2021. April, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators, furthermore provides information on vulnerabilities, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you're interested in ICS security, feel free to contact our experts at cara@blackcell.hu.

List of Contents

ICS good practices, recommendations

Four phases for a cybersecurity initiative

Control Engineering published an article in 2019, where introduced a model to improve the industrial cyber security. The model is the following:

Phase 1: Design and framework

Designing a cybersecurity management system is the most comprehensive phase and requires the most investment in time and effort. Many cybersecurity consulting firms are out there focusing on helping companies design cybersecurity infrastructure, policies and procedures. This task includes identifying all systems and personnel linked to cybersecurity, defining their roles, defining their access and control rights, and building policies around these parameters to ensure safe operations. The cybersecurity design phase requires a significant internal push and buy-in from stakeholders to ensure its successful completion.

Black Cell recommendations in this security feed as it can help to understand this phase in depth.

Phase 2: Gap assessment

The assessment phase primarily consists of reviewing the cybersecurity design, and identifying potential vulnerabilities and risks depending on business impact. Identified gaps are addressed and updated in the design. Assessments can be performed using experienced personnel and various tools that sniff the network level packets and identify anomalous behaviour and gaps in system hardening.

Gap assessment is always a hard task, because the comprehensiveness. Identifying all gaps is possible, recommended to use some frameworks, which can help to address this phase (for example: NIST SP 800-82)

Phase 3: Implementation

This part is the actual implementation of cybersecurity policies, procedures and practices. External help at this stage can help speed up the implementation process and ensure all checklists are marked. A key method of implementation is system hardening.

ICS/SCADA professionals needed to accomplish this phase.

Phase 4: Audit

Auditing cybersecurity covers tasks like comprehensive penetration testing to ensure that the cybersecurity implementation is achieving the desired results. Specialized audit companies usually tackle this job and help ensure solid cybersecurity. This part requires the largest amount of external expertise for a new implementation plan. However, if an internal cybersecurity audit team is trained during all phases, that team can use its learning and expertise to audit other plants and facilities within the company.

In audits, it's essential to conduct and follow every steps appropriately.

The source and more information is available on the following link:

https://www.controleng.com/articles/industrial-control-system-ics-cybersecurity-advice-best-practices/

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in May 2021:

SANS provides online ICS security courses. The details of the trainings and courses are available on the following link:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

Periodic online courses:

The Coursera (https://www.coursera.org/) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

- Industrial IoT Markets and Security
- Developing Industrial Internet of Things Specialization

More details can be found on the following website:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

ICS CERT offers the following courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems
- ICS Cybersecurity
- ICS Evaluation

More details can be found on the following website:

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

ICS-CERT Virtual Learning Portal (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours

- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials
  - 17-22. May 2021.
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - anytime, on demand.

More details can be found on the following website:

https://www.sans.org/find-training/search?types=10&coursecode=ICS410,ICS515

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

- ICS/SCADA Cyber Security

More details can be found on the following website:

https://www.udemy.com/ics-scada-cyber-security/

The Department of Homeland Security's two days training is useful for the ICS/SCADA operators:

- SCADA security training

The courses are available live online.

More details can be found on the following website:

https://www.tonex.com/training-courses/scada-security-training/

SCADAhacker-com website provides ICS security online courses:

- Understanding, Assessing and Securing Industrial Control Systems

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP, CEH, the course can help to add some ICS and SCADA specific knowledge.

More details can be found on the following website:

https://scadahacker.com/training.html

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the "Certified SCADA Security Architect" certification for the candidates.

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a 3 Days Course, which is designed for:

- IT and ICS cybersecurity personnel
- Field support personnel and security operators
- Auditors, vendors and team leaders
- Electric utility engineers
- System personnel & System operators
- Independent system operator personnel
- Electric utility personnel involved with ICS security.
- Technicians, operators, and maintenance personnel
- Investors and contractors in electric industry
- Managers, accountants, and executives of electric industry

More details can be found on the following website:

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

ICS conferences

In May 2021, the following ICS/SCADA security conferences and workshops are held (not comprehensive):

CS4CA World: 24Hr Global Cyber Security Conference

As the global pandemic dramatically reshapes society into the new normal and fuels cyber threat workload, critical infrastructure organizations are busy reassessing their cyber risk while striving to maintain business continuity.

