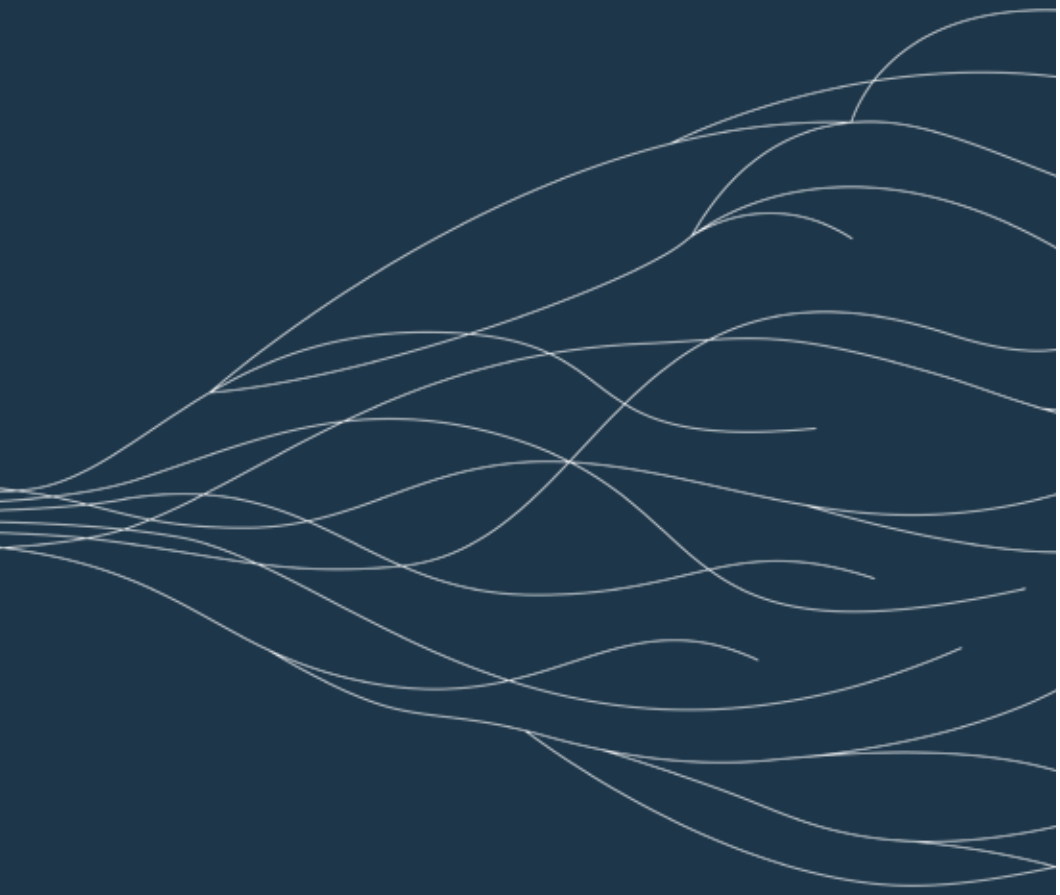


IBM Security

Security trends in the transportation industry

Defending a critical infrastructure segment against cybercrime

IBM X-Force® Research
Managed Security Services Report

IBM

Click here to start ►

Contents

Executive overview
1 • 2

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Executive overview

Transportation is a critical infrastructure sector. Disruption or destruction of its systems or assets can have negative and even disastrous effects on a country's security and public health or safety. Moreover, other sectors—food, agriculture, emergency services—depend on it for continuity of operations and service delivery, so a transportation sector IT security incident can create a widespread domino effect, greatly compounding the threat.

In addition to the danger of terrorism, natural disasters, physical theft and accidents, the transportation sector is increasingly vulnerable to cyber threats because of what the Department of Homeland Security describes as "the growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems, as well as the ease with which malicious actors can exploit cyber systems serving transportation."[1] IBM's own research reflects that trend; the latest IBM X-Force 2016 Cyber Security Intelligence Index shows the transportation industry rising into the top five most-attacked industries in 2015. According to IBM Managed Security Services data, a combination of denial of service (DoS) attacks and malicious attachments or links accounted for over 44 percent of the cyber attacks targeting transportation organizations during the period March 1, 2015 through May 15, 2016.

