19/01/2015

Νέος Οδηγός από τον ENISA: Αξιοποιήσιμες πληροφορίες για την αντιμετώπιση των περιστατικών ασφάλειας

EPR03/2015

www.enisa.europa.eu

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) δημοσιεύει έναν οδηγό ορθής πρακτικής σχετικά με τις Αξιοποιήσιμες πληροφορίες για την αντιμετώπιση των περιστατικών ασφάλειας, επιδιώκοντας να δώσει μια εικόνα των προκλήσεων που τίθενται στις εθνικές Ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) και σε άλλους οργανισμούς ασφάλειας, στην προσπάθειά τους να παραγάγουν αξιοποιήσιμα στοιχεία από μεγάλες ποσότητες δεδομένων.

Η μελέτη προβαίνει σε ευρεία επισκόπηση του υφιστάμενου τοπίου ανταλλαγής πληροφοριών στο πλαίσιο της παραγωγής αξιοποιήσιμων πληροφοριών, προσδιορίζει τα υπάρχοντα εργαλεία και πρότυπα, αναφέρει τις ορθές πρακτικές και τα κενά, ενώ παρέχει συστάσεις για βελτίωση.

Το κύριο μέρος της έκθεσης περιγράφει τον τρόπο που οι αξιοποιήσιμες πληροφορίες αποκτώνται, χρησιμοποιούνται και ανταλλάσσονται με συστηματικό τρόπο. Το προτεινόμενο εννοιολογικό μοντέλο, που αποτελεί το σκελετό της μελέτης, παρουσιάζει ένα γενικευμένο σύστημα επεξεργασίας πληροφοριών με πέντε βήματα: συλλογή, προετοιμασία, αποθήκευση, ανάλυση και διανομή. Σκοπός του μοντέλου είναι να διευκολύνει τον τρόπο που οι CERT χειρίζονται τις πληροφορίες, με στόχο τη βελτιστοποίηση της διαδικασίας αντιμετώπισης των περιστατικών.

Ο Udo Helmbrecht, εκτελεστικός διευθυντής του ENISA, σχολίασε: *«Οι CERT είναι η πρώτη γραμμή της κυβερνοάμυνάς μας. Καθώς η καθημερινή τους εργασία βασίζεται στην επεξεργασία αυξανόμενων ποσοτήτων δεδομένων, η πρόκληση είναι καταλάβουμε τη σημασία τους και να παραγάγουμε αξιοποιήσιμα στοιχεία. Οι αξιοποιήσιμες πληροφορίες θεωρούνται θεμελιώδης δομική μονάδα* για την αντιμετώπιση των περιστατικών. *Αυτή η μελέτη είναι η πρώτη προσπάθεια να παράσχουμε στις CERT έναν οδηγό αναφοράς για το θέμα αυτό. Ο ENISA καλωσορίζει την ευκαιρία υποστήριξης περαιτέρω προσπαθειών στον εν λόγω τομέα, με εκθέσεις, έρευνα και περαιτέρω ανάπτυξη εργαλείων».*

Εξετάζονται τα κενά που συνήθως υπάρχουν στις διαδικασίες χειρισμού των αξιοποιήσιμων πληροφοριών από τις CERT, ενώ παρέχεται επίσης ένα σύνολο γενικών συστάσεων στους οργανισμούς με αρμοδιότητες διάδοσης των πληροφοριών. Το γενικό συμπέρασμα είναι ότι οι ανταλλαγές πληροφοριών δεν έχουν ωριμάσει ακόμα και το περιβάλλον ανταλλαγής θα πρέπει να αναπτυχθεί περαιτέρω για να αξιοποιηθούν πλήρως τα οφέλη αυτών των ανταλλαγών.

Το έργο περιλαμβάνει τρεις μελέτες περιπτώσεων που καλύπτουν διάφορες πτυχές χειρισμού αξιοποιήσιμων πληροφοριών από τις CERT. Αυτά τα σενάρια καταγράφουν τις επιχειρησιακές διαδικασίες αληθινών ομάδων CERT και τα πραγματικά χαρακτηριστικά των χρησιμοποιούμενων εργαλείων, υποδεικνύοντας πώς μπορούν να εφαρμοστούν για να βελτιωθεί η ικανότητα της ομάδας CERT να παράγει, ανταλλάσσει και χρησιμοποιεί αξιοποιήσιμες πληροφορίες.

Κατάλογος για την ανταλλαγή πληροφοριών

Τη μελέτη συμπληρώνει ένας κατάλογος με τίτλο Πρότυπα και εργαλεία για την ανταλλαγή και επεξεργασία αξιοποιήσιμων πληροφοριών που μπορεί να εφαρμοστεί στις δραστηριότητες ανταλλαγής πληροφοριών. Διερευνά τις σχέσεις ανάμεσα στα διάφορα πρότυπα παρέχοντας καλύτερη κατανόηση των βασικών πρωτοκόλλων.

Στο πρώτο μέρος, ο κατάλογος καλύπτει ένα σύνολο πενήντα τριών διαφορετικών προτύπων ανταλλαγής πληροφοριών, ένα μείγμα συχνά χρησιμοποιούμενων μορφών, πρωτοκόλλων, τεχνικών προσεγγίσεων και πλαισίων. Τα παραπάνω χωρίζονται σε επτά κύριες κατηγορίες με βάση το πεδίο εφαρμογής του προτύπου.

Στο δεύτερο μέρος, ο κατάλογος περιλαμβάνει δεκαέξι εργαλεία ανταλλαγής πληροφοριών και πλατφόρμες σχετικές με την ανταλλαγή και την επεξεργασία αξιοποιήσιμων πληροφοριών. Πρόκειται για λύσεις κυρίως ανοιχτής πηγής που είναι στη διάθεση των CERT.

Μια πρακτική άσκηση: χρήση δεικτών για την ενίσχυση των αμυντικών ικανοτήτων - Αξιοποιήσιμες πληροφορίες

Ως μέρος του έργου, δημιουργήθηκε ένα νέο σενάριο πρακτικής άσκησης για την κατάρτιση των μελών των ομάδων αντιμετώπισης περιστατικών και άλλων επαγγελματιών ασφάλειας ΤΠ που είναι υπεύθυνοι για την αντιμετώπισης περιστατικών ασφάλειας.

Στόχος αυτής της άσκησης είναι να διδάξει τον τρόπο δημιουργίας και ανάπτυξης δεικτών παραβίασης με τη χρήση μιας πλατφόρμας Συνεργατικής έρευνας για τις απειλές (CRIT). Επιπλέον, δείχνει πώς μπορούν να αξιοποιηθούν στο μέγιστο οι CRIT ώστε να διακρίνουμε τις σχέσεις ανάμεσα στα διάφορα στοιχεία μιας εκστρατείας, πώς μπορούν να εξαχθούν δείκτες από δεδομένα περιστατικών, να αναπτυχθούν δράσεις μετριασμού και να γίνει παρακολούθηση αυτών των δράσεων. Η άσκηση δημιουργήθηκε για μια πιο δομημένη προσέγγιση της διαχείρισης δεικτών, οδηγώντας τελικά σε καλύτερη προετοιμασία για διασφάλιση των δικτύων.

Για τις πλήρεις εκθέσεις:

- Αξιοποιήσιμες πληροφορίες για την αντιμετώπιση των περιστατικών ασφάλειας
- Πρότυπα και εργαλεία για την ανταλλαγή και επεξεργασία αξιοποιήσιμων πληροφοριών
- Χρήση δεικτών για την ενίσχυση των αμυντικών ικανοτήτων - Αξιοποιήσιμες πληροφορίες

Σημειώσεις προς τους συντάκτες:

https://www.enisa.europa.eu/activities/cert/support/awa

https://www.enisa.europa.eu/activities/cert/support/proactive-detection

Για συνεντεύξεις: Cosmin Ciobanu, Εμπειρογνώμων στην Ασφάλεια δικτύων και πληροφοριών, **Email:** Cosmin.Ciobanu@enisa.europa.eu, **Τηλ.:** (+30) 2814 409663