FIVE MYTHS OF INDUSTRIAL CONTROL SYSTEMS SECURITY

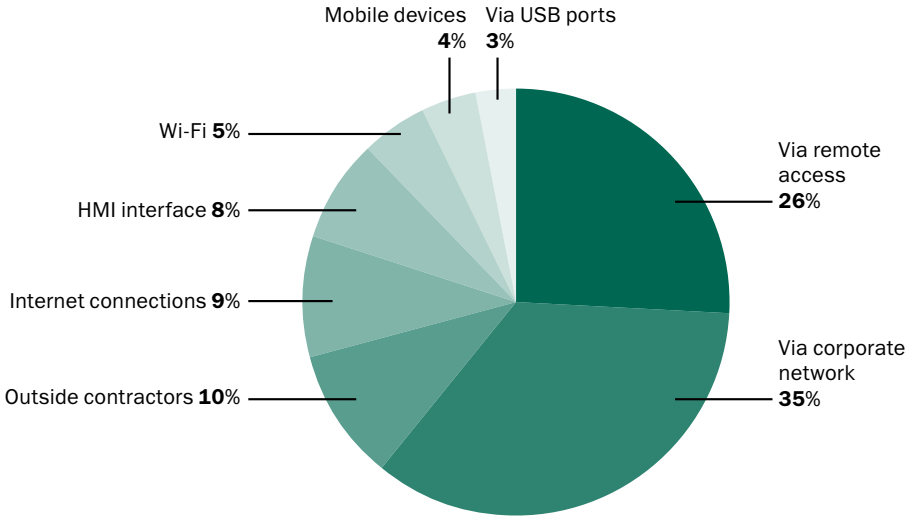
Despite growing awareness of cyber-based attacks on industrial control systems, many IT security models continue to adhere to the outdated belief that physically isolating systems and 'security by obscurity' is enough. It's not. Here's why.

MYTH # 1: **WE'RE NOT CONNECTED TO THE INTERNET**

Bust: The average Industrial Control System (ICS) has 11 direct connections.[1]
Bust: The "Slammer" worm, which affected critical infrastructure as diverse as emergency services, air traffic control and ATMs, achieved its full scanning rate (55 million per second) in under three minutes — thanks to the internet. Ironically, the only thing that slowed it down was a lack of bandwidth on the networks it infiltrated, including:

- Davis-Besse nuclear power plant's process computers and safety display systems were infected via a contractor T1 line, taking its safety monitoring capability offline for five hours.
- The North American Electric Reliability Council found that, of the electrical companies hit by Slammer, one distinct cause was infection via a VPN connection to a remote computer. How was that computer infected? Via the corporate network. The worm propagated, blocking SCADA traffic. [2]
- Harrisburg Water Systems in the US was infiltrated via an infected employee laptop. The cybercriminal used the worker's remote access to infiltrate a SCADA HMI and install malware and spyware.

Sources from which malicious code penetrates industrial networks
(image courtesy of Securityincidents.net)



Bust: An internal survey[3] at a major, representative energy company, found that:

- The majority of business units' management believed control systems were not connected to the business network; an audit showed that 89 per cent of systems were in fact connected.
- Business network security was geared towards general business processes only, with no regard to critical process systems.
- Multiple connection types between the enterprise network and the internet were in place, including intranets, direct internet connection, wireless and dial-up modems.

MYTH # 2: **WE'RE SECURE BECAUSE WE HAVE A FIREWALL**

Bust: A study[4] of 37 firewalls from financial, energy, telecommunications, media and auto companies found that:

- Almost 80 per cent allowed "Any" services on inbound rules as well as unsecured access to the firewalls and demilitarized zone.
- Almost 70 per cent permitted machines outside the network perimeter to access and manage the firewall.

