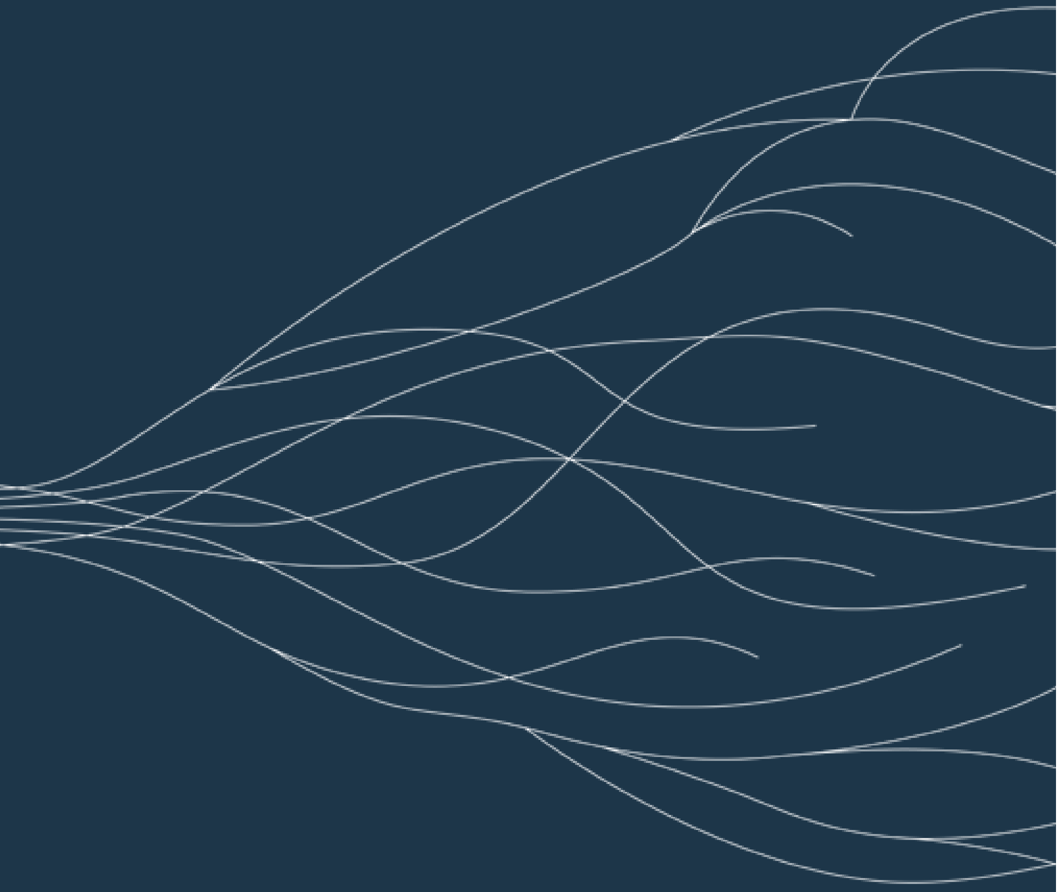
IBM Security



The changing face of IT security in the government sector

Rising attack rates and massive breaches plague government organizations

IBM X-Force® Research

Click here to start ▶

Executive overview

A government's core role is to protect and enhance the lives of its citizens. It must deliver services to create and sustain a robust and efficient public infrastructure, ensure public safety, foster sustainable economic growth, and build stronger communities. Those tasks bring many challenges, but one overriding requirement is common to them all: security. Without it, no government in the world can perform its role. Security is a prerequisite.

Information security is just one element of a much bigger picture. Today's government threat landscape extends from cyber security, physical security and critical infrastructure security to the fight against terrorism and the protection of the citizenry from natural disasters.

About X-Force

The IBM X-Force research team studies and monitors the latest threat trends including vulnerabilities, exploits, active attacks, viruses and other malware, spam, phishing, and malicious web content. In addition to advising customers and the general public about emerging and critical threats, IBM X-Force also delivers security content to help protect IBM customers from these threats. Threat intelligence content is delivered directly via the IBM X-Force Exchange collaborative platform, available at xforce.ibmcloud.com

As the digital and the physical realms have grown more connected over the last few years, cyber threats to the government sector have become a growing concern. IBM's 2016 Cyber Security Intelligence Index reports that in 2015, the government sector advanced from sixth place to fourth place among most frequently attacked industries, and in the longer term the trend is clearer still. Reportedly, cyber attacks against the US government are up 1,300 percent since 2006.[1] This situation is anything but unique. It can become a major issue for any country on earth.

Globally, during 2015, IBM Managed Security Services (IBM MSS) observed a 36 percent increase in security incidents affecting the average government client organization. "Security incident" is the most serious of IBM MSS data classifications (see sidebar "Events, attacks and incidents defined"). That figure wasn't as high as the 64 percent rise we observed in our average client organization across all industries, but it was certainly notable.

Coupled with reports of massive government breaches in 2016, these findings underscore a need to draw attention to threats targeting governments. IBM Security found both newer threats like Shellshock plaguing government organizations and older, tried-and-true threats such as SQL injection and buffer manipulation still prevalent across incidents on government networks.

Events, attacks and incidents defined

Security event: An event on a system or network detected by a security device or application.

Attack: A security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

Security incident: An attack or security event that has been reviewed by IBM security analysts and deemed worthy of deeper investigation.

Cybercriminals: Profiting from today's data-driven economy

Globally, 2.5 quintillion bytes of data are created each day. Most of this "big data" has been created in the last two years from many sources. With the expansion of technologies like the Internet of Things (IoT), digital services, mobile and cloud, the rate of data creation can only continue to increase.[2]

Organizations can adjust to this new reality by leveraging big data to outperform the competition, manage risk, create IT agility and make better decisions—but attackers too can take advantage of this data. Financially motivated cybercriminals are always inventing new theft schemes and finding ways to monetize data in the underground black markets, and that's a big part of why they target data-rich industries like government. The wealth of information within a government record can be put to all kinds of nefarious uses: pivoting to additional sources of information about the individual exposed, gaining access to confidential information, applying for credit cards or loans, even filing fraudulent tax returns.

Furthermore, threats are often asymmetric and attackers are multi-dimensional. They're fully capable of setting their sights on multiple targets and just as adept at launching myriad attacks, from targeted banking malware campaigns to distributed denial of service (DDoS) extortion to command injection attacks. Congruent trends are often found across the threat landscape. Whether it's healthcare, the financial sector or government records, attackers will go wherever there's money to be made.

Massive breaches: Exposure of national databases

Both the number of occurrences and the extent of incidents should be assessed when measuring the impact of security breaches. Although government sector security breaches as a percentage of breaches across all industries rose slightly this year, the previous three years saw a notable decline year by year: 14 percent in 2013 to 10 percent in 2014 to just 7 percent in 2015. The significance of the 2016 breaches isn't so much the rise in their number; it's their magnitude or impact, for example the exposure of entire national databases.

◄ Previous Next ►

According to IBM X-Force Security Incident Data, more than 200 million government records were compromised worldwide between January 1 and October 31 of 2016 (see Figure 1). That's nearly 60 million more than in the whole of 2013, 2014 and 2015 combined. As of October 31, 2016, the government sector ranks second among all industries in terms of records compromised.

Within 2016's massive batch of compromised records are several high-profile breaches of voter data. Most notably, over 93 million records containing Mexican voter data were exposed due to an improperly secured public-facing cloud database. Leaked data included names, parent names, voter identification numbers, addresses, dates of birth and other sensitive information.[3] In another huge breach, hacktivists in the Philippines posted over 300GB of voter data from the country's electronic elections website, affecting about half the population. Leaked data included email addresses, fingerprints, family history and other sensitive data.[4]

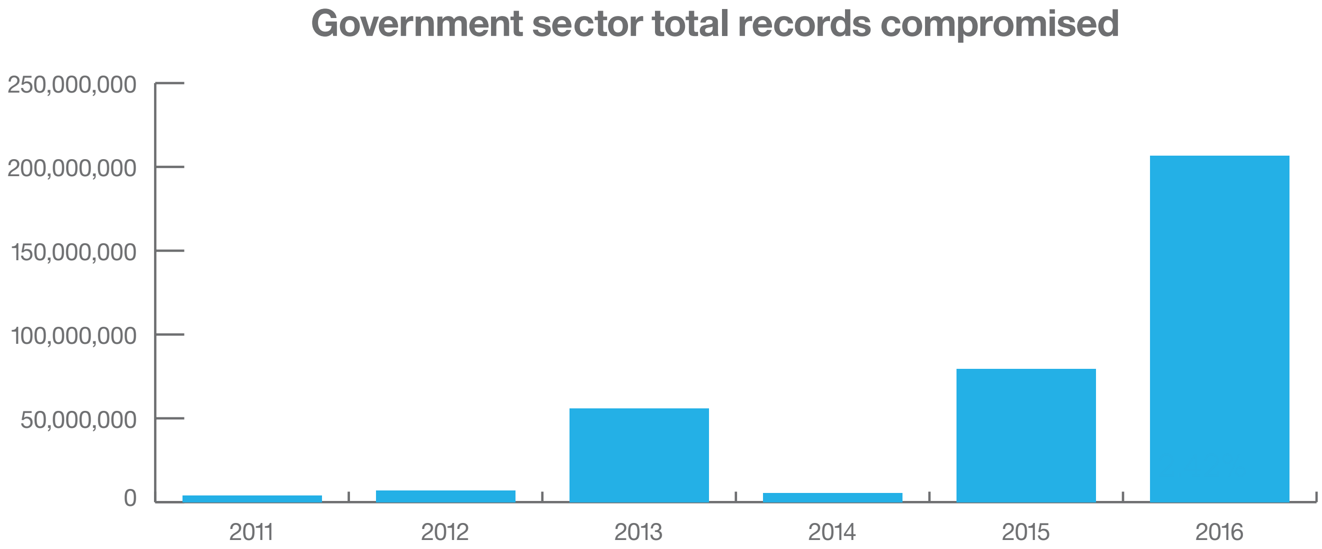


Figure 1. The total number of records compromised in government data breaches has increased substantially over the last five years. Source: IBM X-Force Interactive Security Incidents data, 2011 – October 31, 2016.

The list goes on. A voter database containing personal information of over half the population of Turkey was leaked to a web forum: names, addresses, national ID numbers, dates of birth and parent names.[5] Earlier in 2016, a security misconfiguration on a US political party website exposed the names, addresses, birthdates and voter information of over two million individuals.[6] One report indicated that more than 20 states have experienced attempts to gain unauthorized access to voter registration databases or other election-affiliated systems.[7]

Ransomware

Another way attackers profit from today's data-driven economy is through ransomware. Ransomware is malware that works by encrypting files and deleting the originals, thereby denying access unless a ransom is paid, or by simply locking a whole system and then selling the user a password to unlock it. Victims usually receive ransomware as an attachment to unsolicited email from an unknown sender, or it's injected into their browser session through a web browser vulnerability.

According to the United States Computer Emergency Readiness Team (US-CERT), ransomware is the fastest-growing malware threat, with more than 4,000 ransomware attacks occurring daily during the first half of 2016.[8] In March, the Department of Homeland Security (DHS) revealed that there had been over 300 incidents of ransomware on federal networks since June 2015.[9] One report released in September 2016 found that globally, ransomware in the government sector more than tripled over the previous twelve months.[10]

This threat is a global issue across all industries, and the government sector needs to focus on preparedness. IBM's Ransomware Response Guide helps organizations faced with needing to respond effectively to a ransomware incident.

◄ Previous Next ►

Security is a global problem

As Figure 2 illustrates, for several years now the US has been the clear leader in security incidents involving the compromise of government records. Given the sheer number of federal, state and local government organizations involved, that makes sense; in its last national census, in 2012, the U.S. Census Bureau found no fewer than 90,056 local governments in the United States.[11] More targets, more attacks. As to 2016's apparent surge in security incidents, it's possible that increased reporting played a part, the result of changes mandated for Federal Executive Branch agencies by the Office of Management and Budget (OMB).[12]

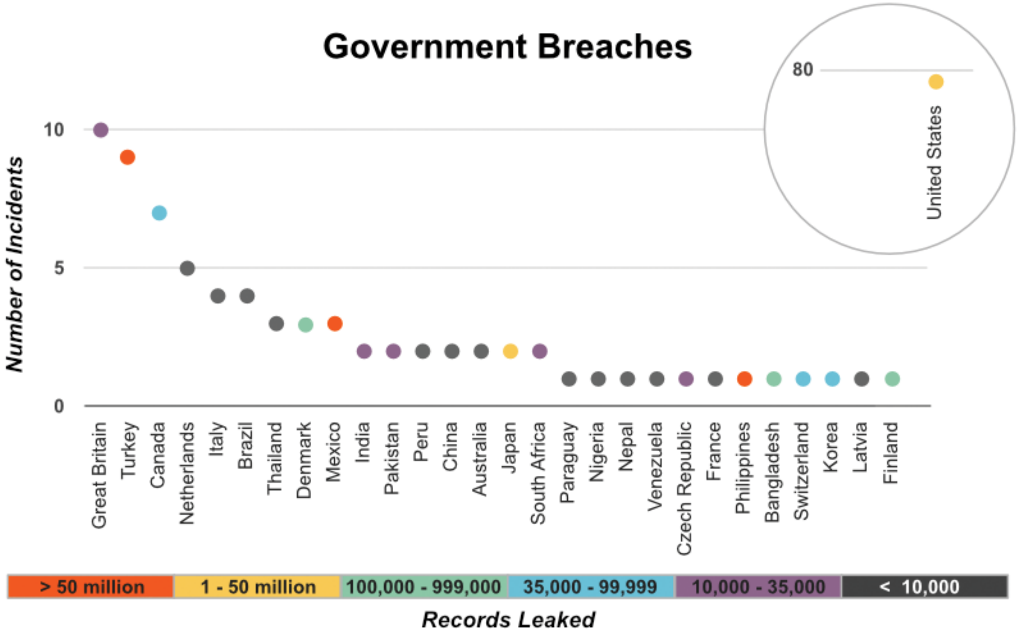


Figure 2. The United States led the world in the number of security incidents, but Turkey, Mexico and the Philippines all had a greater number of records leaked. Source: IBM X-Force Interactive Security Incidents data, 2011 – October 31, 2016.

◄ Previous Next ►

Contents

The issue of government breaches is certainly not unique to the US. It's a global problem with close to 100 reported incidents spanning 29 countries and six continents (see Figure 2). Government entities the world over have been the target of phishing, malware infections and SQL injection attacks, with compromised information including the national ID numbers, fingerprints, confidential documents, emails, passwords and credit card numbers of private citizens, current and former government employees, and military personel. Attackers use information stolen from such resources to conduct fraudulent and malicious activity for financial gain or to conduct state-sponsored attacks. A popular option is to take stolen information and put it up for sale on the Dark Web, as was the case with the breach of the U.S. Office of Personnel Management (OPM) in 2015.[13]

It must be noted that as worrisome as the known record of government breaches may be, it's quite possible, perhaps even likely, that known or reported breaches represent only a fraction of the number that have actually occurred. Whatever the truth of the matter, it's obvious that security is indeed a global agenda for all governments.

Government data breaches often involve compromising personally identifiable information, including national ID numbers, confidential documents, fingerprints and credit card numbers.

Prevalent attacks targeting the government sector

IBM Managed Security Services which monitors billions of security events reported every year by client devices in over 100 countries, analyzed the aggregate data accumulated between October 1, 2015, and September 30, 2016. This data provides insight into the daily cyber experience facing the government sector.

To be clear about our terminology in this section of our report, 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.

We focus on the top five attack categories targeting the government sector, which together account for close to 64 percent of total attack activity (see Figure 3). We also discuss the Tor network, since it came very close to the top five in attack volume.

Top five attack types targeting the government sector

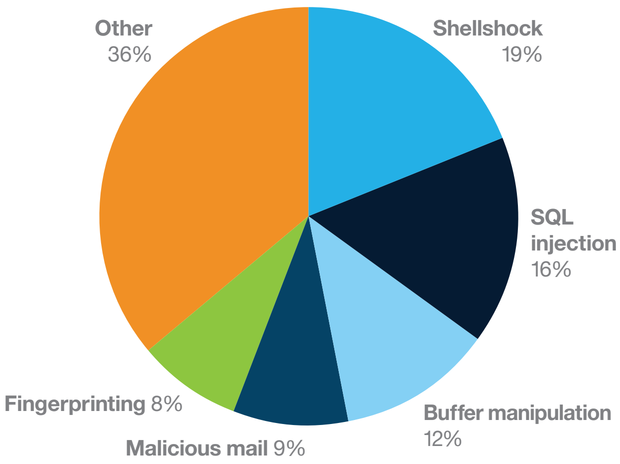


Figure 3. The top five attack types on government entity IT networks monitored by IBM. Source: IBM Managed Security Services, October 1, 2015 – September 30, 2016.

