The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

April 2014
Issue 31

this issue

Global Data Breach Investigative Report

From Verizon DBIR

Verizon's recent global Data Breach Investigative Report turns up these interesting facts from 50 contributing global organizations:

- 1,367 confirmed data breaches
- 63,437 security incidents in 95 countries total
- Attackers over the past ten years are able to compromise systems faster than previous years
- Less than 25 percent of companies discover these incidents in a day or less

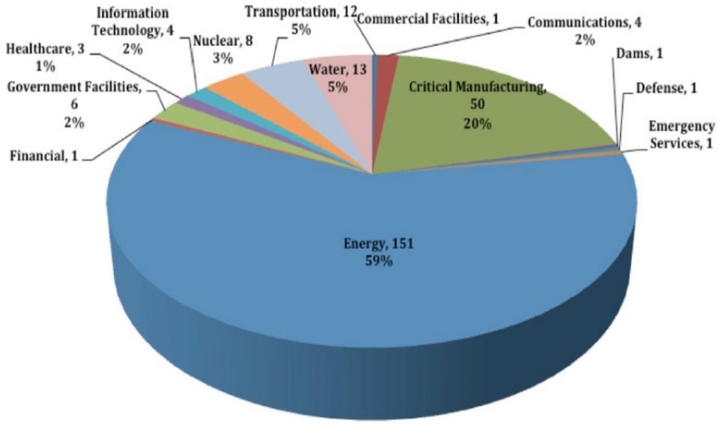
The most pressing threats are web app attacks, cyber espionage, insider misuse/miscellaneous errors, malware, and DDoS.

Cyber Trends from ICS-CERT

Cyber threats are on the rise, with a 91 percent increase in targeted attacks and a 62 percent increase in breaches in 2013, as reported in the Verizon 2014 Security Threat Report. The Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT) reports that for the same period there were 256 reported incidents, which is a 33 percent increase from just last year. This increase is across all critical infrastructure: water plants, pipelines, power plants, and oil and gas refineries.

Some interesting details of the ICS-CERT report include:

- Energy and Critical Manufacturing sectors reported highest
- Energy was 59 percent of reported incidents
- Critical Manufacturing was 20 percent of reported incidents
- 79 organizations were confirmed or suspected to be compromised
- 120 were indeterminate or unknown



ICS-CERT reports that the most threat vectors were unauthorized access, scanning and probing of publicly accessible assets, malware transferred by removable media (USB thumb drives), and exploitation of software/hardware vulnerabilities (outdated patches). The other more disturbing item in the report is ICS-CERT estimates there are many more incidents occurring but are not reported, since incidents may go undetected due to insufficient threat detection capabilities.

This report just reconfirms the constant cyber threat that exists, and that getting hacked is a matter of "when," not "if." Hackers are constantly evolving their techniques, forcing us to continuously update our methods to circumvent them. A good offense starts with a strong defense that consists of assessments, detection, monitoring, and response capabilities.

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
April 2014 / Issue 31

Industry News

Power plants put at risk by security bugs

From www.bbc.com, 4/4/2014

The discovery of bugs in software used to run oil rigs, refineries, and power plants has prompted a global push to patch the widely-used control system. The bugs were found by security researchers and, if exploited, could give attackers remote access to control systems for the installations. The U.S. Department of Homeland Security said an attacker with "low skill" would be able to exploit the bugs. About 7,600 plants around the world are using the vulnerable software.

Oil & gas companies new target for hackers

From timesofindia.indiatimes.com, 4/24/14

The next hacker playground: the open seas—and the oil tankers and container vessels that ship 90 percent of the goods moved around the planet. In this internet age, as more devices are hooked up online, they become more vulnerable to attack. As industries like maritime and energy connect ships, containers, and rigs to computer networks, they expose weaknesses that hackers can exploit. Globally, it is estimated that cyber attacks against oil and gas infrastructure will cost energy companies close to $1.9 billion by 2018. The British government reckons cyber attacks already cost UK oil and gas companies around 400 million pounds ($672 million) a year.

