Καταπολέμηση των απειλών του κυβερνοχώρου, κάλυψη των κενών. Ο Οργανισμός της ΕΕ δημοσιεύει έκθεση σχετικά με την προδραστική ανίχνευση συμβάντων κυβερνοασφάλειας ώστε να καταστεί αποτελεσματικότερη η «ψηφιακή δύναμη πυρόσβεσης»

Ο Οργανισμός δημοσιεύει σήμερα έκθεση στην οποία προσδιορίζονται 16 ελλείψεις όσον αφορά την ανίχνευση των συμβάντων που αφορούν την ασφάλεια των δικτύων. Στην έκθεση αποκαλύπτεται ότι οι «ψηφιακές δυνάμεις πυρόσβεσης», δηλαδή οι ομάδες αντιμετώπισης εκτάκτων αναγκών στην πληροφορική (CERT), δεν κάνουν επαρκώς ευρεία χρήση όλων των διαθέσιμων εργαλείων για την αποτελεσματική καταπολέμηση των απειλών του κυβερνοχώρου. Ως εκ τούτου, ο Οργανισμός εκδίδει 35 συστάσεις προς τους παρόχους δεδομένων, τους καταναλωτές δεδομένων, καθώς και σε επίπεδο ΕΕ/εθνικό επίπεδο, με σκοπό τον περιορισμό των ελλείψεων.

Στη μελέτη διαπιστώνεται ότι οι CERT δεν αξιοποιούν επί του παρόντος κάθε δυνατή εξωτερική πηγή πληροφοριών που έχουν στη διάθεσή τους. Παρομοίως, πολλές CERT ούτε συλλέγουν, ούτε κοινοποιούν σε άλλες CERT δεδομένα σχετικά με συμβάντα που αφορούν άλλες περιοχές. Αυτό είναι ανησυχητικό, δεδομένου ότι η ανταλλαγή πληροφοριών συμβάλλει ουσιαστικά στην αποτελεσματική καταπολέμηση του κακόβουλου λογισμικού και των κακόβουλων δραστηριοτήτων, η οποία είναι εξαιρετικά σημαντική για την καταπολέμηση των διασυνοριακών απειλών του κυβερνοχώρου.

Ελλείψεις. Οι 16 ελλείψεις όσον αφορά την ανίχνευση συμβάντων εξετάζονται σε βάθος. Στα σημαντικότερα τεχνικά κενά περιλαμβάνονται η ανεπαρκής ποιότητα των δεδομένων (ψευδή θετικά αποτελέσματα στα παρεχόμενα δεδομένα, παροχή ανεπίκαιρων δεδομένων), έλλειψη πρότυπων μορφότυπων, εργαλείων, πόρων και δεξιοτήτων. Το σημαντικότερο νομικό πρόβλημα αφορά κανονισμούς περί απορρήτου και νόμους περί προστασίας δεδομένων προσωπικού χαρακτήρα που παρεμποδίζουν την ανταλλαγή πληροφοριών.

«*Οι διευθυντές των εθνικών/κρατικών CERT θα πρέπει να αξιοποιήσουν την έκθεση για να υπερβούν τις προσδιορισθείσες ελλείψεις, χρησιμοποιώντας περισσότερες εξωτερικές πηγές πληροφοριών που αφορούν συμβάντα καθώς και πρόσθετα εσωτερικά εργαλεία για τη συλλογή πληροφοριών με σκοπό την κάλυψη των κενών*» δηλώνει ο εκτελεστικός διευθυντής του Οργανισμού, καθηγητής Udo Helmbrecht.

35 συστάσεις για τον περιορισμό των ελλείψεων. Όσον αφορά τους παρόχους δεδομένων, οι βασικές συστάσεις επικεντρώνονται στον τρόπο βελτίωσης της πρόσβασης στις CERT, στη βελτίωση του μορφότυπου των δεδομένων, στη διανομή καθώς και στη βελτίωση της ποιότητας των δεδομένων. **Όσον αφορά τους καταναλωτές δεδομένων,**

περιλαμβάνονται συστάσεις σχετικά με την εκτέλεση πρόσθετων δραστηριοτήτων από τις CERT με σκοπό την επαλήθευση της ποιότητας των ροών δεδομένων, ενώ προτείνονται και συγκεκριμένοι τρόποι χρήσης νέων τεχνολογιών. Τέλος, **σε επίπεδο ΕΕ ή σε εθνικό επίπεδο,** είναι αναγκαία η εξισορρόπηση των αναγκών προστασίας του απορρήτου και της ασφάλειας, καθώς και η διευκόλυνση της θέσπισης κοινών μορφότυπων, η ενοποίηση των στατιστικών δεδομένων συμβάντων και η έρευνα για τις διαδικασίες αναφοράς διαρροής δεδομένων.

Πληροφοριακά στοιχεία: Προδραστική ανίχνευση συμβάντων είναι η ανακάλυψη κακόβουλης δραστηριότητας πριν από τη λήψη των σχετικών καταγγελιών και αναφορών συμβάντων. Ως τέτοια, αποτελεί ακρογωνιαίο λίθο για τη δημιουργία ενός αποτελεσματικού χαρτοφυλακίου υπηρεσιών CERT. Μπορεί να ενισχύσει σημαντικά την αποδοτικότητα της λειτουργίας των CERT, και συνεπώς ενισχύοντας, κατά συνέπεια, την ικανότητά της χειρισμού συμβάντων, η οποία είναι μία από τις βασικές υπηρεσίες των εθνικών/κυβερνητικών CERT.

Για την πλήρη έκθεση

Πληροφοριακά στοιχεία:Ψηφιακό

Για συνεντεύξεις: Ulf Bergstrom, εκπρόσωπος τύπου, ENISA, press@enisa.europa.eu, Κινητό: +30-6948-460-143 ή Agris Belasovs, ή Andrea Dufkova, CERT-Relations@enisa.europa.eu

Μετάφραση. Η έκδοση στην αγγλική γλώσσα είναι η μόνη έγκυρη.