IBM Security

Reviewing a year of serious data breaches, major attacks and new vulnerabilities

Analysis of cyber attack and incident data from IBM's worldwide security services operations

IBM X-Force® Research
2016 Cyber Security Intelligence Index

IBM

Click here to start ►

Contents

2015 in brief

- **Your next attacker is likely to be someone you thought you could trust.** Insider threats continue to pose the most significant threat to organizations everywhere.
- **IBM found 64 percent more security incidents in 2015 than in 2014.** Improvements in detection and policy refinement made that possible.
- **Healthcare became the most frequently attacked industry.** A significant increase in attacks rocketed healthcare straight past financial services and manufacturing.

Methodology

IBM Security Services continuously monitors billions of events per year, as reported by more than 8,000 client devices in over 100 countries. This report is based on data IBM collected between 1 January 2015 and 31 December 2015. The data has been normalized to account for differences in our clients’ infrastructures across industries and company size.

The annual IBM® X-Force® Research Cyber Security Intelligence Index offers a high-level overview of the major threats to our clients’ businesses worldwide over the past year, and is complemented by other threat intelligence and research publications from IBM X-Force. Our goal is to help you better understand the current threat landscape by offering a detailed look at the volume of attacks, the industries most affected, the most prevalent types of attacks and attackers, and the key factors enabling them. We provide insights into where and how successful attacks can impact today’s technology-dependent organizations. We also discuss how the threat landscape is changing from year to year, as IBM works with companies to help them better detect and insulate themselves from attacks. By continuously “tuning” our threat monitoring algorithms to reflect what we learn in the course of our work, we’re able to provide our clients with a well-informed view of the cyber security landscape as it evolves throughout the year.

Contents

Cyber security becomes a way of life

The year 2015 was filled with serious data breaches, major attacks and an ever-flowing stream of new vulnerability reports—across the entire industry. And while financial gain is still a powerful motivator for cyber criminals, it’s by no means the only one. Last year’s attackers branched out in a big way—inflicting physical damage, stealing intellectual property and lodging political protests.

In particular, a previously reported vulnerability known as Shellshock played a major role in many of last year’s attacks. A flaw in the Bash shell (widely used on Linux, Solaris and Mac OS systems), Shellshock has been around for more than 20 years, but wasn’t disclosed until over a year ago.

Our data for 2015 indicates that Shellshock was behind last year’s surge in unauthorized access attacks—defined by our analysts as encompassing various types of attempts to break into a network, a server or a database, such as exploiting a vulnerability to inject command code into software, exploiting a backdoor, or bombarding a system with random passwords in hopes that one will work.

Looking at the big picture, it’s clear that virtually no industry was immune to the exploits of today’s attackers. However, some industries were targeted far more frequently than others. In 2015, the most targeted industries included healthcare, manufacturing and government organizations around the world—all of which found themselves featured in boldface headlines and scrambling to respond.

Last year’s attackers branched out in a big way—inflicting physical damage, stealing intellectual property and lodging political protests.

Contents

Cyber security by the numbers

In 2015, the average client organization monitored by IBM Security Services experienced approximately 53 million security events annually (see Figure 1). As you can see, that's roughly 28 million—or 35 percent—fewer events than our clients experienced in 2014. Before discussing what this sizable difference means, let's point out that these events or "episodes" are detected by a security device or application on a given system or network that's being monitored by IBM Security Services.

Note that the vast majority of security events can actually be designated as "noise," or extremely low priority traffic. From one year to the next, as the technology supporting security devices improves and analysts continue to fine-tune the policies to which they react, the noise lessens. Additionally, it sometimes happens—as it did in 2014, with an onslaught of attacks on Heartbleed and Shellshock vulnerabilities—that we can attribute a sizable difference in event traffic to one or two specific situations.

At the same time, our average client company experienced 1,157 attacks in 2015, down significantly from 12,017 the year before. We define attacks as those security events that have 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.

Yes, that's a truly sizable drop. We should point out that it reflects specific and continually optimized policy tuning on the part of IBM security analysts, which allowed for far greater efficiency on all levels, cancelling out the "noise" created by false-positive traffic and making it possible for analysts to shift their attention to those events and attacks meriting further analysis. In other words, the world's cyber criminals did not take a break last year.

