

"Everything's fine today, that is our illusion"

uromarion

-Voltaire

I ODEIO | TEOHEU | #IVOIVEIVE | OOPYHYINI SZUTU IVOKWEII AUUHAUUH, IIIO.

Why should we be concerned with ICS Security?



ICS-Focused Campaigns, Attacks, Frequency



Automation

PUBLIC | TechEd | #ROKLive | Copyright ©2019 Rockwell Automation, Inc.

ICS THREAT ACTORS

> 40% **Cyber Events Nation** Cyber **Criminals** Insiders **States Terrorists Hacktivists** The New Hork Times # WIRED Inside the Cunning, Unprecedented Hack of Ukraine's Power Gr = Q TRANSPORT OF A DECOMPTION NOTION OF ELESCRIBE LOG IN Bits **KrebsonSecurity** SCCYBERCRIME Online Attacks on Infrastructure Are Increasing at a F SECURITY ED.00.10 7:00 eM Reaches APTs/Cyberestriousar Worrying Pace INSIDE THE CUNNING, UNPRECEDENTED HACK OF SHARE 000 C Magazine UK X News X RSA 2017. Researchers create parts moves for industrial control extern f 170 by Max Metzger 26 DHS Warns of 'Hacktivist' Threat Against **UKRAINE'S POWER GRID** 27 V New Olympic 1922 c Magazine US > Cyberolime > Disgra Web System administentenced after staaling BritMin demages Industrial Control Systems February 24, 2017 February 15, 2017 • Disgruntled System admin sentenced after causing The U.S. Department of Homeland Security is warning that a witches brew of recent RSA 2017: Researchers create ransomware for events make it increasingly likely that politically or ideologically motivated hackers may launch \$1.1M in damages industrial control systems digital attacks against industrial control systems. The alert was issued the same day that security researchers published information about an undocumented software backdoor in 00000000 industrial control systems sold by hundreds different manufacturers and widely used in power A disgruntled system administrator was sentenced to 34 months in This article originally appeared on + SC Magazine UK. prison after planting malware which cost his formal employer \$11 plants, military environments and nautical ships. At this week's PSA conference researchers simulated a piece of ransomware taking The information about the backdoor was control of a water treatment plant and poisoning a city's water supply On Feb. 4, 2016 Brian Johnson, 44, of Baton Rouge, La, pleaded published by industrial control systems (ICS) guilty to hacking and willful damage charges after using a VPN The piece of ransomware that works on industrial control systems connection to plant the malware within his former employer's security vendor Digital Bond, which and municipal water supplies is here. Brian Johnson 44 ni Batha Bauga La systems and to alter incustrial controls and to cause material leaded guilty to hapiding and willful detailed how a component used in industrial soplage, according to a DOJ press release. Thankfully, it was created by the safe hands of Georgia institute of damage changes after using a WPA control systems sold by 261 manufacturers presection to skert the melward Technology researchers and the water treatment plant on which it FAILED The events took place in February 2014 after Johnson was contains a functionality that will grant took effect was entirely simulated at this week's RSA conference in terminated from his job at Georgia-Pacific, a pulp and paper company. Not long after Johnson **NFRASTRUCTURF** remote access to anyone who knows the San Francisco established a VPN connection with the company's network to conduct a series of intrusion between proper command syntax and inner workings February 14, 2014 and February 27, 2014 when authorities executed a federal search warrant leading to The custom-built ransomware was created as a proof-of-concept COLUMN ADDA ADD Fren abent ins beräntet is thereiten of the device, leaving systems that are is arrest by the researchers, David Formby, a PhD student in the Seorgia minacting during while long stranding setting 1 connected to the public open to malicious We ards Jech School of Flectrical and Computer Engineering, and Raheem. chrison was sentenced on Feb. 15, 2016 and was ordered to pay back the cost of the damages and it was also p.m. last December 23, and residents of the Beyon, the Motorola Poundation Professor and associate chair in the School of Electrical and Computer tampering. ordered to forfeit a variety of computer devices and accessories used in connection with his prime. Engineering and Formby's faculty advisor Ivano-Frankivsk region of Western Ukraine were preparing



,

ICS Threat Vectors





ICS THREAT VECTORS





What is Risk?

	IEC/TS 62443-1-1			
BSI Stai	TECHNICAL SPECIFICATION	3.12 risk combination of the probability of occurrence of harm and the severity of that harm		
	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models			
		3.2.87 risk expectation of loss expressed as the probability that a particular threat will exploit a par vulnerability with a particular consequence [10]		
NO CONTRACTOR				



Where do we start?



The Approach

Strategic

- Develop an OT cybersecurity program
- Adopt an industry framework
- Understand business drivers and risk tolerances to drive target profiles
- Conduct assessments to develop an understanding of gaps
- Create an improvement plan to drive the tactical approach

Tactical

- Execute on filling gaps as defined and prioritized in the strategic approach
- Utilize validated designs and architectures
- Implement pre-engineered infrastructure and software solutions to achieve targets



Holistic View

A secure application depends on multiple layers of protection and industrial security must be implemented as a system.





OT vs. IT

Priority is on reliability and integrity of the system.

Architectures are of proprietary nature and consist of isolated, task specific systems.

End-points are of heterogeneous make and task specific with long lifespans

Outcomes are physical



Priority is pervasiveness of data and confidentiality of such data.

Architectures are ubiquitous in nature and consist of mutli-tiered systems to encourage wide accessibility

End-points are of homogenous make and multi-purpose with short lifespans

Outcomes are digital



4.0

Compliance & Standards Certified Products, Architectures and Solution Delivery

ISA/IEC 62443: Series of standards that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS).

Applies to those responsible for *designing, manufacturing, implementing, or managing* industrial control systems:

- End-users (i.e. asset owner)
- System integrators
- Security practitioners
- ICS product/systems vendors

*Equivalence to ISO 27001 and NIST Cybersecurity Framework







NIST

Strategic Advisor and Security Practioner

utomation



BUILD A SECURE, ROBUST, FUTURE-READY NETWORK FOR YOUR CONNECTED ENTERPRISE



Trusted Supplier

New Security Capabilities



Secure communications with EtherNet/IP

- Authentication helps prevent unauthorized devices from establishing connections
- **Integrity** helps prevent tampering or modification of communications
- **Confidentiality** helps prevent snooping or disclosure of data

Notable features:

- System management
 - Easily create and deploy security policies to many devices, all at once
- Micro-segmentation
 - Segment your automation application into smaller cell/zones.
- Device-based firewall
 - Enable/disable available ports/protocols of devices (ie./ HTTP/HTTPS)
- Legacy Systems Support
 - Whitelisting authorize specific communications based on IP address
 - Retrofit 1756 based systems with the new 1756-EN4TR
 - Leverage a "proxy device" in front of legacy products (Future)

System Components





Industry-Leading Partners

Complimentary Solutions

Rockwell Automation PartnerNetwork



ROCKWELL AUTOMATION & PARTNER PORTFOLIO

Rockwell Automation	Cisco Wireless, Security, Switching & Routing		Microsoft Operating Systems, Database / Cloud Infrastructure, & Application Security	Layer Network Infrastructure, Zone	VMware Data Center Virtualization	PartnerNetwork™ program Alliances, Encompass™ partner, Distributors, System Integrators, OEMs
------------------------	--	--	--	---------------------------------------	---	--





Thank you