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

Executive overview
1 • 2

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Why attack the transportation industry? IBM's Know your cyber enemy report highlights a variety of motives but states quite clearly that "direct financial gain is the aim of profit-motivated attacks and the driver behind the most active areas of cybercrime." As we detail later in this report, that conclusion is evident in the types of transportation industry incidents disclosed over the last few years, especially attackers' increasing focus on certain niche targets from which to steal sensitive information.

Scaling security with the growing demands on transportation's infrastructure and systems is challenging. For example, the industry's trend towards privatization[2] means that the responsibility for identifying critical cyber infrastructure and applying patches falls on each individual owner or operator, so patch management policies may vary widely from one organization to the next. Vulnerable systems could include navigation equipment, air traffic control, and tracking and communication systems. One report published last year found that in the maritime sector, 37 percent of the servers running Microsoft were still vulnerable to a remote exploitation weeks after a patch had been released.[3]

As daunting as these security challenges may seem, transportation organizations willing to invest in cybersecurity can be in a strong position to prevent attacks and compromise.

In addition to terrorism, accidents and natural disasters, the transportation industry is increasingly vulnerable to cybersecurity threats.

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets
1 • 2

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Planes, trains and automobiles: No shortage of targets

In the US, the transportation sector is defined by sub-sectors: aviation, highway infrastructure and motor carrier, maritime transportation system, mass transit and passenger rail, pipeline systems, freight rail and postal and shipping.[4] That's a huge network, and within each system the volume of individual units continues to grow. In 2010, the number of vehicles in operation worldwide passed the 1 billion mark.[5] As of January 2015, the number of merchant ships in the world exceeded 50,000.[6] In the US alone, 70,000 flights were handled daily in 2015.[7]

There are many ways to tamper with these systems. Take for instance the risks associated with connected vehicles. As IBM's Driving security report describes, and security researchers have demonstrated, computerized vehicles can be hijacked with just a laptop computer and some easily obtained software. Attacks can be relatively harmless—a display of false telemetry telling you you're out of gas when in reality you have plenty—or they can be catastrophic: your brakes are suddenly applied or your engine switched off at high speed on a crowded freeway.[8]

There is also legitimate cause for concern about today's highly interconnected aircraft. According to the American Institute of Aeronautics and Astronautics (AIAA), "one of the most complex and integrated systems of information and communications technology (ICT) in the world, the global aviation system is a potential target for a large-scale cyber attack."[9] In 2015, the aviation industry came under intense scrutiny after reports that a security researcher allegedly tampered with flight controls via the in-flight entertainment system (IFE) during flight.[10] The incident exposed serious issues with having physical network ports in an aircraft's general seating area that allowed access to its avionics and IFE.

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets
1 • 2

Transportation industry security incidents by attack type, time and impact
1 • 2 • 3 • 4

Prevalent attacks targeting the transportation industry

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

In the US, the Next Generation Air Transportation System (NextGen) is a new national aerospace system being implemented in stages between 2012 and 2025. During this transformation, a satellite-based system called Automatic Dependent Surveillance Broadcast (ADS-B) will replace radar as the primary means by which air traffic controllers track and manage aircraft.[11] While the ADS-B system and new Aircraft Interface Devices (AIDs) that access aircraft data and communication channels may increase efficiency and reduce costs, they might also open doors to new threats. Globally, the aviation industry is moving towards IP-based systems that will introduce new security challenges and reduce barriers against cyber attack tools and techniques already in use on the public internet.[12] A comprehensive approach to address cyber security is required.

In the highway sector, hackers have changed electronic warning signs at road construction sites to read "Zombies Ahead." That is just a benign prank, but imagine the effect of the same kind of hack on the timing system of even a single traffic light.[13] An alteration of just a few seconds might well mean injury or death(s). Tampering with the controls of the signals that alert train drivers to dangers on the track could lead to catastrophe. These used to be just plots from the movies. Not anymore; today they are real, plausible threats.

Transportation industry security incidents by attack type, time and impact

The transportation industry has already experienced some notable cyber security incidents involving malware. In 2003, the Sobig virus infected a railroad company's computer system, shutting down signaling, dispatching and other systems and causing train delays.[14] Such disruption might not sound serious, but it can have a significant impact on railroad owners via decreased lading revenue and increased crew, locomotive, fuel and equipment costs; on shippers through inventory devaluation and holding costs; and on the public with lost work hours, increased emissions, pollution and traffic congestion at railroad crossings.[15] In 2004, a year after the Sobig attack, the Sasser worm targeted two airlines and one rail transportation company, delaying or cancelling flights and trains.[16]