More importantly, our average client company was found to have experienced 178 security incidents in 2015, up 64 percent from the 109 that were discovered in 2014. The most serious of the three classifications we use, a security incident is an attack or security event that has been reviewed by IBM security analysts and deemed worthy of deeper investigation. The IBM X-Force Incident Response Team notes that of all the security incidents it works through and analyzes, only three percent actually reach a level of severity high enough to consider them "noteworthy"—and most of those commonly result in data disclosure or theft. That being said, we have unquestionably seen a significant rise in cyber crime attempts among our worldwide client base.

Contents

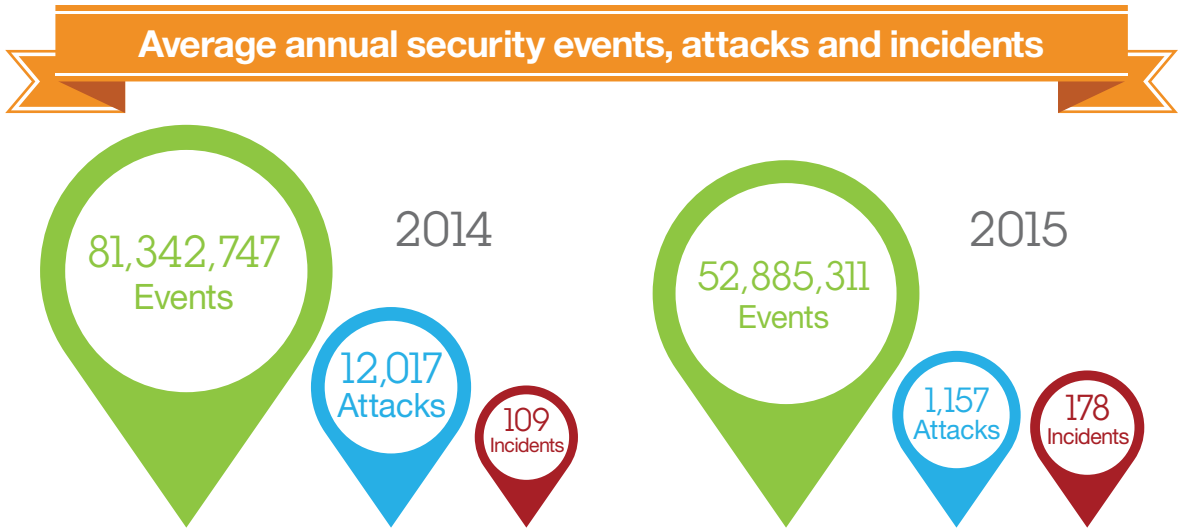

Figure 1. Security events among our clients can appear in many guises and, sometimes, extremely high volume. IBM Managed Security Services highly skilled intelligence and operations teams work to translate those event and attack counts into actionable data and keep it from overwhelming our clients, while allowing them to focus their efforts on more critical issues.

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.

Contents

Revisiting the five most-attacked industries

The industry-focused data for 2015 shows some interesting differences from what we saw for 2014 (see Figure 2). It also reflects a change in the methodology we use to determine which industries were the most frequently targeted. Previously, we based our determinations solely on the number of security incidents experienced by each industry. For 2015, however, we incorporated each industry’s attack counts as well. As a result, we believe that we’ve improved the accuracy with which we can report how frequently each industry is being targeted. Here are the highlights:

- **Healthcare** broke back into the top five rankings for 2015, shooting directly to the top spot. That comes as little surprise to us, after we coined 2015 “The year of the healthcare breach.”[1] The healthcare industry once sat firmly on the sidelines of the cyber war, watching breaches and malicious attacks wreak havoc elsewhere.

But that’s no longer the case. Five of the eight largest healthcare security breaches since the beginning of 2010—those with more than one million records reportedly compromised—took place during the first six months of 2015. In fact, over 100 million healthcare records were reportedly compromised in 2015.[2]

Packed with a wealth of exploitable information, electronic health records fetch a high price on the black market. They typically contain credit card data, email addresses, social security numbers, employment information and medical history records—much of which will remain valid for years, if not decades. Cyber thieves are using that data to launch spear phishing attacks, commit fraud and steal medical identities.

Five of the eight largest healthcare security breaches since the beginning of 2010—those with more than 1 million records reportedly compromised—took place during the first six months of 2015.