The summit offers dedicated sessions, allowing delegates to home in on their specialist areas of interest, as well as topics addressing the issues that bind both IT & OT professionals, with a focus on cyber resilience in a post-covid world.

Online event; 6th May 2021.

More details can be found on the following website:

https://world.cs4ca.com/

Industrial Control Systems (ICS) Security Events

Public Safety Canada organized this conference. The first session was in march, and this is the second session, where the main issues are the following:

- Lessons learned and case studies,
- Security success and fails (Owner/operator and vendor experiences are welcome.)
- Innovations in delivery models

Agenda and registration coming soon; 25-27th May 2021.

More details can be found on the following website:

https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ndstrl-cntrl-sstms/vnts-en.aspx

ICS incidents

Molson Coors suffered a ransomware attack

Molson Coors is a multi-national brewery with many famous beer brands. The company reported a cybersecurity incident, which has caused and may continue to cause a delay or disruption to parts of the Company's business, including its brewery operations, production, and shipments.

Many companies fight against ransomware the past few years, and the number of companies is continuously growing, which has an operational disruption. This case is very similar to the others, and missing the details as a common.

The global DPO said that these attacks illustrate how cyber criminals are targeting high profile organizations to interrupt key business operations and manufacturing.

Supposedly the IT and the OT doesn't separate appropriately, because the ransomware attack affected operations, production, and also shipments. There are many good practices to prevent a ransomware attack, especially the IT and OT separation.

Tony Lambert, intelligence analyst at Red Canary, gave credence to the speculation. "For manufacturing organizations, ransomware poses a major threat to data and system availability. Not only do corporate systems lose access to data, systems managing the manufacturing process may come to a halt as well, preventing the successful production and even delivery of products."

An Italian beverage manufacturer Campari Group was also hit by a ransomware attack in November 2020. This is an alert to these companies, that every firm in this sector is a target.

Sources and more details can be found on the following websites:

https://www.zdnet.com/article/molson-coors-discloses-cyberattack-disrupting-its-brewery-operations/

https://www.securityweek.com/cyberattack-forces-brewery-shutdown-molson-coors

https://www.cpomagazine.com/cyber-security/a-suspected-ransomware-cyber-attack-shuts-down-worlds-fifth-largest-beermaker-molson-coors/

Book recommendation

SCADA security Machine learning concepts for intrusion detection and prevention

This book, published in 2020 is discussing a very hot topic in the field of SCADA security. Machine learning is a possibility to build a resilient operational technology, where the intrusion detection and prevention might be more effective.

The chapters introduce various SCADA security frameworks and approaches, including evaluating security with virtualization-based SCADAVT, using SDAD to extract proximity-based detection, finding a global and efficient anomaly threshold with GATUD, and more. This important book:

- Provides diverse perspectives on establishing an efficient IDS approach that can be implemented in SCADA systems,
- Describes the relationship between main components and three generations of SCADA systems,
- Explains the classification of a SCADA IDS based on its architecture and implementation,
- Surveys the current literature in the field and suggests possible directions for future research.

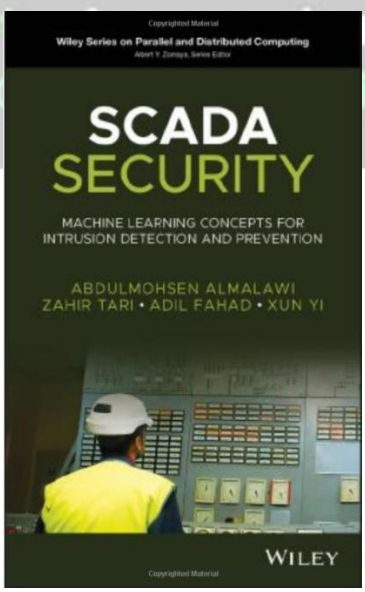
SCADA Security: Machine Learning Concepts for Intrusion Detection and Prevention is a must-read for all SCADA security and networking researchers, engineers, system architects, developers, managers, lecturers, and other SCADA security industry practitioners.