The European Parliament votes through cyber security legislation

From www.thelawyer.com, 4/15/2014

In February 2013, the European Commission released a draft Network and Information Security Directive. In addition to provisions aimed at member state governments, the draft directive applied to a wide range of companies within the definition of market operator. Market operators included private companies in the energy, transport, financial services and health sectors and also included 'enablers of key internet services,' such as providers of e-commerce platforms, social networks, cloud computing services, application stores, internet payment gateways (e.g. WorldPay) and search engines. The draft directive therefore had a direct impact on key players and stakeholders in the world wide web, including global technology brands such as Microsoft, Facebook and Google.

U.K. cyber security plan is voluntary like U.S. Framework, has differences

From www.bna.com, 4/21/2014

The cyber security scheme the U.K. government plans to launch this summer shares some similarities with the U.S. government's critical infrastructure cyber security framework, including being voluntary and aimed at all organizations, regardless of size or sector, Nigel Montgomery, a partner at Sidley Austin LLP in London told Bloomberg BNA. The proposed U.K. Cyber Essentials Scheme (CES) was released April 7. The CES focuses on five critical technical controls that organizations aren't adequately applying, so as to leave them vulnerable to cyber threats:

- Boundary firewalls and Internet gateways: to protect against attacks based on capabilities and techniques that are freely available on the Internet—by restricting inbound and outbound network traffic to authorized connections;
- Secure configuration: to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role;
- User access control: to ensure that special access privileges are assigned only to authorized individuals;
- Malware protection: to monitor for, detect, and disable malicious software; and
- Patch management: to identify that software running on computers and network devices is kept up-to-date.

Japan, U.S. to cooperate on defending critical cyber infrastructure

From www.globalpost.com, 4/11/2014

The United States and Japan agreed to strengthen cooperation on protecting critical Internet infrastructure from rampant cyber attacks, according to sources familiar with the discussions. The talks addressed how to protect critical infrastructure such as electric grids from cyber attacks, how to better define issues regarding cyberspace under international law, and how to increase developing countries' resistance to hacking. The two countries agreed to increase cooperation in these areas ahead of U.S. President Barack Obama's visit to Japan in late April.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
April 2014 / Issue 31

Cyber News

Heartbleed bug puts Internet at risk

From www.katc.com, 4/12/14

An Internet security flaw named "Heartbleed" has sent the I.T. world into panic mode to patch a flay that's been around for nearly two years. The bug allows hackers to pull private information, like passwords from the servers of businesses like Facebook, Google, and more. "The reality is, if you use the Internet, you were affected. Two-thirds of the Internet were vulnerable to this bug," says Daniel Kedinger, Digital Marketing Director for BBR Creative in Lafayette. His team deals with dozens of clients and their websites, and even though their websites were found to be secure, clients were still advised to take caution. "Your site, your bank might not have been affected, but the fact that your password on your email was found, means that now they have access to your bank account. And it doesn't take a lot to find out what else you have out on the Internet to find those services," says Kedinger.

Microsoft XP's massive cyber security problem

From www.politico.com, 4/7/14

Microsoft cut off support to its 12-year -old operating system Windows XP on April 8, leaving more than a quarter of the world's computers effectively undefended against hackers and cybercriminals. And because outdated software renders the computers that run it vulnerable to malicious programs deployed by hackers, that's bad news for everyone in today's ultra-connected world. Security experts liken the estimated 500 million computers still running the antiquated XP program to a group of unvaccinated children: Their vulnerability to infection puts at risk the health of the whole population.