◄ Previous Next ►

Contents

Shellshock

Shellshock is a vulnerability in the GNU Bash shell widely used on Linux, Solaris and Mac OS systems. One of the threat game changers for 2014, it's still very prevalent. As if anticipating its two-year anniversary, Shellshock attack activity surged in September 2016 to levels not seen since 2015. It's not surprising, then, that it's the number one attack vector, accounting for nearly 19 percent of attacks in the government sector.

This "malware-less" attack vector, which has been likened to SQL Slammer in terms of persistence, is a threat to organizations across all industries, not just government. In fact, the government sector ranked eighth in 2016 at 1.65 percent of total Shellshock activity. Failure to apply patches and fixes leaves your organization at risk for Shellshock attacks. Timely patch management is vital in government organizations of any size.

SQL injection

SQL injection, which continues to be one of the most prevalent attack vectors being exploited across multiple industries, is government's number two attack vector at just over 16 percent. This attack attempts to pass SQL commands through a website in order to acquire the contents of databases not intended for public access. Attacks using this threat remain widespread, but in the past few years there has been a substantial decline in the number of SQL injection vulnerabilities disclosed by vendors, researchers and attackers—along with the associated exploit code made publicly available (see Figure 4). In fact, from 2011 to 2015 there was a 54 percent drop in the number of SQL injection vulnerabilities disclosed. The ratio of vulnerability to publicly available exploit code has also declined since its high in 2012. In 2012, just over 93 percent of the SQL injection vulnerabilities disclosed saw exploit code surface publicly. In 2015, the percentage of publicly available source code drops to approximately 81 percent of the total vulnerabilities disclosed in 2015.

◄ Previous Next ►

	2011	2012	2013	2014	2015
SQL injection vulnerabiiities disclosed	796	836	423	404	365
Percentage of vulnerabilities with publicly available source code	85.4%	93.1%	92.7%	80.7%	81.1%

Figure 4. Total number of SQL injection vulnerabilities disclosed yearly and the percentage of those with publicly available exploit code. Source: IBM X-Force Vulnerability Database.

Perhaps the decline in disclosures is the result of vendors incorporating better coding practices, or maybe attackers are spending more time researching “trendier” vulnerabilities like threats to the Internet of Things. Regardless, SQL injection remains a top attack vector, which points to its staying power. Because attackers are able to use older vulnerabilities and exploits to achieve their results, the decline in the number of SQL injection vulnerabilities should not be equated with a weakening of its use as an attack vector. To combat SQL injection attacks, it’s vital that organizations perform vulnerability scans on all applications, both off-the-shelf and homegrown, and teach programmers secure coding practices. Database administrators should implement proper database, table and even column security.

Buffer manipulation

In nearly 12 percent of the attacks IBM MSS observed in the government industry, the attacker was attempting to manipulate an application's interaction with a buffer, an area of physical memory storage used to temporarily store data while it’s being moved from one place to another.[14] This vector includes both overflow[15] and overread[16] buffer attacks. Successful exploitation of buffer vulnerabilities could allow an attacker to obtain sensitive information, cause a system crash or execute arbitrary code. As with SQL injection, targeting buffer vulnerabilities is a longtime favorite among attackers. And as with SQL injection, vulnerability scans are vital for defenders. Automated tools can help you detect and prioritize these types of threats.

Malicious mail

Just over nine percent of the government sector attacks involved malicious SMTP traffic. One such attack might consist of a phishing email containing an attachment that’s a known exploit. Another might involve a phishing email containing an attachment with a highly suspicious filename. For instance, several worms, such as the Nimda worm, use file names with a particular format to take advantage of a vulnerability in some versions of Microsoft Internet Explorer.

◄ Previous Next ►

Fooling victims into opening attachments is a popular attack vector across many industries. The intent is almost always to have the victim download malware. Because social engineering via spear phishing and other scams is often an attacker's first step in a successful compromise of this type, education is the key to effective defense. Consider implementing a phishing awareness campaign to help users identify phishing attacks. The IBM report The perils of phishing provides additional recommendations on how to thwart this threat.

Fingerprinting

Nearly eight percent of the attacks were a type often viewed as more of a pre-attack used to gather information on potential targets and discover existing weaknesses in them. Essentially, the attacker compares output from a target system to known "fingerprints" that uniquely identify specific details about the target, such as the type or version of its operating system or applications. That information can then be used to exploit known vulnerabilities in the target organization's IT infrastructure. Reportedly, this technique has also been used in malvertising campaigns.[17]

Your organization should monitor log files to identify which systems appear to be probing your systems. Additionally, many firewalls and intrusion detection/prevention systems can alert when an attack is detected.