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact
1 • 2 • 3 • 4

Prevalent attacks targeting the transportation industry

Transportation best practices

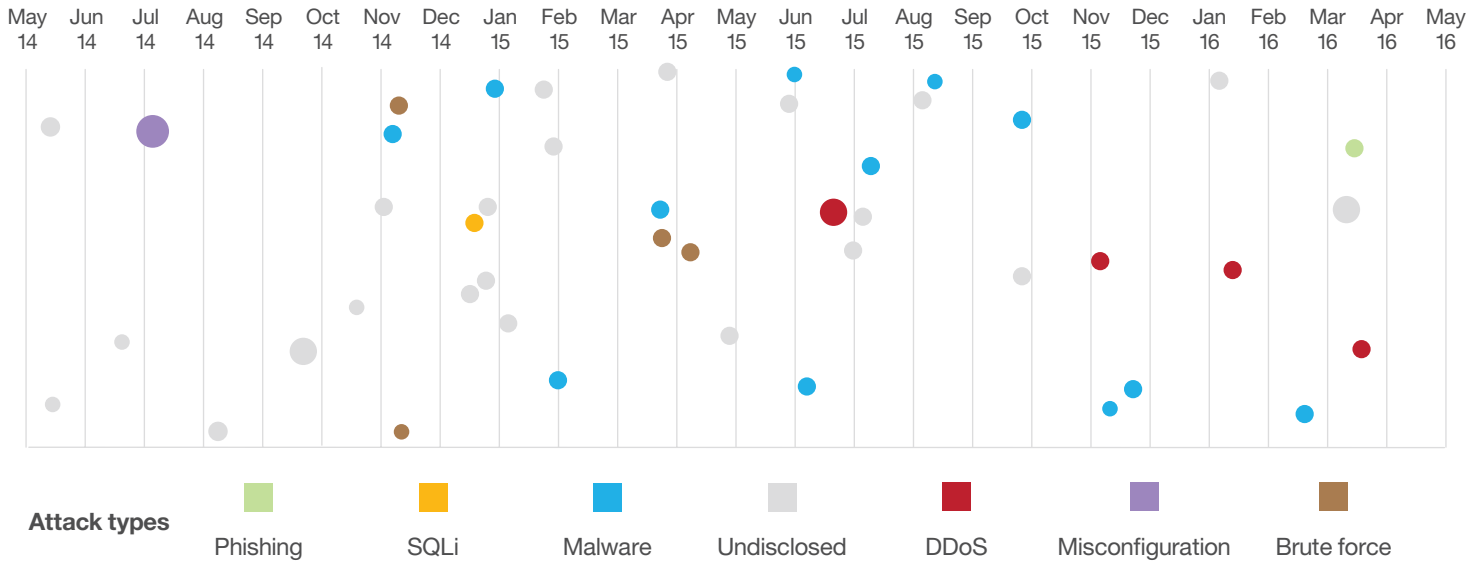
Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

More recently the trend has veered away from disruption of service towards theft of information for financial gain via malware, distributed denial of service (DDoS) attack or another exploit vector. Most incidents publicly disclosed over the last few years have involved inadvertent information leaks and stolen personal identifiable information (PII) and credit card data. That's the new norm across many industries, not just transportation. In 2014, the Chinese national train reservation system was the target of an insider who stole personal data of customers.[17] The following year, sensitive passenger data including travel manifests were stolen from a major US-based airline[18] and the frequent flier accounts of several airlines were targeted.[19] Attackers often use stolen logins, gained through other data leaks and password reuse, to steal miles they can sell or convert into gift cards or other tangible goods.[20]



Size of circle estimates relative impact of incident in terms of cost to business.

Figure 1. Transportation security incidents timeline. Source: IBM X-Force Interactive Security Incidents data (May1, 2014 – May 15, 2016). Note: Data is a sampling of notable incidents, not a full representation of all incidents. Conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses.