Contents

- **Manufacturing,** which includes automotive, electronics, textile and pharmaceutical companies, moved into second place in 2015, despite the fact that no particularly large-scale attacks struck the industry. It is worth noting, however, that automotive manufacturers were the top targeted manufacturing sub-industry, accounting for almost 30 percent of the total attacks against the manufacturing industry in 2015. There was also a lot of automotive industry interest generated in early 2015, when security researchers disclosed that attackers could remotely hack a "connected" car.[3]

  Chemical manufacturers were the second-most targeted sub-industry in 2015. Note, however, that although a cyber attack targeting the safety of a chemical plant or connected car could be devastating, many attackers are more financially motivated and therefore more likely to go after corporate networks—where they could steal potentially valuable intellectual property or sensitive information.[4]

- **Financial services** dropped from first place in 2014 to third place in 2015, due in large part to a significant increase in attack activity in the healthcare and manufacturing sectors—and, to some extent, as a result of our ability to refine and improve our monitoring and detection capabilities over time. In addition, the industry has been making its own strides to bolster cyber security, in reaction to major breaches over the past several years.

  On the consumer side of the financial services business, it's important to recognize that some of the very conveniences that banks now routinely offer customers—including automated teller machines, credit cards and mobile banking apps—have introduced a level of accessibility that goes a long way toward making the financial system highly vulnerable to cyber attacks. At the same time, many commercial banking clients fell victim to the Dyre and Dridex Trojans, which were responsible for a large number of multi-million dollar heists targeting enterprises last year.

  The number of breaches in the financial services industry that involved extortion tactics or theft of currency rose considerably—by 80 percent—in 2015. As for technical methods, together the attacks related to malicious attachments or links and Shellshock made up nearly 38 percent of those targeting financial institutions in 2015.

Contents

- **Government** agencies moved up into fourth place in 2015, coinciding with news reports of a number of high-visibility breaches—including one in the US that exposed millions of employee records containing non-expiring data such as social security numbers, place of birth and even digitized fingerprints.

  In early 2015, more than 50 million Turkish citizens found themselves at risk for identity theft when their national identity information was leaked from a government database. And more than a million Japanese citizens were exposed when employees at the pension service were tricked into opening a malicious email attachment that resulted in a data breach of sensitive, private information.

- **Transportation** was the fifth-most attacked industry in 2015. It includes everything from airlines, bus, subway and commuter rail lines to overland freight lines and overseas container ships that transport goods all around the globe. In many ways, this industry serves as the backbone of world trade, since without it, global economies could easily collapse.

  Politically motivated cyber criminals regularly attempt to bring the transportation industry to its knees in order to produce mass chaos scenarios. Meanwhile, others are motivated solely by financial gain. In 2015, both malicious code and Shellshock attacks accounted for nearly 36 percent of the total security attacks, followed by denial of service attacks at 16 percent.

Politically motivated cyber criminals regularly attempt to bring the transportation industry to its knees in order to produce mass chaos scenarios.