Authors/Editors: Abdulmohsen Almalawi, Zahir Tari, Adil Fahad, Xun Yi

Year of issue: 2020.

The book available at the following link:

https://www.amazon.com/SCADA-Security-Intrusion-Prevention-Distributed/dp/1119606039



Black Cell recommendations

Best Practices in ICS Security for Device Manufacturers

GE released a whitepaper, which is a best practice collection for device manufacturers in ICS security. It is very important to know, that the ICS security is not only an operational responsibility. The device planners, manufacturers, implementors, operators are all involved in the subject.

GE's best practices are focusing on the device manufacturers. The whitepaper mentioned, that 91% of the power generation organizations have experienced a cyberattack. This is a very high percentage of organizations. ICS and SCADA systems are now accessible and becoming high priority targets for hackers.

In order to properly design, develop, and implement strategic best practices for security, it is essential that manufacturers of critical infrastructure understand the organization's current security capabilities and the effect the threat landscape may have on its products. The device manufacturers have to know all of the risks, which are threatening the ICS/SCADA devices.

Regarding the operation and security, the customer expectations are also very important, (these are usually restricting the possibilities to implement the security capabilities), not recommended to ignore these things.

Certification is also very important. If the device manufacturer applies some standards and certified procedures in the phase of device manufacturing, the expected reliability will be higher. Certifications will establish a benchmark for the secure development of the applications, devices, and systems found in critical infrastructure. The certification process presents device manufacturers with an independently verified result to communicate their products' robustness and security to customers while providing control systems operators with complete, accurate, and trustworthy information about the network security and resilience of their deployed products.

The whitepaper describes the importance of rigorous testing and security training of teams. If the organization is following standardized procedures, these two things are essential to be a secure ICS/SCADA device manufacturer.

Device manufacturers for ICS face a dynamic challenge in keeping their devices and their customers' systems secure. The corporate governance and politics are very important. If the corporate culture carries the security attitude within itself, the processes are easier to apply to manufacturing secure devices.

The source and the related article are available at the following link:

https://www.ge.com/digital/sites/default/files/download_assets/best-practices-in-ics-security-for-device-manufacturers-whitepaper.pdf

ICS vulnerabilities

In April 2021 the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

ICSA-21-112-01: **Horner Automation Cscape**
High level vulnerabilities: Improper Input Validation, Improper Access Controls.
https://us-cert.cisa.gov/ics/advisories/icsa-21-112-01

ICSA-21-112-02: **Mitsubishi Electric GOT**
Medium level vulnerability: Improper Authentication.
https://us-cert.cisa.gov/ics/advisories/icsa-21-112-02

ICSA-21-110-01: **Hitachi ABB Power Grids Ellipse APM**
Medium level vulnerability: Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-01

ICSA-21-110-02: **Rockwell Automation Stratix Switches**
High level vulnerabilities: Insufficiently Protected Credentials, Insufficient Verification of Data Authenticity, Use of Out-of-Range Pointer Offset, Insertion of Sensitive Information Into Log File, Command Injection, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-02

ICSA-21-110-03: **Delta Industrial Automation COMMGR**
Critical level vulnerability: Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-03

ICSA-21-110-04: **Delta Electronics CNCSoft ScreenEditor**
High level vulnerability: Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-04

ICSA-21-110-05: **Delta Electronics CNCSoft-B**
High level vulnerabilities: Out-of-bounds Read, Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-05