Honorable mention: Attacks from the Tor network

Falling just outside the top five, the Tor network accounted for over seven percent of attacks targeting government IT networks. As the IBM paper Dangers of the deep, dark web describes, criminals often use the Tor network to launch attacks against targets on the surface web (the publicly accessible Internet). They also use it to hide, communicate and trade with each other without exposing the content of their transactions.

There are ways to prevent attacks coming from the Tor network and minimize their damage. Use web gateways, web proxies and intrusion detection systems to identify outgoing communication to anonymous networks. Block Tor exit nodes from communicating with your network. Additional recommendations can be found in the IBM report referenced above.

Most government attacks come from the outside

According to IBM's 2016 Cyber Security Intelligence Index, insiders were responsible for 60 percent of all attacks across all industry sectors in 2015, up from 55 percent in 2014. Interestingly, though, analysis of IBM Managed Security Services data for the period between October 1, 2015, and September 30, 2016, found that the majority of attacks against government IT networks—approximately 71 percent—came from outsiders, not insiders.

Why this divergent trend? One possibility is the role played by hacktivists, who are often malicious outsiders, in attacks targeting government organizations. According to IBM X-Force Interactive Security Incidents data, government ranked second in terms of the number of incidents associated with hacktivists since 2011, making up approximately 28 percent of the targets.[18]

While most cybercriminals are driven by profit, hacktivists' motivations are usually political or social. For instance, earlier this year the infamous hacktivist group Anonymous leaked over one terabyte (TB) of Kenyan government documents to the Dark Web in an attack reportedly associated with the OpAfrica initiative against child abuse, child labor and corruption in African countries.[19] The leaked documents included emails, trade agreements and other sensitive data, some of it classified.

Hacktivists may also choose to target a government entity via DDoS. In February, the DownSec group carried out DDoS attacks against Belgian government sites, including the Prime Minister's web page.[20] In 2015, a group calling themselves Vikingdom2015 targeted a number of state websites in the US and claimed responsibility for several DDoS attacks. Some sites remained offline for several days.[21]

Another possible explanation for the non-typical outsider/insider balance of attacks against government targets might be that government mitigates insider attacks better than other industries, for instance by more effectively monitoring employee activity to identify misuse and suspicious activities. Government organizations might also have robust access management tools and policies in place, and be more efficient at controlling the network privileges of individual employees as they change roles throughout their employment or leave the organization.

Insider threat may cause more damage

While more attacks against the government industry come from the "outside," the "inside" attacker can cause major damage. Although many insiders are not acting maliciously, such as those who may inadvertently download an infected attachment, other insiders may be bad actors. For example, insiders sponsored by a national government to perform cyber-espionage pose a significant threat not only to the targeted government institution but also to a nation's security and economy. The malicious insider's goals can vary widely, from relatively trivial web defacement to serious or even strategic destruction of critical infrastructure. Earlier this year, attackers reported to be state sponsored breached the computer network of a US political party and stole sensitive files and political intelligence.[22]

Often the insider is an employee of the organization, but he or she could also be a third party such as a business partner, client or maintenance contractor. Any of these individuals could also inadvertently introduce weaknesses in your security posture. Last year, a Japanese government employee opened a malicious email which led to a data leak of pension information for over 1.2 million citizens.[23]

Insider attackers who are sponsored by another national government can pose a significant threat to a nation's security and economy.

The path to achieving government security resilience

In the recent past, it seems, either the government sector has suffered significantly fewer data security breaches than the private sector, or government's breaches weren't all revealed. We just don't know. With the growing spotlight on government, several publicized breaches have demonstrated agencies' recognition of the need to improve data security. Following the breach on their systems, the U.S. Office of Personnel Management released a report identifying current and future actions to strengthen cybersecurity and protect critical IT systems. In May 2016, the General Data Protection Regulation (GDPR) was signed into law with the goal of strengthening and unifying data protection for citizens of the European Union (EU).

These are possible indicators of positive movement globally towards better government data security. We offer government organizations the following recommendations to help achieve that goal.

Data and application security

It's imperative that governments implement a comprehensive data security platform such as IBM® Security Guardium®. Look for a data security solution that can detect SQL injections and malicious stored procedures—identifying when a data repository attack is underway (whether it's an outside or inside attacker).