1 Securing Critical Information Infrastructure: Trusted Computing Base: Securelist October 2012
2 The North American Electric Reliability Council : http://www.myitforum.com/articles/15/view.asp?id=5985
3 Paul Dorey, "Security Management in Process Control: the 3 Waves of Adoption", PSCG Spring 2006 Conference, Process Control Security Forum.
4 Avishai Wool, A quantitative study of firewall configuration errors IEEE Computer, 37(6):62-67, 2004

MYTH # 3: **HACKERS DON'T UNDERSTAND SCADA/DCS/PLC**

Bust: SCADA and process control systems are common topics at hacker's "Blackhat" conferences. There's a good reason for it: cybercrime has become very lucrative financially, with zero-day exploits selling to organized crime for as much as $80k per exploit.

- Targeted worms and other exploits are being tailored for specific applications or targets
- Off the shelf SCADA specifications can be bought or readily accessed online
- The Shodan search engine makes it easy to locate unsecured industrial devices and systems globally. Criminals are all-too-aware that, in many instances, these devices are still operating under factory settings, with generic passwords and login details such as "admin" and "1234"
- Project Basecamp, Nessu plug-ins and Metasploit modules help with pen testing — but can also be used for criminal purposes.

MYTH # 4: **OUR FACILITY IS NOT A TARGET**

Bust: You don't have to be a target to become a victim — 80 per cent of control system security incidents were unintentional, but harmful.[5] It's also worth remembering that attacks such as Slammer were aimed at taking down as many systems globally as possible, it didn't have to specifically target energy companies or emergency services to have a significant impact on them.

Kaspersky research shows that many industrial PCs are infected with the same malware afflicting business systems (IT).

Extensive research by Kaspersky Lab, using data from the Kaspersky Security Network (KSN) indicates that many industrial PCs are infected with the same malware afflicting business systems (IT), including (but not limited to) well-known culprits such as Trojans viruses, worms, potentially unwanted and dangerous programs (PUPs) and other exploits targeting vulnerabilities in the Windows operating system.[6]

	IT	SCADA
Trojan	65.45%	43.44%
PUPs	11.17%	37.03%
Worm	7.52%	13.43%
Virus	15.86%	6.10%

MYTH # 5: **OUR SAFETY SYSTEMS WILL PREVENT ANY HARM**

Bust:

- IEC 61508 Certification (SIL) doesn't evaluate security[7]
- Modern SIS are micro-processor-based, programmable systems that are configured with a Windows PC
- It has become commonplace to integrate control and safety systems using Ethernet communication with open insecure protocols (Modbus TCP, OPC.)
- Many SIS communication interface modules run embedded OS and Ethernet stacks that have known vulnerabilities.
- LOGIIC SIS Project (ICSJWG): SIS-ICS integration imposes risks, default configurations are not secure

▶ KASPERSKY KNOWS INDUSTRIAL SECURITY

As an increasing number of malware attacks and cyber incidents demonstrate, the traditional air-gap and perimeter-based approaches to cyber security are no longer enough to protect industrial systems. Protection must also take place inside the perimeter, on the very vulnerable systems and devices that are being targeted.

As a leader in cyber-security, Kaspersky Lab is continually enhancing critical infrastructure protection and industrial security solutions that do more to meet the specific requirements of industrial control systems and the organisations that are tasked with keeping these systems running in process-centric, high availability environments.

In addition to our current, effective cyber security controls, Kaspersky Lab's long-term strategy involves the development of a secure operating system, underlining our vision of providing the ultimate embedded security basement for a variety of devices used in critical infrastructures, including industrial ones.

By establishing close relationships with government organisations and law enforcement agencies globally, as well as helping to educate, advise and inform industrial operators, Kaspersky is playing a leading role in helping industry and regulators anticipate changes in the threat landscape and defend against attacks.

5 The Repository of Industrial Security Incidents, 2013, securityincidents.net
6 Kaspersky Lab: IT Threat Evolution Q1 2013, Securelist May 16 2013
7 ICS JWG 2011 Fall Meeting, https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

DataSheet_ 5Myths_ICS/April14/Global

KASPERSKY lab