Contents

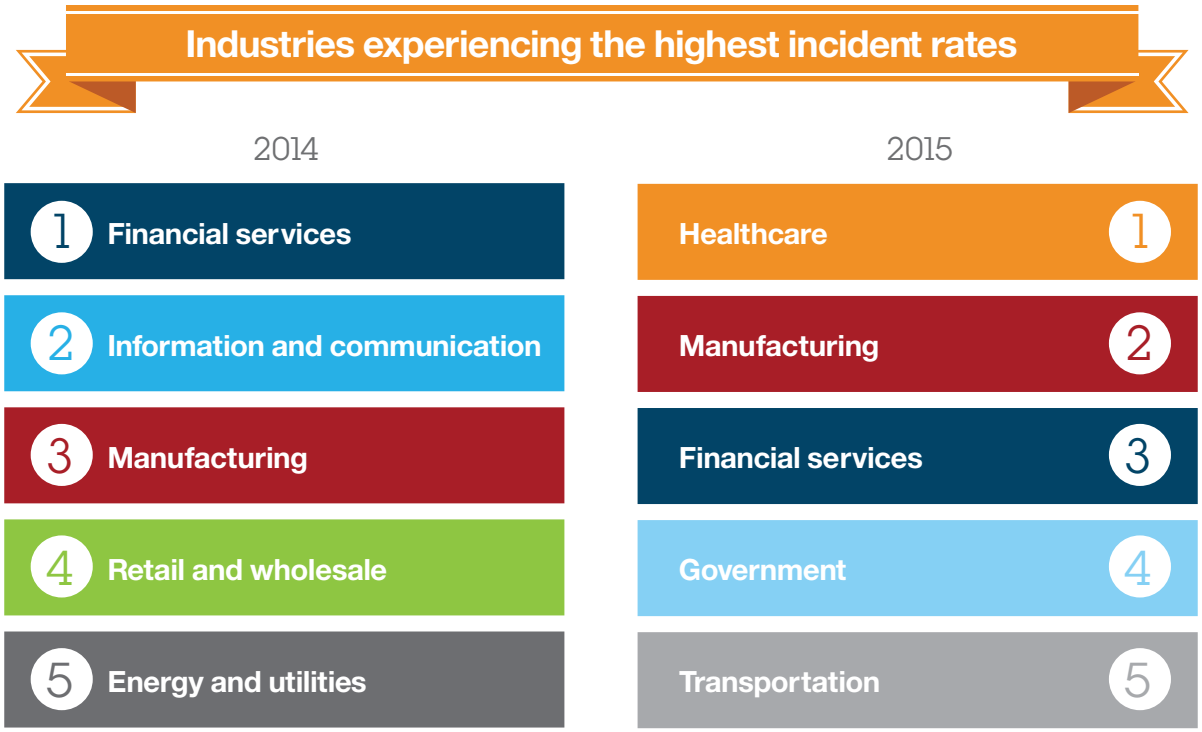

Figure 2. Healthcare moved into the top spot of the rankings as the most-attacked industry in 2015, replacing financial services, which dropped to third place. Second place went to the manufacturing industry, while government and the transportation industry took over fourth and fifth places, respectively.

Contents

Unauthorized access incidents become even more dominant

It became clear in 2015 that unauthorized access has taken hold as the leading cause of incidents across our clients' security incident landscape (see Figure 3). While malicious code and sustained probes or scans dominated the scene in both 2012 and 2013, unauthorized access incidents rocketed to the top in 2014, accounting for 37 percent of the total. That figure rose to 45 percent in 2015—thanks, in part, to Shellshock-related attacks—far outpacing malicious code.

At the same time, the incidence of sustained probes or scans dropped from 20 percent in 2014 to 16 percent in 2015. Scans can make it easy for target organizations to notice they're being attacked—and take action before the attackers can get what they want. So it's possible that attackers have backed off this approach, in favor of conducting more targeted attacks—by exploiting vulnerabilities or launching spear phishing campaigns, for example.