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact
1 • 2 • **3** • 4

Prevalent attacks targeting the transportation industry

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Niche targets: Parking lots, loyalty sites, private transit

In the 2015 IBM report Security trends in the retail industry we revealed a small tactical shift in which attackers had begun moving away from targeting just a few large organizations towards targeting many smaller businesses. In the transportation industry, an interesting emergent trend is a focus on lucrative niche targets, for instance parking management companies. We have seen several incidents in this area during the past couple of years, a number of them involving offsite airport parking companies. One of the largest US-based parking lot companies was targeted recently in a spear phishing attack that resulted in the theft of W-2 data from thousands of employees.[21] Such attacks certainly aren't unique to the transportation sector; many incidents across multiple sectors in the last several months have involved spear phishing attacks and the theft of W-2 data for use in tax fraud and other identity-theft scams.[22]

Loyalty accounts are also attractive targets, and sub-sectors of the transportation industry, including aviation, maritime, passenger rail and postal and shipping, are at risk. Rewards points or miles don't carry any "cash" value according to the terms and conditions of many loyalty programs, but sometimes they can be used as a form of currency in exchange for goods or services. Many airline loyalty programs let consumers use their miles to buy products unrelated to travel, and sometimes they even convert loyalty points to cash, allowing criminals to quickly turn stolen miles into profit. In 2015, the frequent flyer account information of reportedly "tens of thousands" of UK airline customers was leaked.[23] The airline denied having been breached directly, which suggests that either phishing or password reuse opened the door to the data theft. IBM's The price of loyalty programs report provides details on loyalty program attack vectors and offers recommendations for program users and owners.

Although loyalty program reward points may not have actual cash value, they can be stolen and redeemed for goods or services that can in turn be sold.

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact
1 • 2 • 3 • 4

Prevalent attacks targeting the transportation industry
1 • 2 • 3

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Attackers seeking a treasure trove of sensitive information, credit card data included, need look no further than private transit companies such as taxi and limousine services. In 2013, the compromise of a company providing software to US car services exposed the personal and financial information of more than 850,000 customers.[24] The following year, a US taxi company publicly released trip log information simply encrypted with MD5 hashes, enabling easy decryption and access to sensitive private information.[25] In 2015, reports surfaced about customer accounts of a popular multinational transportation company being offered for sale on the dark web marketplace.[26] The previous year, that same organization suffered a database breach in which driver names and license plate numbers were compromised.[27]

Toll operations companies are another niche target. Although there doesn't appear to have been a confirmed compromise, a proposed class action filed in October 2015 illustrates the mistakes these companies can make in securing payment card information. A major California toll operator violated the Fair Credit Reporting Act by disclosing too much of their customers' credit card information on receipts, potentially exposing hundreds of thousands of drivers to identity theft.[28]

Prevalent attacks targeting the transportation industry

We analyzed the aggregate data accumulated between March 1, 2015, and May 15, 2016, by IBM Managed Security Services, which monitors billions of events reported every year by client devices in over 100 countries. Although MSS captures information on only IT networks, it provides some insight into the daily cyber experience facing the transportation industry.

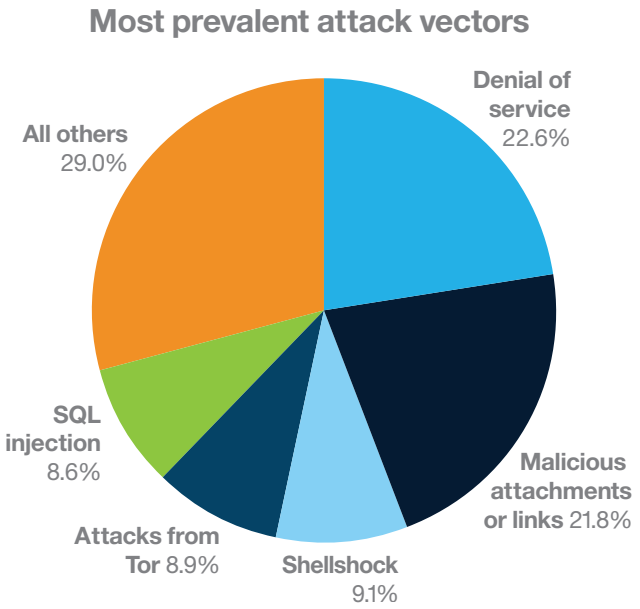


Figure 2. Most prevalent attack vectors in the transportation industry. (March 1, 2015 – May 15, 2016). Source: IBM Managed Security Services data. Note: Attacks are based on monitored IT networks, not attacks against the control networks or the mode of transit (such as airplanes, trains, truck and ships).

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry
1 • 2 • 3

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Denial of service

IBM Managed Security Services data shows denial of service (DoS) as the most popular attack vector against transportation IT networks, accounting for nearly 23 percent of such attacks in the transportation industry, most of them attacks against a web server. Denial of service is often an attacker's go-to weapon because it requires no complicated tools or methods, and its effects can be devastating. In June 2015, ten flights were grounded at a Warsaw airport due to a DoS attack that interrupted the airline's ground control computer systems.[29] In November 2015, domestic and international flights at Swedish airports were canceled because of a DoS attack on national air traffic control systems.[30]

Malicious attachments or links

Attacks aimed at fooling victims into opening malicious documents or clicking on links to malicious sites are popular across many industries, the intent almost always being to have the victim download malware. Over the last year, malicious attachments or links made up nearly 22 percent of the attacks targeting transportation organizations' IT networks.