Since SQL injection holes in web servers and applications seem to be open doors to many government databases, a focus on application security is a must. Tools such as IBM Security AppScan® can reduce the likelihood of web application attacks and data breaches by automating application vulnerability testing and finding issues such as lack of input validation. Beyond open SQL injection vulnerabilities, these tools can help find other Open Web Application Security Project (OWASP) top 10 web application risks[24] before the application hits production.

Unfortunately, misconfiguration can make a "solid" or relatively secure app vulnerable. Examples abound: implementing a firewall rule such as `permit ip any WEB-SERVER1`, which allows all traffic from any source to a web server; or leaving an open port on a web server running; or granting the wrong permissions to a UNIX web server that allows for external or unapproved access to an app or service. System misconfigurations are one of the more common forms of human error resulting in inadvertent insider threats.[25] We recommend reviewing the recommendations on preventing security misconfiguration at OWASP.org.

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. That 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 really work. Perhaps most importantly, the company must disable all 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.

Participate in a trusted cyber threat information-sharing network

It's essential for government entities 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.

Timely communication within your organization on threats and security recommendations goes a long way to protecting government 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.

Adapt to the cognitive era

A 2015 IBM survey found that 83 percent of government leaders familiar with cognitive computing believe it will have a critical impact on the future of their business.[26] Cognitive systems, such as Watson for Cyber Security, provide the means to mine both structured and unstructured data and interpret this data. Governments have constrained budgets, which puts them in the position of competing for valued resources. They are continually challenged to improve program outcomes, optimize service delivery and strengthen security, safety and resilience.

Cognitive security can not only help address the current skills gap and accelerate responses, but also help reduce the cost and complexity of dealing with cybercrime, freeing up budget resources to focus on other needs.

The government sector's road to cyber resilience is fraught with challenges, but the goal of better cyber hygiene is achievable. By improving data and application security, mitigating insider threats, incorporating cyber intelligence and leveraging cognitive and machine learning, government organizations can significantly enhance their ability to prevent or handle cyber incidents.

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. Penetration Testing from IBM X-Force Red can help you determine weakness in your IT systems and strengthen your defenses. 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.

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 3,500 security patents.

◄ Previous Next ►

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.

Contributor

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

◄ Previous Next ►

Contents

References

[1] www.gao.gov/assets/680/6772a93.pdf

[2] http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

[3] https://mackeeper.com/blog/post/217-breaking-massive-data-breach-of-mexican-voter-data

[4] http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/

[5] https://www.wired.com/2016/04/hack-brief-turkey-breach-spills-info-half-citizens/

[6] http://www.engadget.com/2016/02/04/iowa-gop-website-exposes-voter-records/

[7] http://www.cnn.com/2016/10/31/politics/election-2016-cyber-threats-states-request-help/index.html

[8] https://www.us-cert.gov/sites/default/files/publications/Ransomware_Executive_One-Pager_and_Technical_Document-FINAL.pdf

[9] https://fcw.com/articles/2016/03/30/ransomware-carper-hsgac.aspx

[10] https://www.bitsighttech.com/press-releases/new-research-shows-ransomware-is-not-just-in-healthcare

[11] http://www2.census.gov/govs/cog/g12_org.pdf

[12] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

[13] http://securityaffairs.co/wordpress/37803/cyber-crime/opm-data-dark-web.html

[14] https://en.wikipedia.org/wiki/Data_buffer

[15] https://capec.mitre.org/data/definitions/100.html

[16] https://capec.mitre.org/data/definitions/540.html

[17] http://betanews.com/2016/03/02/malvertising-fingerprinting/

[18] https://securityintelligence.com/hacktivism-fearmongering-or-real-threat/

[19] https://www.hackread.com/anonymous-hacks-kenya-ministry-foreign-affairs/

[20] http://www.politico.eu/article/belgium-government-agencies-plagued-hackers-downsec-ddos-attacks-cyber-crime/

[21] http://uk.businessinsider.com/vikingdom2015-anonymous-hacking-group-threatens-gov-websites-2015-3?r=US

[22] https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html

[23] http://www.japantimes.co.jp/news/2015/06/02/national/social-issues/japan-pension-service-hack-used-classic-attack-method/#.WD87DX2WLmM

[24] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[25] https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/

[26] http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=XB&htmlfid=GBE03714USEN

◄ Previous Next ►

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
December 2016

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.