04/12/2013

EPR/17/2013
www.enisa.europa.eu

Verhaltensregeln bei Attacken auf Industrielle Steuerungssysteme (ICS) der neue Leitfaden der EU-Agentur ENISA

Die „Internet-Sicherheits"-Agentur der Europäischen Union, ENISA, hat neue Richtlinien für einen besseren Umgang mit Attacken auf Industrielle Steuerungssysteme (ICS) herausgegeben. Der Leitfaden richtet sich insbesondere an Industrieprozesse innerhalb von IT-Infrastrukturen mit sensiblen Informationen (wie zum Beispiel Energie oder Transport von chemischen Gütern), Bereiche in denen ausreichendes Wissen oft fehlt. Da ICS heutzutage häufig mit dem Internet verbunden sind, müssen zusätzliche Sicherheitsvorkehrungen getroffen werden. Der nun vorliegende Leitfaden bietet Hilfe für Teams welche für ICS-Notsituationen geschult wurden (ICS-CERC).

Industrielle **S**teuerungssysteme (ICS) sind für eine lange Reihe von Industrieprozessen, wie Energieversorgung, Wasseraufbereitung, Beförderung, sowie chemische, staatliche, Verteidigungs- und Nahrungsmittelprozesse unabdingbar. ICS stellen verlockende Ziele für Angriffe von kriminellen Gruppen, Geheimdiensten, Phishern, Spammern oder Terroristen dar. Cyber-Vorfälle, die ICS betreffen, können desaströse Folgen für die Volkswirtschaft eines Landes sowie für die Leben der Bürger haben. ICS-Attacken können zu einem lang andauernden Zusammenbruch der Energieversorgung und einer Totalblockade der Beförderungsmittel führen sowie ökologische Katastrophen nach sich ziehen. Es ist daher von größter Bedeutung, gefährdete Informationssysteme zu schützen und Cyber-Sicherheit auf nationaler, europäischer und internationaler Ebene zu verbessern. Dieses Resultat kann nur erreicht werden, wenn auf ICS-Attacken angemessen reagiert wird und somit die Folgeschäden minimiert werden können. Aus diesen Gründen hat ENISA den Leitfaden über Good Practices für Prävention und Vorbereitung für Körperschaften mit ICS-CERC herausgegeben. ENISA weist auf folgende Schlussfolgerungen hin:

- Integrität ist die wichtigste Komponente von herkömmlichen Informations- und Kommunikationssystemen (IKT), während für Industrielle Steuerungssystem die Verfügbarkeit im Vordergrund steht (ausgehend von der „CIA"-Skala: Confidentiality, Integrity, Availability). Dieser Umstand kann damit erklärt werden, dass ICS für einen reibungslosen Ablauf von kritischer Infrastruktur unverzichtbar ist.
- Die wichtigsten ICS -Akteure verfügen nicht immer über ausreichende Kenntnisse im Bereich der Cyber-Sicherheit. Des Weiteren verstehen CERTs nicht unbedingt sektorspezifische, technische Aspekte der ICS.
- Da der mögliche Schaden durch eine ICS-Attacke substantiell sein kann, sollte der **Rekrutierungsprozess** für ICS-CERC-Experten gründlich durchgeführt werden. Besonderes Augenmerk sollte auf die Belastbarkeit und Bereitschaft auch außerhalb der Arbeitszeiten abrufbar zu sein, geprüft werden.
- Der Stellenwert von **Kooperation auf dem nationalen wie auch internationalen Level** muss anerkannt werden.

- Die einzigartige Herausforderungen von Dienstleistungen im ICS-Cybersicherheitsbereich, können durch identifizierte Good Practices im Bereich CERTs bereits existierende globale und europäische Erfahrungen sowie einen besseren Austausch von Good Practices effizienter gestaltet werden.

Der Geschäftsführer von ENISA, Professor Udo Helmbrecht kommentierte: „Bis vor wenigen Jahrzehnten liefen ICS diskret in einem separaten Umfeld ab, aber heutzutage sind diese Systeme häufig an das Internet angeschlossen. Diese Tatsache ermöglich ein Abgleichen und Automatisieren von Industrieprozessen, aber erhöht auch maßgeblich das Risiko von Cyber-Attacken."
Für den vollständigen Report; https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems/

Hintergrund: EU Cyber Security Strategy. Dieser Leitfaden baut auf früheren ENISA-Arbeiten zu CERTs[1] auf und stellt nicht fest, welchen Körperschaften der Mitgliedsstaaten mit ICS-CERC-Serviceleistungen vertraut werden können.

Für Interviews; Ulf Bergström, Sprecher, ulf.bergstrom@enisa.europa.eu,Mobiltelefon: + 30 6948 460 143, oder Andrea Dufkova, Expertin, [cert-relations [AT]enisa.europa.eu

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.
http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch
www.enisa.europa.eu

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