March 2012 / Issue 06

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

The Report Card Is In

Verizon's annual report, 2012 Data Breach Investigations Report, cites over 855 data breaches since 2011. Resulting in the compromise of more than 174 million records around the world. The Verizon Data Breach Investigations Report, is a highly respected analysis that includes data from the U.S. Secret Service, four other investigative agencies, and the telecom giant's own vast trove of information. The biggest change this year was the 58 percent rise in hacktivism. Hacktivism probably contributed to the report's finding that 98 percent of all attacks were committed by outsiders. Nearly 70 percent of breaches originated in Eastern Europe. The report also indicates that the percentage of internal attackers has reduced significantly over the last few years, making up only 4 percent of last year's attacks, down from a high of 48 percent in 2009. A number of findings that may surprise you can be seen in the 'What Commonalities Exist' table.

Although no victims are named in the report, two of the biggest breaches in 2011 involving Sony and RSA resulted in the exposure of tens of millions of Records was the result of unpatched software (cyber security best practices). The report again affirms that specialized anti hacking tools and software are not needed. What's needed is more consistent application of the basics. Worse, 85 percent of victims were unaware of the compromise for weeks to months. And when they discovered the breach, 92 percent learned about it from a third party.

Summary of data findings

WHO IS BEHIND DATA BREACHES?
98% stem from external agents
58% tied to Hactivist
4% implicated internal employee
<1% committed by business partner

HOW DO BREACHES OCCUR?
81% utilize some form of hacking
69% incorporated malware
10% involved physical attacks
7% employed social tactics
5% resulted from privilege misuse

WHAT COMMONALITIES EXIST?
97% of breaches avoidable through simple controls
96% of victims of PCI DSS had NOT achieved compliance
96% of attacks were not highly difficult
94% of all data compromised involved servers
92% of incidents were discovered by third parties
85% of breaches took weeks or more to discover
79% of victims were targets of opportunity

Click here for the full Verizon report

NERC-CIP YTD Status

- Total Fines $16,857,793

NERC-CIP 1Q12 Status

- Fines $317,500
- Top 5 CIP Violations
  - CIP-002
  - CIP-004
  - CIP-007
  - CIP-003
  - CIP-006
- 44% of violations are NERC CIP

Industry News

DuQu Mystery Language Solved With Help of Crowdsourcing - *From Threatlevel.com 03/19/2012*

The S/W language origin of the DuQu virus has been solved, thanks to crowdsourcing help from programmers who wrote in to offer suggestions and clues. The language, which DuQu used to communicate with command-and-control servers, turns out to be a special type of C code compiled with the Microsoft Visual Studio Compiler 2008. Researchers at Kaspersky Lab, who put out the call for help two weeks ago after failing to figure out the language on their own, said they received more than 200 comments to a blog post they wrote seeking help, and more than 60 direct emails from programmers and others who made suggestions. DuQu, an espionage tool that followed in the wake of the infamous Stuxnet code, had been analyzed extensively since its discovery last year. But one part of the code remained a mystery – an essential component of the malware that communicates with command-and-control servers and has the ability to download additional payload modules and execute them on infected machines. A reader who led them in the right direction was a commenter who identified himself as Igor Skochinsky and wrote in a thread posted to Reddit.com that he was certain the code was generated with the Microsoft Visual Studio Compiler "programmers who coded this part of DuQu – they were probably ol - school coders, Kaspersky's researchers say.

Dueling legislation over cybersecurity regulations - attacks on U.S. critical infrastructure - *From HomelandSecurityNewsWire.com 03/23/2012*

Attacks on U.S. critical infrastructure may bring about a Katrina-like situation: no electricity, no fresh water, limited traffic control, severely curtailed emergency response, and more; about 85 percent of U.S. critical infrastructure is privately owned; two different cybersecurity bills in Congress envision different solutions to U.S. infrastructure's cyber vulnerability No one doubts that one of the leading concerns in anti-terrorist security is the possibility that terrorists with more advanced computer skills would be able to access the control systems for critical infrastructure components. Consider post-Katrina New Orleans to help visualize the impact of such a cyberattack. No electricity. No fresh water. Limited traffic control, and difficulties in leaving the affected area. Severely curtailed emergency response. There is a legislative conflict, however, regarding what is the best way to prevent and prepare for a cyberattack on U.S. critical infrastructure. There is now a conflict on the Hill between two competing bills, one imposing stringent standards on utilities and infrastructure providers, while the second makes such protection voluntary.

DHS recognizes AWWA security standards - *From AWWA.org 03/05/2012*

Two AWWA utility security standards, J100-10 and G430-09, have been awarded SAFETY Act designation by the U.S. Department of Homeland Security. Under the new designation, utilities in the drinking water and wastewater sector have the assurance of knowing that the standards have been determined by DHS to be effective.