ICSA-21-110-06: **Eaton Intelligent Power Manager**
High level vulnerabilities: SQL Injection, Eval Injection, Improper Input Validation, Unrestricted Upload of File with Dangerous Type, Code Injection.
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-06

ICSA-21-110-07: **Siemens Mendix**
High level vulnerability: Improper Privilege Management.
https://us-cert.cisa.gov/ics/advisories/icsa-21-110-07

ICSA-21-096-01: **Hitachi ABB Power Grids Multiple Products (Update A)**
High level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-096-01

ICSA-20-161-02: Mitsubishi Electric MELSEC iQ-R Series (Update C)
Medium level vulnerability: Resource Exhaustion.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-02

ICSA-20-070-01: Siemens and PKE SiNVR/SiVMS Video Server (Update A)
High level vulnerabilities: Cleartext Storage in a File or on Disk, Path Traversal, Improper Input Validation, Weak Cryptography for Passwords.
https://us-cert.cisa.gov/ics/advisories/icsa-20-070-01

ICSA-21-105-01: Schneider Electric C-Bus Toolkit
High level vulnerabilities: Improper Privilege Management, Path Traversal.
https://us-cert.cisa.gov/ics/advisories/icsa-21-105-01

ICSA-21-105-02: EIPStackGroup OpENer Ethernet/IP
High level vulnerabilities: Incorrect Conversion Between Numeric Types, Out-of-bounds Read, Reachable Assertion.
https://us-cert.cisa.gov/ics/advisories/icsa-21-105-02

ICSA-21-103-01: Schneider Electric SoMachine Basic
High level vulnerability: Improper Restriction of XML External Entity Reference.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-01

ICSA-21-103-02: Advantech WebAccessSCADA
High level vulnerability: Incorrect Permission Assignment for Critical Resource.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-02

ICSA-21-103-03: JTEKT TOYOPUC products
High level vulnerability: Improper Resource Shutdown or Release.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-03

ICSA-21-103-04: Siemens Nucleus Products DNS Module
High level vulnerabilities: Out-of-bounds Write, Use of Out-of-Range Pointer Offset.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-04

ICSA-21-103-05: Siemens Nucleus Products IPv6 Stack
High level vulnerability: Infinite Loop.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-05

ICSA-21-103-06: Siemens Solid Edge File Parsing
High level vulnerabilities: Out-of-bounds Write, Improper Restriction of XML External Entity Reference, Out-of-bounds Read.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-06

ICSA-21-103-07: Siemens Web Server of SCALANCE X200
Critical level vulnerabilities: Heap-based Buffer Overflow, Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-07

ICSA-21-103-08: Siemens SINEMA Remote Connect Server

High level vulnerabilities: Missing Release of Resource after Effective Lifetime, Infinite Loop.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-08

ICSA-21-103-09: Siemens LOGO! Soft Comfort

Medium level vulnerability: Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-09

ICSA-21-103-10: Siemens and PKE Control Center Server

Critical level vulnerabilities: Cleartext Storage of Sensitive Information in GUI, Improper Authentication, Relative Path Traversal, Use of a Broken or Risky Cryptographic Algorithm, Exposed Dangerous Method or Function, Path Traversal, Cleartext Storage in a File or on Disk, SQL Injection, Cross-site Scripting, Insufficient Logging.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-10

ICSA-21-103-11: Siemens TIM 4R-IE Devices

Critical level vulnerabilities: Incorrect Type Conversion or Cast, Improper Input Validation, Improper Authentication, Security Features, Null Pointer Dereference, Data Processing Errors, Exposure of Sensitive Information to an Unauthorized Actor, Race Condition.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-11

ICSA-21-103-12: Siemens Tecnomatix RobotExpert

High level vulnerability: Out-of-bounds Write.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-12

ICSA-21-103-13: Siemens SIMOTICS CONNECT 400

Medium level vulnerabilities: Improper Null Termination, Out-of-bounds Read, Access of Memory Location After End of Buffer, Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-13