A malware infection on any transportation system has the potential to be devastating. In 2015, a major Ukranian railway operator and other government organizations were reportedly infected with BlackEnergy malware thought to be used to conduct DDoS attacks and cyber espionage.[31] Transportation is also vulnerable to the trickle-down effects of malware infections in other industries such as manufacturing. If a manufacturer's production system is compromised by malware, for instance, machines designed to produce automobiles, trains, airplanes and ships could introduce flaws into the final product used in the transportation industry.

Phishing email campaigns targeting transportation industry consumers are also a concern. An email might purport to contain the recipient's airline ticket order[32] or attempt to capitalize on a recent tragedy by coaxing the victim to view a related news article or video.[33] One important way to minimize attack attempts via spear phishing and other scams is education. Consider implementing a phishing awareness campaign among your customers to help users identify phishing attacks.

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry
1 • 2 • 3

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Shellshock

Shellshock accounts for just over nine percent of the attacks against transportation IT networks. Shellshock is a vulnerability in the GNU Bash shell widely used on Linux, Solaris and Mac OS systems and is well documented by the IBM 2015 Cyber Security Intelligence Index. This "malware-less" attack vector has been a significant and persistent threat across all industries, not just transportation, since it first surfaced in September 2014.

Attacks from the Tor network

Nearly nine percent of attacks targeting the transportation industry's IT networks came from the Tor network. As described in the IBM paper Dangers of the deep, dark web, criminals often use the Tor network to launch attacks against surface web targets as well as to hide, communicate and trade with each other without exposing the content of their transactions.

SQL injection

SQL injection continues to be one of the most prevalent attack vectors exploited across multiple industries; for the transportation sector's IT networks it's in fifth place at over eight percent. This attack attempts to pass SQL commands through a website in order to obtain the contents of databases not intended for public access. To combat SQL injection attacks it is vital that organizations perform vulnerability scans on all applications, off the shelf or homegrown, and teach programmers secure coding practices. Proper database, table and even column security should be implemented by database administrators.

Denial of service and malicious attachments or links are the leading attack types in the transportation industry, followed by Shellshock, attacks from the Deep Web and SQL injection.

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry

Transportation best practices
1 • 2

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Transportation best practices

The transportation industry is huge and some specific cyber security recommendations are unique to one or another of its many sub-sectors, but this paper seeks to provide an overview of best practices across the industry as a whole.

Ask your manufacturers the right questions

The manufacturing industry plays a crucial role in the security of the transportation industry. An attack on a nation's transportation system may come through a vulnerability in products developed by private manufacturing companies. As the IBM report Security trends in the manufacturing industry states, "weaknesses in any segment of a manufacturer's network can threaten the integrity and availability of manufacturing production systems." A lack of end-to-end security designed into individual products such as airplanes, navigation systems and connected cars could create opportunities for attackers to penetrate wider technologies and modes of transit. For example, a research paper published in 2014 highlighted how vulnerabilities in popular satellite land equipment could be exploited by attackers to hijack and disrupt communications links to ships, airplanes, military operations, industrial facilities and emergency services.[34]

Transportation companies should be asking their manufacturers questions: Do your products stem from a trusted supply chain? Does your quality assurance program adhere to industry best practices? The answers will show which manufacturers fit with their cybersecurity program.

Integrate information security sharing

Incorporating external threat intelligence provider information into your organization's risk management strategy can enhance your decision making. Establish an internal team that can digest and act upon such information. Platforms like the IBM X-Force Exchange allow organizations to readily incorporate research of security threats, aggregated intelligence and collaboration. Join an established information sharing organization—one that collaborates and disseminates information and alerts about sector-specific threats—that your internally designated team can use across your organization. Timely communication on cyber threats and security recommendations internally goes a long way to protecting your networks. The transportation sector has many niches and these are being addressed across the industry segments and by region, so consider participating in these collaboration efforts if you aren't already.

