

SOFTWARE

Protecting Industrial Networks

Torsten Roessel is director of business development for Innominate Security Technologies AG (Berlin, Germany), a Phoenix Contact company, that develops and markets industrial network security products.

Manufacturing Engineering: How widespread are attacks on industrial networks by hackers?

Torsten Roessel: The number of published security incidents is relatively small. However, roughly 80% of network breaches, directed or undirected, are never reported, because organizations are unable to recognize that their systems were penetrated, or are reluctant to report the breach. Of those breaches that have been investigated or reported, approximately 70% involved deliberate, targeted attacks, and did not require high levels of computer skill. Insider breaches account for some 30% of the total. While targeted hacking attacks attract most of the media attention, accidental infections with malware such as viruses, worms, and Trojans spreading across public and private networks in mostly undirected ways are in fact much more significant, in terms of frequency and number of affected operations.

ME: Describe some recent events in which manufacturing operations were significantly disrupted by hackers.

Roessel: The most famous event, publicized worldwide, occurred in

PASSWORD

“Roughly 80% of network breaches, directed or undirected, are never reported, because organizations are unable to recognize that their systems were penetrated or are reluctant to report the breach.”



Torsten Roessel

2005 when the Zotob worm infected DaimlerChrysler, Caterpillar, General Electric, and more than 175 other corporations. Thirteen US DaimlerChrysler plants had to be shut down, idling their assembly lines and 50,000 workers. Other incidents in the public record are listed in the white paper ‘Hacking the Industrial Network,’ available from Innominate at www.innominate.com. In the first quarter of 2009, a steel producer contacted us after they had to shut down a production line due to infection with the Conficker worm. On April 1, 2009, when this worm had its next wave of activity, I was giving a seminar on industrial Ethernet security during which several attendees in the audience received urgent phone calls because their production networks had

been affected while they were listening to my presentation! And just a few months earlier, a large steel tube manufacturer called for help after having been forced to shut down production due to repeated virus outbreaks infecting a large number of Windows 2000-based automation components.

ME: What industries and/or defense facilities have been hit the most by such attacks?

Roessel: Directed attacks are typically targeted at highly visible utilities or infrastructure and other large corporations. In contrast, undirected malware attacks can affect any type and size of manufacturing business. For example, a leading manufacturer of machine tools now using our mGuard technology had been urged by several of his customers to add a layer of hard-

ening to the company's machine controller and HMI systems. These systems had been infected with malware from within the customer networks, despite standard 'perimeter defense' facilities, such as corporate firewalls being in place. Cyber-crime experts suspect that such traditional perimeter protection against the intrusion of attackers via firewalls at central network access points might be virtually nonexistent today due to millions of 'zombies,' Trojan-type software, unconsciously downloaded to and sleeping undiscovered on user PCs. It may eventually wake up and check on the Internet for their master's command, with outgoing requests that will look like harmless Web browsing to the less-attentive eye.

"Accidental infections with malware are much more significant."

ME: What types of networks are most vulnerable to hackers?

Roessel: Ethernet networks with TCP/IP protocols and Microsoft Windows-based automation components are vulnerable, because their adoption and knowledge about their open technology is widespread. Less known but potentially even more severe are the vulnerabilities of the more proprietary industrial controllers, such as the PLCs and SCADA devices used in manufacturing and process automation today. Most of them lack serious mechanisms for authentication and authorization. They will execute any commands transmitted to them over the network in well-formed and correctly ad-

ressed data packets, without questioning the identity or privileges of the sender. It is only a matter of time until we will see some of these systems fall victim to what Ralph Langner, a well-known German consultant on industrial network security, calls ZCADA, or Zero Control Automated Destructive Attack software.

ME: What kinds of precautions can manufacturing operations take against these attacks?

Roessel: At the organizational level, create awareness for security issues, and educate people on easy-to-follow security policies to reduce the human factor in the operation's vulnerability. Establish a risk management and security-implementation program to identify critical assets with a worthwhile return on security investments (RoSI), and mediate those risks. At the technical level, one has to respect the weaknesses resulting from production systems often containing legacy components. Their processor and memory resources are too limited to install additional security functions. Often, they do not receive regular patches and security fixes, as there is reluctance to update software on a functioning production system. The adage, 'If it ain't broke, don't fix it,' applies here. Besides, such security updates may no longer be available, when components and operating systems remain in use beyond their vendor's support lifecycle. Therefore, our technology was designed with the capability to retrofit security with small external appliances added to a running system without any network reconfiguration, thus shielding groups of critical assets.

ME: What combination of software and network hardware can best thwart hackers?

Roessel: Every industrial IT security specialist will most likely recommend the same approach to improved network security, as do the US National Laboratories, which are dedicated to protecting the national infrastructure. That best-practice approach is called 'defense-in-depth,' and it follows a strategy of distributed layers of defense for individual [groups of] critical assets, such as the components of a manufacturing cell. Ideally, dedicated hardware resources are devoted to these security functions, which control and filter network communication, enforce authentication and authorization schemes, and monitor, defend, or at least restore system integrity after violations have been discovered.

"The adage, 'If it ain't broke, don't fix it,' applies here."

ME: Regarding return on security investments, how expensive have network security incidents been to manufacturers in recent years?

Roessel: Estimates vary, but surveys have shown that \$300,000 is a fair average loss annually for companies whose systems have been breached by viruses, malware, or hackers. Each virus infection is estimated to cost about \$40,000 to clear. The validity of the statistics and information I have provided may be verified by reviewing the 2008 CSI/FBI Computer Crime and Security Survey, the 2008 Verizon Data Breach Investigations Report, and the Idaho National Laboratories white paper, 'Cyber Incidents Involving Control Systems.' Other resources may be found in our company's white paper, 'Hacking the Industrial Network.' ■