ευρώπη πρέπει να είναι ένας τόπος ασφαλούς διαβίωσης και επιχειρηματικής δραστηριότητας. Και δεν πρέπει να περιμένουμε άλλο. Η νέα νομοθεσία πρέπει να θεσπιστεί άμεσα.

Γιατί είναι σημαντικό να δράσουμε άμεσα ;

Όταν πρόκειται για κυβερνοασφάλεια, πρέπει να βεβαιωθείς ότι δεν είσαι ο πιο αδύναμος. Οι ευρωπαϊκές εταιρίες ήδη επενδύουν 41% λιγότερο από ό,τι επενδύουν οι εταιρίες στις ΗΠΑ. Οι ΗΠΑ κινούνται γρήγορα. Ο Μπάιντεν αυτή τη στιγμή θεσπίζει νομοθεσία έκτακτης ανάγκης και δεν πρέπει να επιτρέψουμε να γίνει η Ευρώπη πιο ελκυστική για τους ransomware χάκερς σε σύγκριση με άλλα μέρη του κόσμου. Οι επενδύσεις στην κυβερνοασφάλεια πρέπει να γίνουν τώρα.

Δεύτερον, υπάρχουν προβλήματα στην κυβερνοασφάλεια που χρειάζεται να επιλυθούν άμεσα. Οι επαγγελματίες του χώρου έχουν συχνά ανησυχίες όσον αφορά την προστασία της ιδιωτικής ζωής. Μπορούν ή δεν μπορούν να μοιράζονται δεδομένα που αφορούν την κυβερνοασφάλεια; Θα πρέπει να έχουμε ισχυρή νομική βάση για την ανταλλαγή δεδομένων που συμβάλλουν στην πρόληψη κυβερνοεπιθέσεων.

Τι προκλήσεις μπορεί να αντιμετωπίσει το Κοινοβούλιο κατά τη διάρκεια των διαπραγματεύσεων ;

Θα υπάρξει συζήτηση σχετικά με το εύρος του πεδίου εφαρμογής: ποιες οντότητες θα πρέπει να συμπεριληφθούν; Θα πρέπει επίσης να συζητήσουμε το διοικητικό κόστος για τις εταιρείες. Το Κοινοβούλιο πιστεύει ότι η νομοθεσία πρέπει να προστατεύει τις εταιρείες αλλά ταυτόχρονα να είναι πρακτική και εφικτή. Τι μπορούμε να ζητήσουμε μέσα σε λογικά πλαίσια;

Ένα άλλο ζήτημα αφορά τον πυρήνα του διαδικτύου: την υπηρεσία ονομάτων τομέα (domain name service). Η Ευρωπαϊκή Επιτροπή και το Συμβούλιο θέλουν να το εντάξουν στο πεδίο εφαρμογής των κανόνων και να το ρυθμίσουν. Δεν συμφωνώ όμως καθόλου με αυτό γιατί η Ρωσία και η Κίνα θα θελήσουν να κάνουν το ίδιο - πρέπει να διατηρήσουμε τον πυρήνα ελεύθερο και προσβάσιμο και να διατηρήσουμε το πολυσυμμετοχικό μας μοντέλο.

Γιατί είναι σημαντικό να υπάρχουν κοινοί κανόνες για την κυβερνοασφάλεια σε όλες τις χώρες της ΕΕ;

Η λειτουργία της εσωτερικής αγοράς αποτελεί τη βάση αυτής της νομοθεσίας. Δε θα πρέπει να έχει σημασία αν δραστηριοποιείσαι στη Σλοβακία, στη Γερμανία ή στην Ολλανδία. Πρέπει να υπάρχει ένα κοινό επίπεδο απαιτήσεων για την ασφάλεια στον κυβερνοχώρο και κάθε χώρα πρέπει να διαθέτει τις κατάλληλες υποδομές για αυτόν τον σκοπό. Οφείλουμε να εναρμονίσουμε τους κανόνες και να διασφαλίσουμε τις ζωές των πολιτών.

Η παραπάνω συνέντευξη διεξήχθη πριν την υιοθέτηση της οδηγίας για την ασφάλεια δικτύου και πληροφοριών (NIS2) από το Κοινοβούλιο, τον Νοέμβριο του 2022.

Μάθετε περισσότερα

Κυβερνοασφάλεια: Οι ευρωβουλευτές ενισχύουν τις απαιτήσεις σε επίπεδο ΕΕ (28/10/2021)
Νομοθετική διαδικασία
Νομοθετική αμαξοστοιχία

Υπηρεσία έρευνας του ΕΚ
Ευρωπαϊκή Επιτροπή
Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (Enisa): Ransomware (ορισμός)