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry

Transportation best practices
1 • 2

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

Combine security intelligence with data analytics

Security intelligence should be combined with data analytics to obtain insights into security risks. Tools such as the IBM QRadar® Security Intelligence Platform and IBM Big Data Platform can provide a comprehensive, integrated approach with real-time correlation for continuous insight and custom analytics across massive structured and unstructured data.

Vulnerability patching and anti-virus

Because many attack vectors exploit unpatched vulnerabilities, timely patch management is vital. Use the analysis obtained from security intelligence and data analytics tools, such as the IBM QRadar Security Intelligence Platform, to identify the greatest vulnerabilities in your sector, and keep your systems patched and up to date. Anti-virus solutions remain highly recommended, but just like operating systems and applications, the solution and its relevant signatures must be kept current.

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 offers a range of services to help you strengthen protection of your resources against unauthorized access. 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

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

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

David McMillen – Senior Threat Researcher, IBM Security

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

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

[1] https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation systems-2015-508.pdf

[2] https://people.hofstra.edu/geotrans/eng/ch7en/appl7en/ch7a2en.html

[3] http://www.networkworld.com/article/2917856/microsoft-subnet/maritime-cybersecurity-firm-37-of-microsoft-servers-not-patched-vulnerable-to-hacking.html

[4] https://www.dhs.gov/transportation-systems-sector

[5] http://wardsauto.com/news-analysis/world-vehicle-population-tops-1-billion-units

[6] http://www.statista.com/statistics/264024/number-of-merchant-ships-worldwide-by-type/

[7] http://www.natca.org/index.php/acronyms-breakdown/facts-sheet8http://wot.motortrend.com/video-find-watch-hackers-hack-into-toyota-prius-ford-escape-389065.Html

[9] http://www.aiaa.org/uploadedFiles/Issues_and_Advocacy/AIAA-Cyber-Framework-Final.pdf

[10] http://www.darkreading.com/attacks-breaches/planes-tweets-and-possible-hacks-from-seats/d/d-id/1320499

[11] https://www.faa.gov/nextgen/

[12] http://aviationcybersecurity.blogspot.com/2015_08_01_archive.html

[13] http://www.networkworld.com/article/2466551/microsoft-subnet/hacking-traffic-lights-with-a-laptop-is-easy.html

[14] http://www.cbsnews.com/news/virus-disrupts-train-signals/

[15] http://railtec.illinois.edu/articles/Files/Conference%20Proceedings/2015/Lovett-et-al-2015-IAROR.pdf

[16] http://www.coderedsecuritypr.com/blogs/35-understanding-scada-attacks

[17] http://english.cri.cn/12394/2014/12/25/3241s858286.htm

[18] http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines

[19] http://www-03.ibm.com/security/xforce/xfisi/

[20] http://www.nydailynews.com/news/national/thousands-american-united-airlines-accounts-hacked-article-1.2075162

[21] http://www.sandiegouniontribune.com/news/2016/mar/15/laz-parking-w2-compromise/

[22] https://blog.cloudmark.com/2016/03/31/55-companies-and-counting-w-2-spear-phishing-attacks-continue-to-increase/

[23] http://www.theguardian.com/business/2015/mar/29/british-airways-frequent-flyer-accounts-hacked

[24] http://krebsonsecurity.com/2013/11/hackers-take-limo-service-firm-for-a-ride/

[25] http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/

[26] http://motherboard.vice.com/read/stolen-uber-customer-accounts-are-for-sale-on-the-dark-web-for-1

[27] http://arstechnica.com/business/2015/02/50000-uber-driver-names-license-plate-numbers-exposed-in-a-data-breach/

[28] http://www.law360.com/articles/717358/calif-tolls-put-drivers-at-risk-for-identity-theft-suit-says

[29] http://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot

[30] http://www.scmagazine.com/swedens-airspace-shut-down-by-russian-apt-not-a-solar-storm/article/489572/

[31] http://securityaffairs.co/wordpress/44452/hacking/blackenergy-mining-and-railway-systems.html

[32] http://www.spamfighter.com/News-19866-Malware-Laced-Scam-Email-Imitating-American-Airlines-Circulating.htm

[33] https://www.scamwatch.gov.au/news/scammers-using-videos-of-malaysian-airlines-flight-mh370-to-spread-malware

[34] http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

Contents

Executive overview

Planes, trains and automobiles: No shortage of targets

Transportation industry security incidents by attack type, time and impact

Prevalent attacks targeting the transportation industry

Transportation best practices

Protect your enterprise while reducing cost and complexity

About IBM Security

About the author

References

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
June 2016

SEL03097-USEN-00