2013/10/09

EPR12/2013

www.enisa.europa.eu

Ασφάλεια στον κυβερνοχώρο: Λευκή βίβλος του ENISA: Μπορούμε να μάθουμε από τα περιστατικά ασφάλειας κατά των Βιομηχανικών συστημάτων ελέγχου/SCADA

Ο Οργανισμός ENISA της ΕΕ για την ασφάλεια στον κυβερνοχώρο δημοσίευσε σήμερα μια λευκή βίβλο, όπου δίνει συστάσεις σχετικά με την πρόληψη και την ετοιμότητα για μια ευέλικτη και ολοκληρωμένη αντίδραση στις επιθέσεις και τα περιστατικά ασφάλειας στον κυβερνοχώρο κατά των Βιομηχανικών συστημάτων ελέγχου (ICS)/Συστημάτων εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA). Η αύξηση του αριθμού των πρόσφατων περιστατικών ασφάλειας κατά των βιομηχανικών συστημάτων ελέγχου/συστημάτων εποπτικού ελέγχου και απόκτησης δεδομένων (SCADA) εγείρει ερωτήματα αφ' ενός ως προς την ικανότητα πολλών οργανισμών να αντιδράσουν σε κρίσιμα περιστατικά, και αφ' ετέρου ως προς τις αναλυτικές τους ικανότητες. Κατά συνέπεια, ένα ενεργητικό περιβάλλον μάθησης μέσω της εκ των υστέρων ανάλυσης των περιστατικών είναι ιδιαίτερα σημαντικό, υπογραμμίζει ο Οργανισμός.

Τα ICS χρησιμοποιούνται ευρέως για τον έλεγχο βιομηχανικών διαδικασιών κατασκευής, παραγωγής και διανομής προϊόντων. Συχνά χρησιμοποιείται ξεπερασμένο λογισμικό εμπορίου. Γνωστοί τύποι ICS είναι, μεταξύ άλλων, ο εποπτικός έλεγχος και η απόκτηση δεδομένων (SCADA), όπου τα συστήματα SCADA είναι η μεγαλύτερη υποομάδα βιομηχανικών συστημάτων ελέγχου. Τα πρόσφατα περιστατικά ICS/SCADA υπογραμμίζουν τη σημασία της καλής διακυβέρνησης και του ελέγχου των υποδομών SCADA. Ειδικότερα, **η ικανότητα αντίδρασης σε κρίσιμα περιστατικά, καθώς και η ικανότητα ανάλυσης των αποτελεσμάτων μιας επίθεσης, προκειμένου να αντληθούν διδάγματα από τέτοια περιστατικά, είναι ζωτικής σημασίας, υπογραμμίζει ο Οργανισμός.**

Στόχος της εκ των υστέρων ανάλυσης ενός περιστατικού είναι να αποκτηθεί εις βάθος γνώση γι' αυτό. Αυτό σας δίνει τη δυνατότητα να:

- βασιστείτε σε ισχυρά στοιχεία, ώστε να αντιδράσετε στη μεταβαλλόμενη φύση των εσωτερικών και ξένων απειλών·
- διασφαλίσετε ότι συντελείται επαρκής μάθηση, προκειμένου να εγκατασταθούν ανθεκτικά συστήματα.

Εντοπίσαμε τέσσερα βασικά σημεία για ένα ενεργό περιβάλλον μάθησης, που με τη σειρά του θα διασφαλίσει την ταχεία αντίδραση στα περιστατικά στον κυβερνοχώρο και την εκ των υστέρων ανάλυσή τους:

- Συμπλήρωση της υπάρχουσας βάσης δεξιοτήτων με εμπειρογνωμοσύνη στον τομέα της εκ των υστέρων ανάλυσης, και κατανόηση των επικαλύψεων ανάμεσα στις ομάδες αντιμετώπισης κρίσιμων περιστατικών, τόσο υλικής φύσεως όσο και στον κυβερνοχώρο·
- Διευκόλυνση της ενοποίησης των διαδικασιών αντίδρασης στα περιστατικά υλικής φύσεως και στα περιστατικά στον κυβερνοχώρο, με μεγαλύτερη κατανόηση για το πού μπορούν να βρεθούν ψηφιακά στοιχεία και ποιες θα ήταν οι κατάλληλες ενέργειες για τη διατήρησή τους·

- Σχεδιασμός και διαμόρφωση συστημάτων με τρόπο που να επιτρέπει τη διατήρηση ψηφιακών στοιχείων, και
- Αύξηση των διοργανικών και διακρατικών προσπαθειών συνεργασίας.

Ο Καθηγητής Udo Helmbrecht, εκτελεστικός διευθυντής του ENISA, σχολίασε: «Τα συστήματα SCADA είναι συχνά ενσωματωμένα σε τομείς που αποτελούν μέρος της υποδομής ζωτικής σημασίας ενός έθνους, για παράδειγμα στον έλεγχο της διανομής και μεταφοράς της ηλεκτρικής ενέργειας. Αυτό τα καθιστά όλο και ελκυστικότερο δυνητικό στόχο επιθέσεων στον κυβερνοχώρο, από δυσαρεστημένα πρόσωπα που κατέχουν εμπιστευτικές πληροφορίες, έως ομάδες αντιφρονούντων και ξένα κράτη. Τέτοια συστήματα θα πρέπει να λειτουργούν με τρόπο που να επιτρέπει τη συλλογή και την ανάλυση ψηφιακών στοιχείων, για να προσδιορίζεται τι συνέβη όταν παραβιάστηκε η ασφάλεια.

Για την πλήρη έκθεση και συστάσεις, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents

Γενικές πληροφορίες: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Για συνεντεύξεις: Ulf Bergström, Εκπρόσωπος Τύπου: ulf.bergstrom[at]enisa.europa.eu, κινητό: +30 6948 460 143, ή Adrian Pauna, Εμπειρογνώμων, resilience[at]enisa.europa.eu

Μετάφραση. Η έκδοση στην αγγλική γλώσσα είναι η μόνη έγκυρη.
http://www.enisa.europa.eu/media/enisa-in-greek/
www.enisa.europa.eu