The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

January 2014
Issue 28

this issue

January 2014 Cyber Attack Statistics Hackmageddon.com

Attack Motivations
44% Hacktivism
57% Cyber Crime
5% Cyber Espionage

Top 3 Attack Targets
23% Government
22% Industry
7% Organization

Top 5 Attack Techniques
14% Defacement
18% Unknown
9% Account Hijacking
23% DDoS
19% SQL

Invensys is becoming Schneider Electric

The Worst Hacks of 2013

A report released by NextGov earlier this month claimed that "many breaches disclosed in 2013 bore the markings of political tension… and not just leaks by ex-National Security Agency contractor Edward Snowden. Nationalistic hacks hit citizens worldwide in the pocketbook, violated expectations of privacy and spooked military forces." Though 2013 is behind us, the effects of some of these attacks will be long-lasting and some have already set the stage for what we may expect to see in 2014: heightened online privacy concerns, critical infrastructure risk, mobile malware, and debit/credit card theft. Only one month into the new year and at least two major retailers have already been victims of data breaches.

The worst hacks reported in 2013 included:

1. An unauthorized user gained access to an Army database of U.S. dams that documented the number of people who would be killed in the event of a collapse. The breach raised concerns that China was preparing for a cyber attack against the U.S. power grid, including energy produced by hydroelectric dams.
2. A suspected government-sponsored Chinese hacking team allegedly penetrated a decoy U.S. water utility.
3. During a fall summit in St. Petersburg, G20 heads of state and staff allegedly received tainted thumb drives and smartphone chargers from their Russian hosts.
4. Ex-NSA contractor Edward Snowden exposed a cache of government secrets documenting mass domestic surveillance and intercepts of foreign allies' emails and phone calls.
5. Almost 3 million customer records were stolen from Adobe, in addition to valuable software code.
6. Between late November and early December, cyber criminals stole credit and debit card data from up to 40 million in-store Target customers nationwide.

Even though decisions concerning security have usually been driven by compliance, the increased likelihood of cyber attacks have companies realizing that they must protect themselves. As 2014 progresses, we must be prepared for the number of cyber attacks and data breaches to escalate. Firewalls and anti-virus software alone are inadequate against cyber events. Having a cyber mitigation plan in place as well as implementing a thorough and comprehensive cyber security program is the best defense.

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

January 2014 / Issue 28

Industry News

Tech firms vie to secure energy sector against cyber attacks

From phys.org, 1/22/2014

To hear cyber security companies tell it, the U.S. energy industry is a ticking time bomb. Smart electric meters on the sides of houses can be entryways for cyber terrorists to shut off a city's power grid. Remote-controlled valves in oil refineries can be manipulated to cause costly spills. As reports of hacking perpetuate around the globe, security and technology firms are rushing to introduce high-tech products and services to protect power plants, pipelines, and oil companies from cyber attacks. The emerging business could soon be worth billions of dollars a year as agencies including the Federal Energy Regulatory Commission and the Nuclear Regulatory Commission order companies to better protect the infrastructure. "It's huge," said Greg Bell, a partner with the consulting firm KPMG who works in its cyber security division. "Almost every device we put in a power plant or an oil refinery is computer-controlled. They all have to be secured. Cyber security is a growth area across all the different industries, but especially oil and gas and (power) transmission."

Energy sector a growing target for cyber attacks

From itwire.com, 1/16/2014

There's a rising tide of cyber attacks on the energy sector, with a warning from a global security company that the growing adoption of smart grids, smart meters and the "Internet of Things," will likely lead to even greater risks and challenges for energy firms this year. In a whitepaper just released by Symantec, the global security firm examines the rising trend of attempted attacks against the energy sector, noting that in the first half of 2013, the energy sector was the fifth most targeted sector worldwide, experiencing 7.6% of all cyber attacks. In fact, Symantec said that from July 2012 to June 2013, it observed an average of nine attacks per day against the energy sector. "Disturbingly, reports of attempted attacks against the companies and industries that supply it (the energy sector) are increasing every year," Symantec notes.

Grant seeks to counter attacks on power grid

From fcw.com, 1/21/2014

The Energy Department gave Georgia Institute of Technology researchers $5 million to develop protocols and tools that can detect cyber attacks on the nation's utility companies. According to the Georgia Tech Research Institute (GTRI), the grant will fuel a cooperative effort to detect "adversarial manipulation of the power grid." The initiative seeks to provide real-time protection for the energy infrastructure by using advanced modeling and simulation technologies linked to a network of sensors.

Cyber attack by China on power grid alleged

From www.inquisitr.com, 1/17/2014

The power grid has reportedly been under a constant state of attack by English-speaking Chinese computer experts nestled in a rather unimposing building in Shanghai. The alleged cyber attacks by the computer hackers pose as significant a threat to America as the 2 million soldiers in the Chinese army ever could, if the cyber warfare studies by the Mandiant security firm are accurate. Technological Leadership Institute Director Massoud Amin believes the power grid problems are fixable, but a major change in the culture of the utilities industry would be required. Crippling the power grid would be perhaps the quickest way to destroy the American economy and decrease the effectiveness of the United States military. The People's Liberation Army would not have to step foot on American soil or fire a single shot in order to win a silent war virtually. In addition to the power grid, Amin also believes that the water and sewer infrastructure systems were at risk from Chinese and Russian cyber hackers as well.

Weak cyber security practices could cost world economy $3 trillion by 2020

From gadgets.ndtv.com, 1/20/2104

Failure to boost cyber security could cost the world economy a staggering $3 trillion as new regulations and approaches to deal with destructive attacks would stifle innovation, says a report. With the recent proliferation of cyber attacks, corporate executives need to devote increasing attention to protecting information assets and online operations, according to a report released by the World Economic Forum (WEF) in collaboration with global consultancy McKinsey & Company. Titled "Risk and Responsibility in a Hyperconnected World,'" the report cautioned that there could be increased cyber attacks if there is a failure to strengthen capabilities for deterring such activities. Major technology trends, including massive analytics, cloud computing, and big data, could create between $9.6 trillion and $21.6 trillion in value for the global economy. "However, if attacker sophistication outpaces defender capabilities—resulting in more destructive attacks—a wave of new regulations and corporate policies could slow innovation, with an aggregate impact of approximately $3 trillion by 2020," the report said.

Schneider Electric

The Global Cyber Advisor

Invensys Critical Infrastructure & Security Practice

January 2014 / Issue 28

Cyber News

1.1 million payment cards exposed to malware in Neiman Marcus hack

From arstechnica.com, 1/24/2014

Neiman Marcus has determined that a data breach extending from July until October of 2013 exposed as many as 1.1 million payment cards to malware, and that 2,400 cards have been used fraudulently as a result. "While the forensic and criminal investigations are ongoing, we know that malicious software (malware) was clandestinely installed on our system," Neiman Marcus wrote. "It appears that the malware actively attempted to collect or 'scrape' payment card data from July 16, 2013 to October 30, 2013. During those months, approximately 1,100,000 customer payment cards could have been potentially visible to the malware. To date, Visa, MasterCard, and Discover have notified us that approximately 2,400 unique customer payment cards used at Neiman Marcus and Last Call stores were subsequently used fraudulently." The Neiman Marcus breach did not expose any Social Security numbers and birth dates, nor did it affect customers who shop online. "PINs were never at risk because we do not use PIN pads in our stores," the company said.

Craft store Michaels may be latest mega-retailer to get hacked

From arstechnica.com, 1/24/2014

While Michaels has not yet confirmed a data breach, it published a press release (PDF) on Saturday saying “The Company is working closely with federal law enforcement and is conducting an investigation with the help of third-party data security experts to establish the facts. Although the investigation is ongoing, based on the information the Company has received and in light of the widely-reported criminal efforts to penetrate the data systems of U.S. retailers, Michaels believes it is appropriate to let its customers know a potential issue may have occurred.” The US Secret Service has confirmed that it is investigating the matter.

Microsoft retains weapon to silently scrub XP

From computerworld.com, 1/26/2014

Microsoft will be able to silently reach into Windows XP PCs for more than a year after it stops patching the aged OS to clean malware-infected machines, sources close to the company confirmed. The Malicious Software Removal Tool (MSRT) will continue to be updated and deployed via Windows Update through July 14, 2015, 15 months after the Redmond, Wash. company serves its final public security patches for XP on April 8 of this year. By extending the life of the MSRT—and more importantly, automatically running it each month—Microsoft will be able to clean some PCs if massive malware outbreaks hit Windows XP after it's retired from support.

“Password” is no longer the worst password

From threatpost.com, 1/21/2014

If you think you’re being clever by basing your password on the site you’re visiting or adding a zero to the end of 123456789, you’re not. A new list of the 25 worst passwords, culled from public dumps of passwords stolen in data breaches, shows that these are some of the least useful passwords you can come up with. The good news is that “password” is no longer the most popular bad password. The bad news is that the new loser is even worse. The most often-used password found in public password dumps in 2013 was “123456, about as far as you can get away from being a complex password. The list, compiled by SplashData, shows that “password,” which had been the most popular bad password for several years, fell to number two, while several variations of consecutive digits were also found in the top 10.

13 indicted in $2M gas station card-skimming scheme

From news.cnet.com, 1/22/2014

Prosecutors have charged 13 defendants with using card skimmers installed at gas stations to steal more than $2 million from customers throughout the southern US. The ring allegedly used card readers installed inside gas pumps to record payment card data and PINs from customers. The skimmers were installed internally and used a Bluetooth chip that allowed the thieves to retrieve the data without having to physically connect to the devices, according to an indictment unsealed Tuesday by Manhattan District Attorney Cyrus R. Vance Jr.

The FBI is warning retailers to expect hackers

From www.nextgov.com, 1/24/2014

In light of a massive security breach that revealed the information of 70 million Target customers, the FBI has begun warning retailers to expect similar intrusions. Reuter reports that the bureau has discovered 20 cases that used software similar to what was used against Target. The brief, confidential report given to retailers dated January 17 described "malware that infects point-of-sale (POS) systems, which include cash registers and credit-card swiping machines found in store checkout aisles." The malware takes advantage of the brief window in a computer's RAM when credit card information is unencrypted.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
January 2014 / Issue 28

Schneider Electric Acquires Invensys

On January 17, 2014 Schneider Electric's acquisition of Invensys was approved by all stakeholders and the deal closed. This acquisition sees two of the leading players in the industrial market join forces to create a more global, innovative, technology company with a strong position in integrated industrial automation, software and energy management.

Increased value for all our customers

Both Schneider Electric and Invensys customers stand to significantly benefit from this acquisition. Schneider Electric's customers can take advantage of improved industrial automation capabilities and a commitment to expand our offers in this market space. The deal also expands Schneider Electric's position in energy management and grows our software portfolio. For Invensys customers, this deal brings an exciting industrial future to become part of a company with high R&D investments, high levels of customer satisfaction and a promise to our combined customers to bring the highest efficiency by combining automation and energy management technologies.

In addition, leveraging the technology, innovation and joint development capabilities of both Schneider Electric and Invensys will enable new systems, applications and technologies to be brought to market faster.

More global coverage

With this acquisition, Schneider Electric and Invensys are creating a global leader in industrial automation, with a more balanced presence across all regions. We gain a stronger footprint in North America and in emerging markets, and a greater market resilience to help us better manage the cyclical nature of today's business and adapt quickly to changing technology trends.

Business as usual – focused on growth

Schneider Electric and Invensys are working on business as usual and all commitments we hold with our customers will be honored.

Schneider Electric and Invensys expect to realize accelerated growth through the synergies and opportunities born from stronger leadership in our targeted market segments. This means:

- More global coverage to be closer to customer needs
- More offers, solutions and services increasing the value we offer
- More diversity in our portfolio for greater market resilience

Check our website for more information

As the integration of Schneider Electric and Invensys continues, there will be more information available over the next few months on our websites. For our customers, all questions and concerns can be directed to your usual Schneider Electric or Invensys contact.

Schneider Electric

The Global Cyber Advisor
Invensys Critical Infrastructure & Security Practice
January 2014 / Issue 28

Critical Infrastructure and Security Practice

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.

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.

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!

Industry Knowledge

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

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, Implement and Management.

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**