Verizon annual cybersecurity report: 'The bad guys are winning'

From www.latimes.com, 4/22/14

The latest grim picture comes courtesy of Verizon's 2014 Data Breach Investigations Report. The report taps information from more than 50 organizations around the world to analyze more than 63,000 security incidents and 1,300 confirmed breaches. Amid the onslaught of breaches and statistics, the report also tries to offer some hope that organizations such as Verizon are starting to better leverage information about cyber attacks to craft strategies to fight back. "After analyzing 10 years of data, we realize most organizations cannot keep up with cybercrime—and the bad guys are winning," said Wade Baker, principal author of the Data Breach Investigations Report series, in a statement. "But by applying big data analytics to security risk management, we can begin to bend the curve and combat cybercrime more effectively and strategically." This year's report says that 97 percent of attacks fall into nine categories, including denial-of-service attacks, cyber espionage, and point-of-sale intrusions.

Nasty Heartbleed bug exposes OpenVPN private keys, too

From www.arstechnica.com, 4/16/14

Private encryption keys have been successfully extracted multiple times from a virtual private network server running the widely used OpenVPN application with a vulnerable version of OpenSSL, adding yet more urgency to the call for operators to fully protect their systems against the catastrophic Heartbleed bug. Developers who maintain the open source OpenVPN package previously warned that private keys underpinning VPN sessions were vulnerable to Heartbleed. But until recently, there was no public confirmation such a devastating theft was feasible in real-world settings, said Fredrik Strömberg, the operator of a Sweden-based VPN service who carried out the attacks on a test server.

Michaels breach exposes nearly 3M payment cards

From www.computerworld.com, 4/18/14

About 2.6 million payment cards at Michaels stores and another 400,000 at subsidiary Aaron Brothers may have been affected in a card skimming attack that compromised its point-of-sale systems, the retailer said earlier this month. Michaels said it had found evidence confirming that its systems and those of Aaron were attacked using sophisticated malware that had not been encountered previously by either of the security firms it had retained to investigate a suspected breach. It did not provide details of the malware. The arts and crafts supplier in Irving, Texas, said in January it was investigating a possible data security attack after it learned of suspicious activity on some U.S. payment cards that had been used at its stores. The attack on Michaels was one of several attempts to penetrate the point-of-sale systems of U.S. retailers.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
April 2014 / Issue 31

Monitoring Your Network

Today's complex network systems have become the foundation of business. A network's reliability and performance are essential. With so many interrelated devices and applications running simultaneously, system event diagnosis can be a challenge. Real-time visibility can significantly reduce the reaction time to system events, thus maintaining continuous operations and, more importantly, revenue.

How can real-time network performance monitoring help? For one, our customers are seeing a reduction in operation costs. They are using less effort to manage their networks with application-based technology with built-in automation. This proactive approach to network management allows real-time visibility spanning the entire critical IT infrastructure.

Some of the features and benefits of network performance monitoring include:

- Monitoring the health of key Critical Assets
- Viewing current bandwidth usage and identifying bottlenecks
- Detecting network system trouble before it happens
- Increased security by monitoring for "rogue" devices that have been connected without authorization
- Monitoring resources to track metrics such as disk space, CPU load, storage space, offline/online state, and memory utilization
- System event alert management from anywhere 24 hours a day, 7 days a week

Viewing all your key critical IT assets is a snap with built-in customizable dashboards. You'll also find the reporting tool handy for documentation. The benefits include:

- Real-time dashboards for quickly viewing your network's overall state
- Storage of time-based data from millions of elements
- Establishing a performance baseline
- Identification of all of your IT network inventory devices
- Pre- and post-deployment performance monitoring metrics
- Trending metrics provides data to project future growth

In summary, protecting your IT infrastructure can be easy and cost-effective with a comprehensive real-time network performance monitoring solution.

This month's contributor to Consultant's Corner is Curt Christian
Consultant, Critical Infrastructure & Security Practice, Invensys
curt.christian@schneider-electric.com

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
April 2014 / Issue 31

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 Critical Infrastructure 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 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 active participation 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 Assessments, Development,

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!

Schneider Electric

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

1820 Preston Park Blvd. Suite 1900 Plano, TX 75093 ▪ P 469.365.6400 ▪ F 888.758.7675 ▪ **iom.invensys.com**