Chemical Industry Calls for Improved Implementation of Chemical Security Program - *From AmericanChemistry.com 03/06/2012*

"Congress and the Administration have an opportunity to build on the chemical industry's initiatives\ to enhance security by improving implementation of the Chemical Facilities Anti-Terrorism Standards (CFATS)." That's according to Timothy Scott, Chief Security Officer and Corporate Director of Emergency Services and Security at The Dow Chemical Company, who testified today on behalf of the American Chemistry Council (ACC) before the House Home and Security Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies.

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
March 2012 / Issue 06

Cyber News

It's True: Compliance Can Be Good for Your Business - *From DarkReading.com 03/01/2012*

Organizations insure their physical assets against loss from fire, theft, and other damage. Most protect their data with a robust backup system. What they most commonly skip is protecting how things get done in the business. Processes and procedures, both technical and operational, are often poorly documented, if documented at all. If key staff becomes unavailable for any reason, it can be very expensive to determine how they did their job and why they did it that way. "Who knows how to restore the backup?" "How do we add a new user to the accounting system?" There are literally thousands of answers to questions like these that go undocumented. Across the range of the various compliance standards, the most common element is thorough, current documentation. After all, no one can assess or confirm compliance without the steps, process, or procedure explained in detail. No auditor will accept "The IT staff said they do this correctly," as verification the process is done, managed, tracked, and verified. Current, useful documentation is the answer, because inevitably the question will be "How?" Documentation explains How: how tasks are performed, how often they are performed, how they are tracked, how they are verified, and a host of other "hows." When done right, this documentation is your operations guide for much of your business.

US Outgunned In Hacker War - *From WSJ.com 03/27/2012*

WASHINGTON—The Federal Bureau of Investigation's top cyber cop offered a grim appraisal of the nation's efforts to keep computer hackers from plundering corporate data networks: "We're not winning," he said. Shawn Henry, who is preparing to leave the FBI after more than two decades with the bureau, said in an interview that the current public and private approach to fending off hackers is "unsustainable.'' Computer criminals are simply too talented and defensive "I don't see how we ever come out of this without changes in technology or changes in behavior, because with the status quo, it's an unsustainable model. Unsustainable in that you never get ahead, never become secure, never have a reasonable expectation of privacy or security,'' Mr. Henry said.

NATO struggles to build effective cyber defense - *From DefenseSystems.com 03/02/2012*

As warfare evolves into the cyber era, the global organization charged with collective Western defense since World War II is finding itself woefully behind on the times, according to a Danger Room. It's a fact the North Atlantic Treat Organization has been quietly acknowledging, including at the conference for defense leadership in Brussels this week. NATO's approach to cyber is barely even in its infancy – there are no guidelines for response to a cyber attack, or even a definition of a cyber Attack.

DoD Networks Completely Compromised, Experts Say - *From blogs.CIO.com 03/22/2012*

The Defense Department's (DoD) computer networks have been totally compromised by foreign spies, according to federal cybersecurity experts. The experts, speaking before the Senate Armed Services Subcommittee on Emerging Threats and Capabilities, say current efforts to protect those networks are misguided at best. Those expert claim that the billions spent by the government on cybersecurity have provided only a limited increase in protection; attackers can penetrate DoD networks; and the defense supply chain and physical systems are at high risk of attack. ' I think we have to go to a model where we assume that the adversary is in our networks. It's on our machines, and we've got to operate anyway. We have to protect the data anyway." The DoD has layered security onto a uniform architecture which only protects against known threats and doesn't adapt to new ones, according to Acting Director of the Defense Advanced Research Projects Agency (DARPA) Kaigham Gabriel.

The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
March 2012 / Issue 06

Invensys Critical Infrastructure and Security Practice (CISP)

Invensys CISP has capability in establishing, implementing, and maintaining industry best practices to meet the demands for government regulations (NERC-CIP, NEI 08-09, CFATS), industry requirements, and company compliance requirements. Attributes of Invensys CISP Consulting include:

Hardware Independence

CISP can work with any type of control system or type of technology a customer prefers for the security environment.

Industry Knowledge

CISP has a number of resources that help them understand the demands of Controls Networks and the requirements for continued uptime.

Regulation Knowledge

CISP has a number of subject matter experts who understand a whole host of regulatory requirements as well as actively participate in a number of industry and government groups.

Proven Methodology

CISP follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the life cycle approach are Assessment, Development, Implementation, and Management.

Technical Knowledge

The same CISP personnel who have regulatory knowledge are also well versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, DCS, and network architecture.

Join us on Blogger

invensys™

For additional information, please visit us at
http://iom.invensys.com/CyberSecurity

5601 Granite Pkwy. Suite 1000 Plano, TX 75024 ▪ P 214.295.6365 ▪ F 888.758.7675 ▪ **iom.invensys.com**