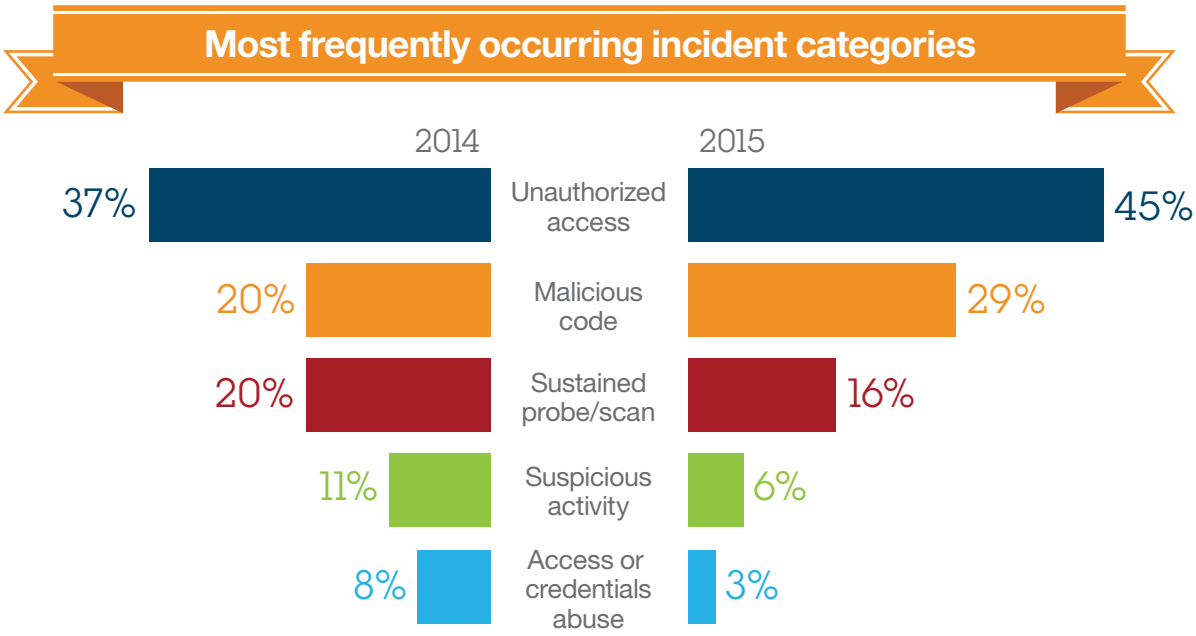

Figure 3. In 2015, unauthorized access once again topped the list of incident categories affecting the top five industries named in this report.

Contents

Sixty percent of all attackers are "insiders"

We'd all like to think that the people who work for us—including employees, contractors and consultants—are "good guys." And the truth is, most of them are. But in 2015, 60 percent of all attacks were carried out by insiders, either ones with malicious intent or those who served as inadvertent actors (see Figure 4). In other words, they were instigated or initiated by people you'd likely trust. They can pose a significant threat, resulting in substantial financial and reputational losses.

What's an insider? An insider, in this case, is anyone who has physical or remote access to a company's assets. Those are tangible items—including hard copy documents, disks, electronic files and laptops—as well as non-physical assets, such as information in transit. Although the insider is often an employee of the company, he or she could also be a third party. That includes business partners, clients or maintenance contractors, for example. They're individuals you trust enough to allow them access to your systems.

It's difficult to think of your employees as a potential "threat." And thankfully, while the great majority of them pose no threat whatsoever, we know that at least some of them do. The problem, of course, is that you don't know which ones. What's more, these insiders typically have insights into your company's weaknesses—along with potential access to "insider-only" data. That can allow them an obvious opportunity, since it's unlikely they need to bypass protection systems to obtain or leak sensitive information because they already have access.

Interestingly, this year's data revealed that while insiders were responsible for 60 percent of all attacks in 2015, up from 55 percent in 2014, roughly one-third of those attacks were carried out by inadvertent actors in 2015, compared with nearly one-half the previous year. Inadvertent actors are typically well-meaning employees (or other insiders) who either mistakenly allow an attacker access to your data or fail to pay attention to your company's cyber security policies. For example, an inadvertent actor might be someone who is duped in a phishing scam or lured into opening a malware-laden email attachment. In other words, it's not likely they were acting with criminal intent. What's more, a reduction in the number of attacks attributed to inadvertent actors could mean that more organizations are implementing security policies and employee education—and that they're doing a better job of communicating what's expected and why it's important.

Contents

On the other hand, there's no denying the level of danger posed by insiders who set out to take advantage of the organization for which they work. It's more difficult to thwart their intentions because they're willing to take significant risks to circumvent access controls and are typically unconcerned with corporate policies or the potential consequences of their actions.

