2013/12/04

EPR/17/2013

www.enisa.europa.eu

Μετριασμός των επιθέσεων κατά των Βιομηχανικών συστημάτων ελέγχου (ICS) – Ο νέος οδηγός από τον Οργανισμό ENISA της ΕΕ

Ο Οργανισμός ENISA της ΕΕ για την ασφάλεια στον κυβερνοχώρο εκπόνησε ένα νέο εγχειρίδιο για τον καλύτερο μετριασμό των επιθέσεων κατά των Βιομηχανικών συστημάτων ελέγχου (ICS), τα οποία υποστηρίζουν ζωτικές βιομηχανικές διαδικασίες, κατά κύριο λόγο στον τομέα των υποδομών πληροφοριών ζωτικής σημασίας (όπως οι κλάδοι της ενέργειας και της μεταφοράς χημικών ουσιών), όπου συχνά δεν υπάρχει επαρκής γνώση. Καθώς τα ICS συνδέονται πλέον συχνά με τις διαδικτυακές πλατφόρμες, πρέπει να ληφθούν επιπλέον μέτρα ασφάλειας. Αυτός ο νέος οδηγός παρέχει τα απαραίτητα βασικά σημεία που πρέπει να λάβει υπόψη της μια ομάδα που έχει επιφορτιστεί με ικανότητες αντιμετώπισης έκτακτων αναγκών στην πληροφορική σε σχέση με τα ICS (ICS-CERC).

Τα Βιομηχανικά συστήματα ελέγχου (**I**ndustrial **C**ontrol **S**ystems – ICS) είναι απαραίτητα για μια σειρά βιομηχανικών διαδικασιών, μεταξύ των οποίων η διανομή ενέργειας, η επεξεργασία ύδατος, οι μεταφορές, καθώς και χημικές, κυβερνητικές, αμυντικές και διατροφικές διαδικασίες. Τα ICS αποτελούν προσοδοφόρους στόχους για τους παρείσακτους, συμπεριλαμβανομένων εγκληματικών ομάδων, ξένων μυστικών υπηρεσιών, δραστών ηλεκτρονικού «ψαρέματος», αποστολέων ανεπίκλητων μηνυμάτων ή τρομοκρατών. Τα περιστατικά στον κυβερνοχώρο που πλήττουν τα ICS μπορούν να έχουν καταστροφικές συνέπειες στην οικονομία μιας χώρας και στις ζωές των ανθρώπων. Μπορούν να προκαλέσουν μακρόχρονες διακοπές ρεύματος, να παραλύσουν τις συγκοινωνίες και να προκαλέσουν οικολογικές καταστροφές. Ως εκ τούτου, η ικανότητα αντιμετώπισης και μετριασμού των επιπτώσεων των περιστατικών σε σχέση με τα ICS είναι κρίσιμη για την προστασία των υποδομών πληροφοριών ζωτικής σημασίας και για την ενίσχυση της ασφάλειας στον κυβερνοχώρο σε εθνικό, ευρωπαϊκό και παγκόσμιο επίπεδο. Κατά συνέπεια, ο ENISA εκπόνησε αυτόν τον οδηγό σχετικά με τις ορθές πρακτικές πρόληψης και ετοιμότητας για τους φορείς με ICS-CERC, και τονίζει τα ακόλουθα συμπεράσματα:

- Ενώ για τα παραδοσιακά συστήματα ΤΠΕ πρώτη προτεραιότητα είναι η ακεραιότητα, για τα συστήματα ICS, ύψιστη προτεραιότητα (στην κλίμακα «CIA»: Confidentiality, Integrity, Availability – Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) αποτελεί η **διαθεσιμότητα**. Αυτό έχει να κάνει με το γεγονός ότι τα ICS είναι απαραίτητα για την απρόσκοπτη λειτουργία των υποδομών ζωτικής σημασίας.
- Οι κύριοι συντελεστές ICS μερικές φορές δεν έχουν επαρκείς εξειδικευμένες γνώσεις για την ασφάλεια στον κυβερνοχώρο. Παρομοίως, οι καθιερωμένες Ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT) δεν κατανοούν οπωσδήποτε τις τεχνικές πτυχές των ICS συγκεκριμένα στον κάθε τομέα.
- Δεδομένης της δυνητικής σημαντικής ζημιάς στα ICS, η **διαδικασία πρόσληψης** για τις ομάδες ICS-CERC απαιτεί να υποβληθεί το προσωπικό σε εξονυχιστική έρευνα, και πολλά πράγματα πρέπει να ληφθούν υπόψη, για παράδειγμα, η ικανότητα ενός ατόμου να αποδίδει υπό πίεση και η προθυμία του να ανταποκρίνεται εκτός των ωρών εργασίας.

- Πρέπει να αναγνωριστεί η σημασία της **συνεργασίας τόσο στο εσωτερικό μιας χώρας όσο και σε διεθνές επίπεδο**.
- Οι μοναδικές προκλήσεις που τίθενται στις υπηρεσίες ασφάλειας στον κυβερνοχώρο σε σχέση με τα ICS μπορούν να μετριαστούν με τη χρήση **αποδεδειγμένα ορθών πρακτικών για τις CERT**, υφιστάμενων παγκόσμιων και ευρωπαϊκών εμπειριών, και **της καλύτερης ανταλλαγής ορθών πρακτικών**.

Ο Καθηγητής Udo Helmbrecht, εκτελεστικός διευθυντής του ENISA, δήλωσε: «Μέχρι πριν από μερικές δεκαετίες, τα ICS λειτουργούσαν σε διακριτικά, χωριστά περιβάλλοντα, αλλά σήμερα συνδέονται συχνά με το διαδίκτυο. Αυτό δίνει τη δυνατότητα βελτιστοποίησης και αυτοματισμού των βιομηχανικών διαδικασιών, αλλά αυξάνει επίσης τον κίνδυνο έκθεσης σε επιθέσεις στον κυβερνοχώρο».

Για την πλήρη έκθεση: https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems/

Γενικές πληροφορίες: Στρατηγική της ΕΕ για την ασφάλεια στον κυβερνοχώρο. Αυτός ο οδηγός βασίζεται σε προηγούμενο έργο του ENISA στον τομέα των CERT[1]. Αυτός ο οδηγός δεν ορίζει σε ποιες οντότητες των κρατών μελών θα πρέπει να ανατεθούν οι υπηρεσίες ICS-CERC.

Για συνεντεύξεις: Ulf Bergström, Εκπρόσωπος Τύπου: ulf.bergstrom@enisa.europa.eu, κινητό: +30 6948 460 143, ή Andrea Dufkova, Εμπειρογνώμων, [cert-relations [AT]enisa.europa.eu

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

[1] *http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities*