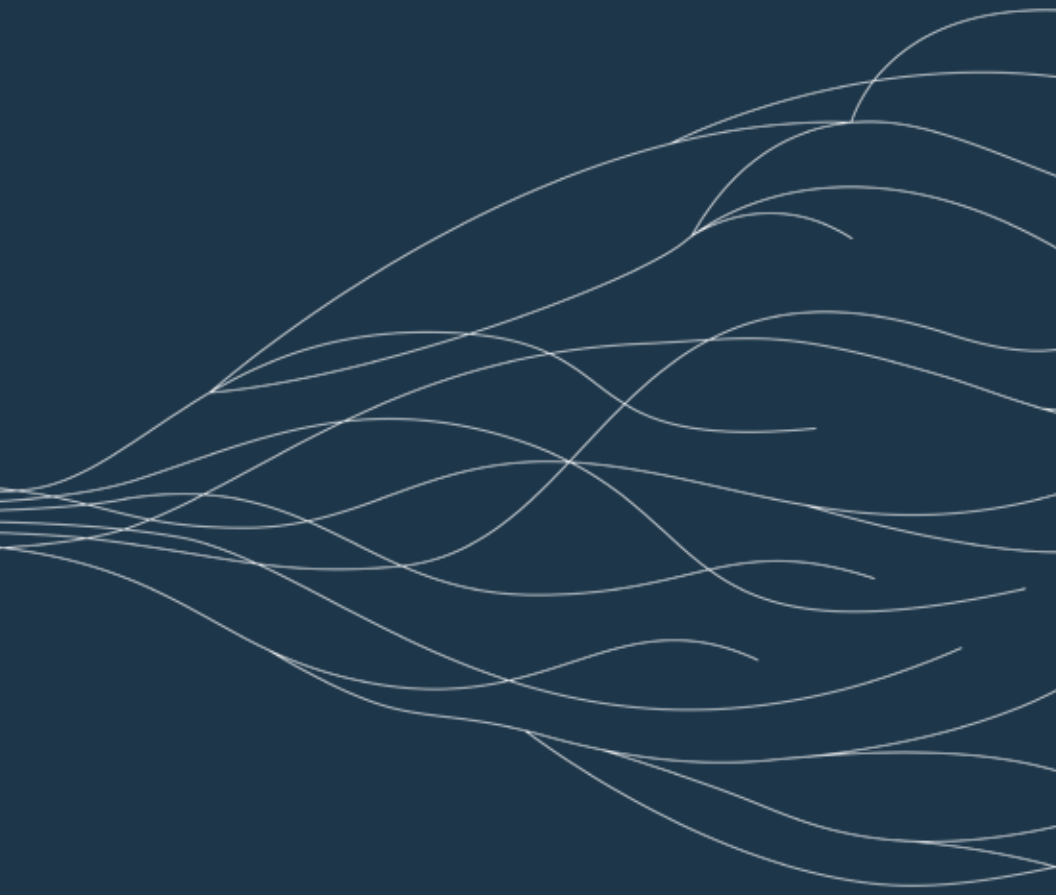


IBM Security

Keeping the lights on

Security trends in the energy and utilities industry

IBM X-Force® Research
Managed Security Services Report

IBM

Click here to start ►

Contents

Executive overview

Reliable. Secure. Constant. These qualities should define the energy and utilities industry, and usually they do. Electric, gas, and water utilities are built on a highly regulated framework, run by professionals, and backed by decades of operating experience and billions of dollars of infrastructure investment. Even so—and even with strong regulatory compliance—a successful cyber attack is still in the cards. The industry views that prospect with grave concern, for the consequences of such an attack on the companies supplying a city or a nation's fuel, electricity and drinking water could reach far beyond any purely economic impact. The health and welfare of a whole region or even an entire nation could be at risk.

Recent media attention has focused mostly on cyber incidents affecting the retail, finance and healthcare industries, but now the spotlight is also shining on the energy and utilities industry. Attacks on electrical grids and utility providers have increased steadily over the past decade, most notably the coordinated cyber attack on a Ukrainian power grid in December 2015 that resulted in tens of thousands of people losing electricity.

About this report

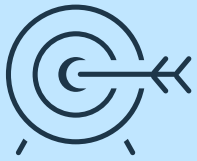
This IBM® X-Force® Research report was created by the IBM Managed Security Services Threat Research group, a team of experienced and skilled security analysts working diligently to keep IBM clients informed and prepared for the latest cybersecurity threats. This research team analyzes security data from many internal and external sources, including event data, activity and trends sourced from thousands of endpoints managed and monitored by IBM.

Contents

More recently, sophisticated malware designed to perform reconnaissance on an energy grid's system was found on a dark web hacking forum.[1] Cyber espionage attacks often have a reconnaissance phase in which the attacker seeks the vector most likely to yield access to systems and information against which additional, disruptive attacks might be launched.

Clearly, bad actors are actively seeking ways to attack the energy and utilities industry, and there is obvious and immediate cause for concern. The consequences across multiple industries could be significant. In the US, the Department of Homeland Security (DHS) describes the energy sector as "uniquely critical because it provides an 'enabling function' across all critical infrastructure sectors."[2] In other words, an attack on an energy company could have a domino effect impacting all the industries that depend on it.

Cyber attack preparedness is necessary. Your organization needs to recognize the areas of risk in your environment, understand potential attackers' motivations and know what types of attack you face.



Energy grids are increasingly a target of opportunity for cyber criminals.

Contents

Multiple targets, unique complexities

The energy and utilities sector has a broad threat surface, providing many points of entry into networks hosting critical assets. In some cases, the assets themselves are directly exposed to wireless or dial-in access. Potential targets include power generating plants, electrical substations, water and sewage treatment plants, fuel storage facilities and pipelines used for resource transport. Here, the potential impact on operations is more immediately apparent than in other industries: think loss of power or sewage backups.

Power generation comes in many forms—hydroelectric, wind, solar, biomass, biofuel, wood, nuclear, coal, natural gas, geothermal—and each has unique security considerations. Wind power, for instance, is generated via turbines that may be susceptible to cyber attacks. In 2015, several vulnerabilities affecting the embedded web server of a few different wind turbine models were reported.[3] The most serious of them could have been exploited remotely to change the administrator password for the web management interface, allowing an attacker to gain complete control of the turbine and cause loss of power.

Remotely exploitable vulnerabilities have also been found in web-based supervisory control and data acquisition (SCADA) systems used to monitor solar panels.[4] These products, reportedly used primarily in Europe and Asia, could be targeted to obtain the source code of executable scripts, view passwords in plain text, or inject malicious code via a cross-site scripting attack.

The energy and utilities sector is a highly regulated industry. According to RegData, in 2014 the electric power generation, transmission and distribution sector was the second most federally regulated industry in the US.[5] In a 2015 survey of senior corporate counsel in energy organizations, 28 percent indicated that regulation was a major challenge to their businesses.[6] A recent report stated that in Europe there are “wide-ranging methods of regulation.” While the “European Commission is likely to continue to push for greater consistency in regulatory regimes . . . rising energy costs are politically controversial for all national governments, and the trend toward greater convergence may well be countered by government interference with regulatory decisions.”[7]

Complex regulatory and compliance issues can often occupy much of an organization’s attention, potentially pushing the need to address security down the priority list and leaving gaps in protection. Coupled with the multitude of targets, these challenges leave the energy and utilities industry open to a wide variety of attacks.

Contents

Main motivations: sabotage and espionage

The IBM report *Know your cyber enemy* notes that while the motivation behind a cyber attack isn't always clear, a common theme across many energy and utilities cyber incidents seems to be sabotage. According to the report, "attackers in this category seek to damage or disrupt infrastructure and critical systems for various reasons—state-operated cyber groups seeking to reduce an adversary's effectiveness, extortionists looking for money, malicious actors purely for their own self-gratification."

Notable incidents including the 2015 Ukrainian power grid attack have involved sabotage. A Saudi energy company was targeted in 2012 with "Shamoon wiper" malware, affecting 30,000 workstations and causing disruptions to business.[8] In 2014, a South Korean nuclear power plant was the victim of wiper malware which erased servers and endpoints by disabling the master boot record.[9]

The profit motivation may not be as prevalent across the energy and utilities industry because cyber criminals don't necessarily benefit financially from attacking industrial control systems (ICS). That's not to say the energy and utilities industry doesn't hold sensitive and confidential information from which malicious individuals could profit. It certainly does. In 2013 two separate New York-based utility companies suffered incidents in which customer data was breached.[10,11] Then too, espionage could be involved. Corporate or state-sponsored attackers, including advanced persistent threat (APT) groups, might for instance be working to obtain SCADA data and power flow models that can help locate weak or hard-to-replace parts of the grid, creating the potential for additional, harmful attacks against a particular target.

Notable areas of risk

Insider threat from inadvertent actors

Inadvertent actors are typically well-meaning employees or other insiders who either mistakenly enable an attacker to access to data or fail to pay attention to a company's cyber security policies. *The 2016 Cyber Security Intelligence Index* reported that insiders were responsible for 60 percent of all attacks in 2015, up from 55 percent in 2014. Inadvertent actors were responsible for roughly a third of those attacks in 2015, compared with nearly half the previous year. The downward trend is a positive sign, especially for the energy and utilities industry.

IBM X-Force Interactive Security Incidents data reveals several compromises caused by inadvertent actors over the last few years (Figure 1):

- (Nov 2011) Several Norwegian businesses, including oil and gas, were targeted in a sophisticated spear-phishing attack used to steal sensitive documents and user credentials.[12]
- (Jan 2014) A system in a Japanese nuclear power plant reactor room was remotely accessed over 30 times after an employee installed free software containing a virus.[13]
- (April 2014) A US oil company was compromised via a watering hole attack in which attackers injected malware into the online menu of a Chinese take-out restaurant popular with the company's employees, gaining a foothold from infected endpoints.[14]
- (Aug 2014) A large targeted attack on numerous Norwegian oil companies used spear phishing to compromise systems.[15]
- (Dec 2014) A nuclear power plant in South Korea was targeted with wiper malware. The initial attack vector was a spear-phishing email.[16]
- (Dec 2015) A multi-tiered attack initiated with a spear phishing email was carried out on a Ukrainian power grid.[17]

Phishing and spear-phishing are common denominators among these incidents. The IBM report *Perils of phishing* provides additional information on this topic, including recommendations for addressing this threat.

Contents

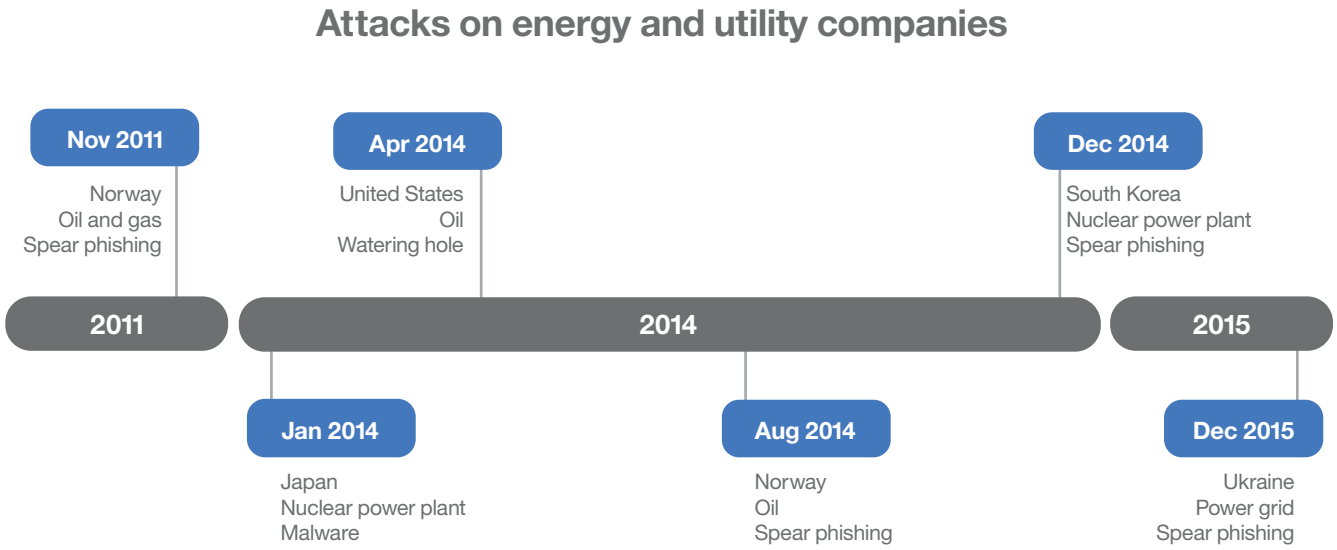


Figure 1. Timeline showing compromises to energy and utility companies caused by inadvertent actors.

While inadvertent actors are a notable threat, the energy and utilities industry should remain vigilant against the malicious insider. Unauthorized users may be able to log in to applications to which they really shouldn't have access, and even authorized users might present a problem if their actions aren't monitored. The aforementioned 2012 attack on the Saudi energy company was carried out by an individual with privileged access.[18]

Focusing on access management, specifically privileged identity management, is an important step towards an effective defense against malicious insiders, but it takes effort, and expediency can trump virtue. More information can be found in the IBM report *Battling security threats from within your organization*.

Contents

ICS and SCADA

There are a great many ICS configurations operating in the energy and utilities industry, including SCADA systems, distributed control systems (DCS) and programmable logic controllers (PLC), that are susceptible to malicious attacks including destructive malware. The Black Energy malware, for instance, was used in the coordinated attack on a Ukrainian power grid in 2015 that resulted in tens of thousands of individuals losing electricity.[19]

While technology and regulatory environments vary globally amongst utility firms, that incident serves as an example of the fragility of SCADA and ICS networks. It wasn't the first time a variant of the malware had been used. In 2014, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned of an ongoing campaign using Black Energy, active since at least 2011, to target ICS systems running GE's CIMPLICITY HMI product.[20] The IBM report *Security attacks on industrial control systems* details the susceptibility of these systems to certain attacks and outlines how they can be defended.

Technology transformations

In June 2010, an ICS malware known as Stuxnet targeted an Iranian nuclear facility, causing the shutdown of several nuclear centrifuges. The malware was introduced via a USB drive.[21] Today the threat of malware via USB still exists and is compounded by additional vectors opened up by technological advances.

The IBM paper *The future of energy and utilities* details five technology "happenings" shaping the energy and utilities industry: IT and operational technology, the Internet of Things (IoT), situational awareness, big data, and cloud. And while adapting to these technological transformations keeps today's energy and utility companies busy, attackers stay busy finding ways to target them, potentially disrupting the delivery of reliable and safe energy.

Contents

Take for example the smart grid, a class of technology that uses computer-based remote control and automation. These systems are used in transmission and distribution systems and wind farms and include connections to homes and businesses that use smart meters.[22] They offer benefits like increased energy efficiency and reduced operational costs, but they also introduce new security challenges, such as a multi-layered infrastructure, that could lead to grid instability, utility fraud, and loss of user information and energy consumption data.[23]

Another technological development is currently undergoing trials in Italy: smart meter interconnection between different energy services such as gas, water and waste.[24] This innovation brings automation efficiently to several utilities by using a common infrastructure, but from a security standpoint it might also mean greater complexity and increased susceptibility to a cascading affect across interconnected services when there is an incident.

Legacy infrastructure

A 2015 report by the U.S. Government Accountability Office (GAO) revealed that the amount federal agencies spent on obsolete technology increased over the past six fiscal years, while the amount invested in developing new systems decreased.[25] The challenge of maintaining legacy infrastructure isn't faced only by government agencies; the energy and utilities industry is built on decades worth of infrastructure in which legacy equipment still exists. For instance, older Remote Terminal Units (RTUs) that control electric substations use out-of-date serial communication standards like CDC Type 1 and GETAC that don't have a security component or monitoring capability. Replacement can cost up to a $100,000 per substation.[26]

Every organization faces the challenge of how best to address cyber risk while investing IT resources efficiently and cost-effectively. In the case of an older RTU, the risk to an older or proprietary communication protocol is plausible, but it's not a significant threat.[27]

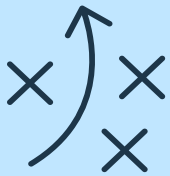
Contents

However, the threat from older unpatched ICS products is of rising concern. For several years now the ICS-CERT has been releasing alerts detailing vulnerabilities in ICS products that are end of life and for which no new firmware releases will be made available.[28] This equipment is difficult to replace without disrupting critical processes, which results in patches and upgrades not being installed despite the obvious security benefits of doing so. That makes ICS systems highly prized targets because many their vulnerabilities offer an attacker the chance to achieve complete system compromise.

Supply chain

Complex supply chains like those in the energy and utilities industry offer many potential entry points for invasion of a utility's IT infrastructure. A recent report on vulnerabilities found in solar panel systems illustrates the potential consequences of a breakdown in the supply chain. Reportedly, as many as 1,000 US homes that should have received production devices were mistakenly shipped development devices with vulnerabilities that could allow an attacker to gain remote root access to the solar panel controller and shut down the power.[29]

Managing safety, quality and performance along with cyber security risks is a significant challenge. It is important that supply chain managers understand how their suppliers' cyber security practices could affect them, then take appropriate steps to mitigate those risks. Often a cyber security contract clause or demonstration of best practices, such as using the NIST Cybersecurity Framework in the procurement process, can be a significant step towards understanding and managing risk.



Failure to apply patches and fixes can leave utility infrastructure at risk of penetration.

Contents

Prevalent attacks targeting the energy and utilities industry

IBM Managed Security Services (IBM MSS), which monitors billions of events reported every year by client devices in over 100 countries, analyzed the aggregate data accumulated between November 1, 2015 and July 31, 2016. Although MSS handles information only on IT networks, this data provides insight into the daily cyber experience facing the energy and utilities industry. In this section we define an attack as a security event observed in a system or network that has been identified by correlation and analytics tools as malicious activity attempting to collect, disrupt, deny, degrade, falsify or destroy information system resources or the information itself.

Malicious attachments or links

As Figure 1 shows, phishing was the initial attack vector in several incidents plaguing the energy and utilities industry. Phishing and malware are closely associated, as phishing is one of the main mediums by which malware is introduced on a network. Attacks aimed at fooling victims into opening malicious documents or clicking on links to malicious sites ranked number one in the energy and utilities sector, accounting for nearly 14 percent of all attacks. That closely mirrors the picture we see across the threat landscape in all industries.

Shellshock

Shellshock, a "malware-less" attack vector, is a vulnerability in the GNU Bash shell widely used on Linux, Solaris and Mac OS systems.[30] A significant and persistent threat across all industries ever since its first appearance in September 2014, today it ranks as the energy and utilities sector's number two attack vector, accounting for nearly seven percent of all attacks.

Probes and scans

Sustained probes and scans against a network are reconnaissance missions, usually aimed at gathering information about the targeted systems such as operating systems, open ports and running services. This activity, often viewed as a kind of pre-attack and known as "footprinting," is discussed in the IBM report *Beware of older cyber attacks*.

Footprinting encompasses several attack techniques, including port scanning. Generally, multiple ports are scanned, often in company with a service (or port) sweep in which multiple hosts in a network are checked for a specific open service port. Scans can make it easy for target organizations to notice they're being attacked and take action before the attackers get what they want.

Contents

The attackers are using this vector in the hope of gaining information that will help them launch subsequent cyber attacks. This type of activity accounted for 6.5 percent of the traffic observed targeting the energy and utilities industry. An additional problem is that older DCS systems have incomplete TCP/IP stacks, and just scanning an unused port can potentially cause a failure in the DCS.

SQL injection

Still prevalent across multiple industries, this attack attempts to pass SQL commands through a website in order to obtain the contents of databases not intended for public access. In the energy and utilities sector it accounts for just over 5.5 percent of attacks. To combat SQL injection, it's vital that organizations perform vulnerability scans on all applications, whether off-the-shelf or homegrown, and teach programmers secure coding practices. Database administrators should implement proper database, table, and even column security, and web servers and applications must be tested regularly for SQL injection vulnerabilities using tools such as IBM® Security AppScan®.

Cross-site scripting

Attackers take advantage of companies too narrowly focused on putting out the major fires by targeting their low-hanging-fruit vulnerabilities. For example, cross-site scripting allows an attacker to introduce a malicious script within a web page. The script executes once the page is accessed by a user who's usually been tricked into clicking on the page. Cross-site scripting accounts for almost 3.5 percent of attacks in the energy and utilities sector and stands at number three on the current Open Web Application Security Project (OWASP) Top Ten list, a ranking of the most critical web application vulnerability types.[31]

Contents

Energy and utilities industry: sources and targets of attacks

Based on IBM MSS data from November 1, 2015 through July 31, 2016, the United States hosted nearly half the attacks against energy and utilities targets (see Figure 2), with China a close second at nearly 40 percent. Nearly 60 percent of the attacks came from outside the targets and nearly 40 percent were insider attacks, either malicious or inadvertent.

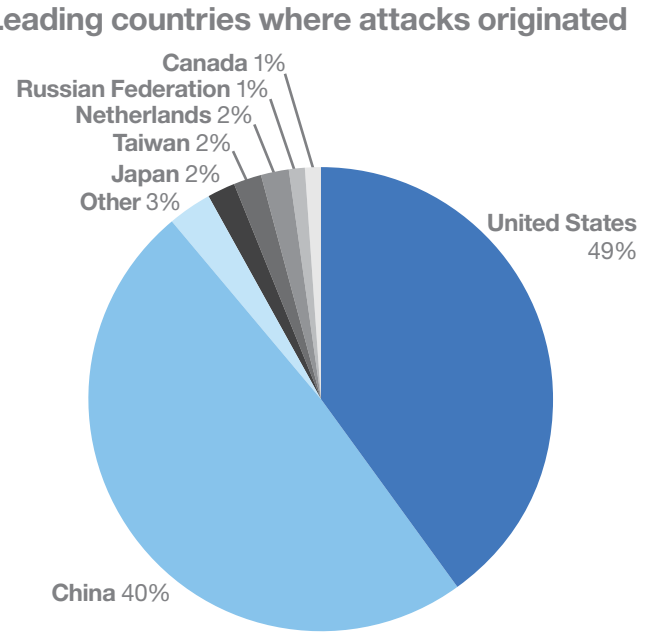


Figure 2. Leading countries where attacks against energy and utility institutions originated (November 1, 2015 – July 31, 2016). Source: IBM Managed Security Services data.

Recommendations

This report outlines a number of risks and attack vectors targeting the energy and utilities industry. A proper assessment of cyber risk is critical to effective direction of your IT investment and resources. Below we offer recommendations for you to consider when making strategic decisions to safeguard your business.

Incident response plan and team

A comprehensive incident response plan, or IRP, can help you shift your security stance from reactive to proactive mode, potentially saving you a great deal of time and money. Your IRP should be a dynamic document reviewed regularly, with changes made wherever they're needed after an incident.

Well-documented procedures go only so far, however. Every organization must also have staff capable of carrying out the IRP and calming the chaos of a security incident. Only a team well versed in the response program can deliver the consistency and efficiency needed to streamline responsiveness. Above all, the team must be well trained.

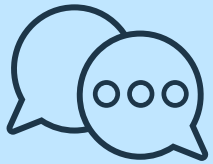
Contents

Participate in a trusted cyber threat information-sharing network

Few incidents in the energy and utilities industry are publicly disclosed. That means you have to examine breaches in other industries to learn about the impact of incidents and the attack vectors used in them, and then incorporate that knowledge into an effective risk management strategy. To that end, it's essential for your organization to establish an internal team that can digest and act on the lessons of external threat intelligence. Platforms like the IBM X-Force Exchange allow organizations to readily incorporate research of security threats, aggregated intelligence and collaboration.

When an incident is underway there's no time to waste; fast, effective response to an active attack is vital. Often the ability to provide it depends on having trusted partnerships across the energy and utilities industry. The smaller your organization, the truer this is, so small organizations should seek the assistance of larger companies with more experience and resources. In the US, organizations such as the North American Electric Reliability Corporation (NERC) provide a wealth of intelligence and can be a valuable resource during a cyber incident. Another US-based resource for sector-specific cyber and physical threat intelligence is the Electricity Information Sharing and Analysis Center (E-ISAC).[32]

Timely communication within your organization on threats and security recommendations goes a long way to protecting networks. For that to happen, your internal cyber security team must have timely intelligence, so we recommend joining an established information-sharing organization that collaborates and disseminates information and alerts about sector-specific threats. In the not-so-distant future, we anticipate that advanced tools such as Watson for Cyber Security will become essential to an organization's understanding of threats and decisions about protection and remediation.



Sharing information about incidents across the industry can help inform responses to future attacks.

Contents

Mitigate internal threats

Identifying misuse and suspicious activity on corporate networks is critical, so employee activity must be monitored in accordance with corporate security policies. There are various approaches to the task. Products that monitor behavior and detect anomalies, such as IBM QRadar® Security Intelligence platform, are essential. Most companies use this type of detection to monitor for anomalies such as an increased number of connections between a host computer and an internal client computer. This could indicate malware propagating itself and communicating with its associated command and control servers.

Another top corporate security priority should be access management. Users' access must be managed throughout their entire employment and even after their service with the company is terminated. Employees' access should be assessed regularly—annually at least—and whenever an individual changes roles or responsibilities, his or her access should be assessed and any unnecessary privileges revoked.

When employees leave the company, the employer must obtain all their usernames and passwords before they depart and verify that those passwords actually work. Perhaps most importantly, the company must disable all of an employee's accounts immediately upon departure. Solutions that include an identity manager and account-provisioning component, such as IBM Privileged Identity Manager, help an organization centrally manage and audit the use of privileged IDs across different scenarios.

Secure your ICS resources

ICS and SCADA systems are high-profile targets and potential gateways for an attacker to penetrate energy and utility company networks. It's important to define your ICS network infrastructure and ensure that practices such as monitoring all ICS critical applications and infrastructure are in place. Several of these practices are outlined in the IBM report *Security attacks on industrial control systems*. Connecting ICS systems to IT systems, such as to enterprise resource planning (ERP) systems for the purposes of key performance indicator (KPI) dashboards, may cause a security exposure if the IT system also has outside connections, such as an electronic purchase order portal.

Contents

Another vital part of mitigating risk is ICS vulnerability analysis and penetration testing. Regular penetration testing can help you uncover gaps in your network. Penetration testing services such as those performed by the IBM X-Force Red security experts allow organizations to focus on the management of vulnerability data and develop actionable plans to test any target. Additionally, connecting security components such as IBM QRadar® to SCADA-aware business partner products can provide some safeguards to legacy systems.

Vulnerability patching

As in the transportation industry, scaling security with the growing demands on the energy and utilities sector's systems and infrastructure is challenging. The industry's trend towards privatization, for example, means that the responsibility for identifying critical cyber infrastructure and applying patches falls on each individual owner or operator, so patch management policies can vary widely from one organization to the next. The Department of Homeland Security notes that in the US, "more than 80 percent of the country's energy infrastructure is owned by the private sector."[33] There are close to 200 large investor-owned electric utilities in the US, plus another 2,000 smaller publicly-owned utilities, all with varying levels of internal cyber security but all connected to the same electric grid.[34]

Many attack vectors exploit unpatched vulnerabilities, so timely patch management is vital in organizations of any size. With the analysis you gather from security intelligence and data analytics tools such as the IBM QRadar Security Intelligence Platform and IBM BigFix® Endpoint Management solution, you need to identify the greatest vulnerabilities in your sector and always—always!—keep your systems patched and up to date.

Business continuity and disaster recovery

When disruptions occur, businesses that have implemented an effective resiliency strategy will be better equipped to reduce risk and recover quickly. IBM Managed Resiliency Services can track compliance items in a response situation. IBM Emergency Response Services can help organizations prepare for, manage, and respond to computer security incidents by providing intelligence gathering, analysis, prevention, containment, eradication, recovery and forensics.

Contents

Identify, protect, respond and trust

Protecting the energy and utilities industry from cyber threats has become one of the most crucial issues facing world governments today. They and the industry itself must deal with a stew of often contradictory factors and forces: the multitude of targets, the complexity of regulations, the variety of threats from actors motivated by sabotage or espionage, the confusion of innovation from technologies such as smart grid, the foundational vulnerability of legacy infrastructure. Whatever the uncertainties of the situation, one thing is very clear: this is a collection of challenges that must be addressed. Relationships with trusted partners must be built and security providers with an extensive breadth of solutions, expertise and skills must be involved.

Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimize your security program, stop advanced threats, protect data and safeguard cloud and mobile. Security Intelligence Operations and Consulting Services can assess your security posture and maturity against best practices in security. Identity and Access Management Services help you ensure that only the right people have access to your applications and data. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that will help you improve your security posture—often at a fraction of the cost of in-house security resources.

Contents

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. IBM operates one of the world's broadest security research, development and delivery organizations, monitors billions of security events per day in more than 130 countries, and holds more than 3,000 security patents.

About the author

Michelle Alvarez, a Threat Researcher and Editor for IBM Managed Security Services, brings more than 10 years of industry experience to her role. Michelle is responsible for researching and analyzing security trends and developing and editing security and threat mitigation thought leadership papers. She joined IBM through the Internet Security Services (ISS) acquisition in 2006. At ISS she served as an analyst and contributed to the development of the X-Force Database, one of the world's most comprehensive threats and vulnerabilities database. For many years, Michelle played an important operational role within the Information Technology-Information Sharing and Analysis Center (IT-ISAC), a non-profit, limited liability corporation formed by members within the information technology sector. She is a regular contributor to the IBM-sponsored security blog, SecurityIntelligence.com, and has her master's degree in information technology.

Contributors

Scott Craig – Threat Researcher, IBM Security

For more information

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit:
ibm.com/security

For more information on security services, visit:
ibm.com/security/services

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog

Contents

[1] http://motherboard.vice.com/read/researchers-found-a-hacking-tool-that-targets-energy-grids-on-dark-web-forum

[2] https://www.dhs.gov/energy-sector

[3] http://securityaffairs.co/wordpress/37792/hacking/wind-turbines-hacking.html

[4] https://ics-cert.us-cert.gov/advisories/ICSA-15-265-02

[5] http://regdata.org/mclaughlin-sherouse-list-10-regulated-industries-2014/

[6] http://www.metrocorpcounsel.com/pdf/2016/January/25.pdf

[7] http://www.ey.com/Publication/vwLUAssets/Mapping_power_and_utilities_regulation_in_Europe/$FILE/Mapping_power_and_utilities_regulation_in_Europe_DX0181.pdf

[8] http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0

[9] http://blog.trendmicro.com/trendlabs-security-intelligence/mbr-wiper-attacks-strike-korean-power-plant/

[10] http://www.networkworld.com/article/2286787/4g/135100-The-worst-data-breach-incidents-of-2013.html#slide24

[11] http://www.databreaches.net/nyseg-online-hiring-site-hacked-customers-not-affected/

[12] http://www.bbc.com/news/technology-15790082

[13] http://enformable.com/2014/01/computer-control-room-monju-fast-breeder-reactor-infected-virus/

[14] http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html

[15] http://securityaffairs.co/wordpress/27895/cyber-crime/oil-energy-industry-norway-attack.html

[16] http://blog.trendmicro.com/trendlabs-security-intelligence/mbr-wiper-attacks-strike-korean-power-plant/

[17] https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[18] http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0

[19] http://arstechnica.com/security/2016/01/analysis-confirms-coordinated-hack-attack-caused-ukrainian-power-outage/

[20] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01B

[21] http://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/

[22] http://energy.gov/oe/services/technology-development/smart-grid

[23] http://timreview.ca/article/702

[24] http://www.european-utility-week.com/talkcommunityagnesececchini

[25] http://www.gao.gov/assets/680/670745.pdf

[26] http://www.belden.com/blog/industrialsecurity/Connecting-and-Securing-Legacy-Electrical-Substations-to-the-Smart-Grid.cfm

[27] http://www.electricenergyonline.com/show_article.php?mag=103&article=845

[28] https://ics-cert.us-cert.gov/advisories/ICSA-16-070-01

[29] http://www.forbes.com/sites/thomasbrewster/2016/08/01/1000-solar-panels-tigo-vulnerable-hackers/#41383fdc3811

[30] https://exchange.xforce.ibmcloud.com/, vulnerabilities CVE-2014-7169, CVE-2014-6271

[31] http://www.ibm.com/developerworks/library/se-owasp-top10/

[32] https://www.esisac.com/

[33] https://www.dhs.gov/energy-sector

[34] http://www.publicpower.org/files/PDFs/USElectricUtilityIndustryStatistics.pdf

Contents

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
September 2016

IBM

SEL03101-USEN-00