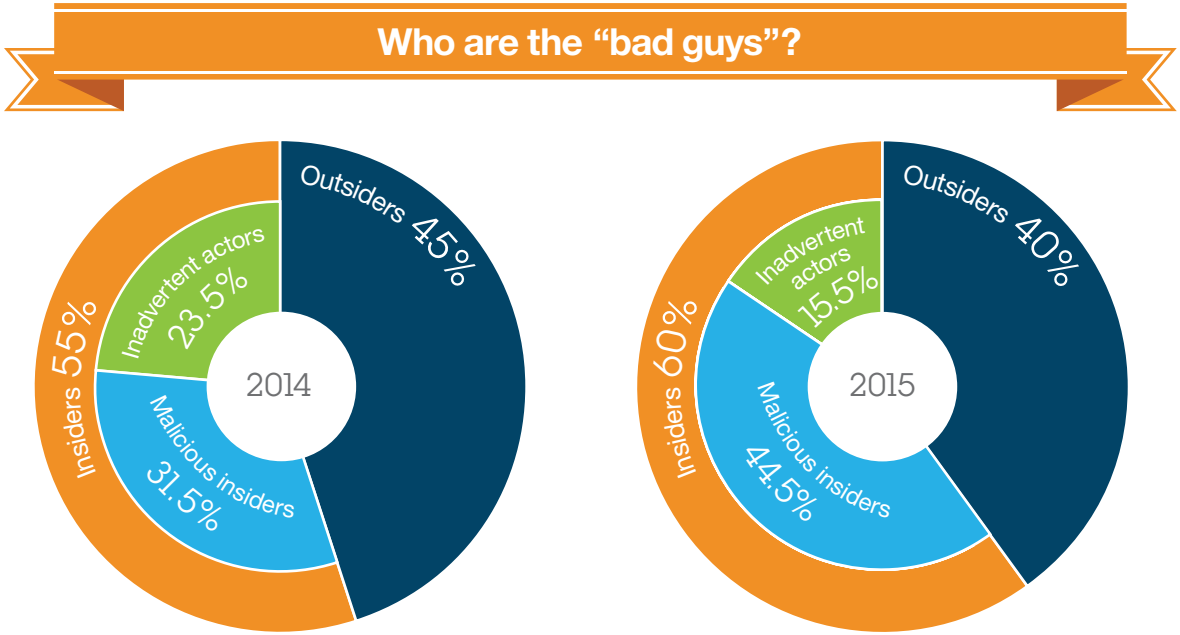

Figure 4. In 2015, outsiders were found to be responsible for 40 percent of the attacks recorded, while 60 percent of attacks were carried out by those who had insider access to organizations' systems.

Contents

One more look at the numbers

Taking one more look at our findings for 2015, we’ve found that some of the numbers we’ve discussed bear repeating. Our average client company experienced 178 security incidents in 2015, up 66 percent from the 109 that took place in 2014. Do the math and you’ll see that nets out to roughly 3.4 incidents per week, up from 2 per week in 2014.

It’s easy to look at those numbers and convince yourself that yours isn’t the “average” company. Your organization is too big, or too small, or too specialized to be considered average. Besides, you’ve got some pretty decent safeguards in place. And the people who work there wouldn’t hurt a fly—let alone do anything that could lead to a security breach.

It’s easy to think all those things. It’s more difficult to face the reality that your organization may already have been breached, or may even be under attack at this very moment.

Our team of highly skilled security professionals is constantly identifying and analyzing new threats, often before they are even known by the world at large.

Contents

Outthink threats

Organizations of all sizes are at risk, as are those in all industries. For better or worse, yours is no exception.

When it comes to cyber security, every company needs a strategy. And security leaders are now realizing that neither “checking the box” to address compliance requirements, nor conducting annual penetration testing and incident response exercises are by themselves are sufficient approaches. Today’s CISOs and security leaders are now looking for fundamental ways to influence and improve both their own programs and established best practices—because they know that simply being compliant isn’t acceptable for a well-governed organization. Here are four key steps you can take toward developing a strategic cyber security program:

- **Prioritize your business objectives and set your risk tolerance:** Striking a balance between protecting data assets and enabling productive, innovative workplaces has challenged security professionals for decades. The truth is, there’s no such thing as 100-percent secure. That means you need to make hard decisions about the different levels of protection required for different parts of the business.
- **Protect your organization with a proactive security plan:** Awareness is essential to security planning. Understanding the threat landscape, and actively working to protect your organization against those threats, requires both technology and policy.
- **Prepare your response to the inevitable, a sophisticated attack:** With the constant evolution of advanced persistent threats—and a growing presence of hackers intent on finding a vulnerability—it’s fairly certain that your organization may eventually fall victim to a data breach. Having a coordinated and tested incident response plan is critical at a time like this, as is access to the right resources and skills.
- **Promote and support a culture of security awareness:** All it takes is one careless employee to undo a chief security officer’s master plan. That’s why every employee must work in partnership with security professionals to help ensure that the safety of critical data is built into the culture of the organization.

Doing so will help you understand and prepare to deal with the real risks facing your organization.

Contents

Why IBM Security?

Traditional security defenses are no match for today’s unrelenting, well-funded attackers, while disruptive technologies introduce new vulnerabilities to exploit. Organizations must accelerate their ability to limit new risk and apply intelligence to stop attackers—regardless of how advanced or persistent they are. New analytics, innovation, and a systematic approach to security are necessary. And there are very few companies able to meet those requirements on their own. Gartner has named IBM a Leader in the Magic Quadrant for Managed Security Services (MSS), Worldwide for its ability to execute and completeness of vision.[5]

When you engage with IBM for managed services and consulting security expertise, you gain access to a full suite of capabilities that can help you extend protection from the back office to the front office. We also help ensure that it’s all integrated and coordinated end-to-end across your enterprise.