ICSA-21-103-14: Siemens Nucleus DNS

Medium level vulnerability: Use of Insufficiently Random Values.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-14

ICSA-21-103-15: Siemens and Milestone Siveillance Video Open Network Bridge

Critical level vulnerability: Use of Hard-coded Cryptographic Key.
https://us-cert.cisa.gov/ics/advisories/icsa-21-103-15

ICSA-21-068-02: Siemens SCALANCE and RUGGEDCOM Devices SSH (Update A)

High level vulnerability: Improper Restriction of Excessive Authentication Attempts.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-02

ICSA-21-068-03: Siemens SCALANCE and RUGGEDCOM Devices (Update A)

High level vulnerability: Stack-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-068-03

ICSA-20-343-05: Siemens Embedded TCP/IP Stack Vulnerabilities–AMNESIA:33 (Update C)
Medium level vulnerability: Integer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-05

ICSA-20-252-07: Siemens Industrial Products (Update D)
Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07

ICSA-20-196-05: Siemens UMC Stack (Update G)
Medium level vulnerabilities: Unquoted Search Path or Element, Uncontrolled Resource Consumption, Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05

ICSA-20-161-05: Siemens SIMATIC, SINAMICS (Update C)
High level vulnerability: Uncontrolled Search Path Element, Heap-based Buffer Overflow.
https://us-cert.cisa.gov/ics/advisories/icsa-20-161-05

ICSA-20-042-02: Siemens Industrial Products SNMP Vulnerabilities (Update D)
High level vulnerabilities: Data Processing Errors, NULL Pointer Dereference.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-02

ICSA-20-042-07: Siemens SCALANCE X Switches (Update B)
Law level vulnerability: Protection Mechanism Failure.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-07

ICSA-20-042-10: Siemens SCALANCE S-600 (Update B)
High level vulnerabilities: Resource Exhaustion, Cross-site Scripting.
https://us-cert.cisa.gov/ics/advisories/icsa-20-042-10

ICSA-19-344-02: Siemens and PKE SiNVR, SiVMS Video Server (Update A)
Critical level vulnerabilities: Missing Authentication for Critical Function, Weak Cryptography for Passwords.
https://us-cert.cisa.gov/ics/advisories/icsa-19-344-02

ICSA-19-253-03: Siemens Industrial Products (Update L)
High level vulnerabilities: Excessive Data Query Operations in a Large Data Table, Integer Overflow or Wraparound, Uncontrolled Resource Consumption.
https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03

ICSA-15-335-03: Siemens SIMATIC Communication Processor Vulnerability (Update C)
Critical level vulnerability: Authentication Bypass Issues.
https://us-cert.cisa.gov/ics/advisories/ICSA-15-335-03A

ICSA-21-098-01: FATEK Automation WinProladder
High level vulnerability: Integer Underflow.
https://us-cert.cisa.gov/ics/advisories/icsa-21-098-01

ICSMA-19-080-01: **Medtronic Conexus Radio Frequency Telemetry Protocol (Update C)**

Critical level vulnerabilities: Improper Access Control, Cleartext Transmission of Sensitive Information.
https://us-cert.cisa.gov/ics/advisories/ICSMA-19-080-01

ICSA-21-096-01: **Hitachi ABB Power Grids Multiple Products**

High level vulnerability: Improper Input Validation.
https://us-cert.cisa.gov/ics/advisories/icsa-21-096-01

ICSA-21-091-01: **Rockwell Automation FactoryTalk AssetCentre**

Critical level vulnerabilities: OS Command Injection, Deserialization of Untrusted Data, SQL Injection, Improperly Restricted Functions.
https://us-cert.cisa.gov/ics/advisories/icsa-21-091-01

The vulnerability reports contain more detailed information, which can be found on the following website:

https://ics-cert.us-cert.gov/advisories

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

In April 2021, ICS-CERT hasn't published alerts.

The previous alerts can be found at the following link:

https://www.us-cert.gov/ics/alerts