At IBM, our IT security services can cover every corner of your network, from infrastructure to applications to devices. We monitor, in near real time, some of the most complex corporate networks in the world. We develop some of the most sophisticated testing tools in the industry, many of which are used by our competitors. And our team of highly skilled security professionals is constantly identifying and analyzing new threats, often before they are even known by the world at large. In fact, we maintain one of the largest single databases of known cyber security threats in the world.

Contents

IBM Security

Authors

This report was created by the IBM X-Force research team. Dedicated to delivering industry-leading cyber threat intelligence, the group works diligently to keep IBM clients informed and prepared for the latest cybersecurity threats.

Nicholas Bradley, Practice Lead, Threat Research Group, IBM Managed Security Services

Michelle Alvarez, Threat Researcher and Editor, Threat Research Group, IBM Managed Security Services

David McMillen, Senior Threat Researcher, IBM Managed Security Services

Scott Craig, Threat Researcher, IBM Managed Security Services

For more information

To learn more about how IBM can help you protect your organization from cyber threats and strengthen your IT security, contact your IBM representative or IBM Business Partner, or visit this website: **ibm.com**/security/services

Follow us

[1] “Security trends in the healthcare industry,” IBM X-Force Research Managed Security Services Report, November 2015.

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

[3] “Driving security, Cyber assurance for next-generation vehicles,” IBM Global Business Services, Executive Report, June 2014.

[4] “Know Your Enemy: Understanding the Motivation Behind Cyberattacks,” Lyndon Sutherland, IBM Security Intelligence, March 31, 2016.

[5] Gartner Magic Quadrant for Managed Security Services, Worldwide, December 2015.

IBM

Contents

Glossary

Term	Definition
Access or credentials abuse	Activity detected that violates the known use policy of that network or falls outside of what is considered typical usage.
Attacks	Security events that have been identified by correlation and analytics tools as malicious activity attempting to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. Security events such as SQL Injection, URL tampering, denial of service and spear phishing fall into this category.
Breach or compromise	An incident that has successfully defeated security measures and accomplished its designated task.
Denial of service	Attempts to flood a server or network with such a large amount of traffic or malicious traffic that it renders the device unable to perform its designated functions.
Droppers	Malicious software designed to install other malicious software on a target.
Event	An event is an observable occurrence in a system or network.
Inadvertent actor	Any attack or suspicious activity sourcing from an IP address inside a customer network that is allegedly being executed without the knowledge of the user.
Incidents	Attacks and/or security events that have been reviewed by human security analysts and have been deemed a security incident worthy of deeper investigation.
Keyloggers	Software designed to record the keystrokes typed on a keyboard. This malicious software is primarily used to steal passwords.
Malicious code	A term used to describe software created for malicious use. It is usually designed to disrupt systems, gain unauthorized access or gather information about the system or user being attacked. Third-party software, Trojan software, keyloggers and droppers can fall into this category.

Contents

Term	Definition
Outsiders	Any attacks that are sourced from an IP address external to a customer’s network.
Phishing	A term used to describe when users are tricked into opening an infected email attachment or browsing to a malicious website disguised as a trusted destination where they provide information that can be used to access a system or account or steal their identities.
Security event	An event on a system or network detected by a security device or application.
Security device	Any device or software designed specifically to detect and/or protect a host or network from malicious activity. Such network-based devices are often referred to as intrusion detection and/or prevention systems (IDS, IPS or IDPS), while the host-based versions are often referred to as host-based intrusion detection and/or prevention systems (HIDS or HIPS).
Spear phishing	Phishing attempts with specific targets. These targets are usually chosen strategically in order to gain access to very specific devices or victims.
SQL injection	An attack that attempts to pass SQL commands through a website in order to elicit a desired response.
Suspicious activity	These are lower priority attacks or suspicious traffic that could not be classified into one single type of category. These are usually detected over time by analyzing extended periods of data.
Sustained probe/scan	Reconnaissance activity usually designed to gather information about the targeted systems such as operating systems, open ports, and running services.
Trojan software	Malicious software hidden inside another software package that appears safe.
Unauthorized access	This usually denotes suspicious activity on a system or failed attempts to access a system by a user or users who do not have permission.
Zero-Day	An unknown vulnerability in an application or a computer operating system.

Contents

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
April 2016

IBM

SEW03133-USEN-01