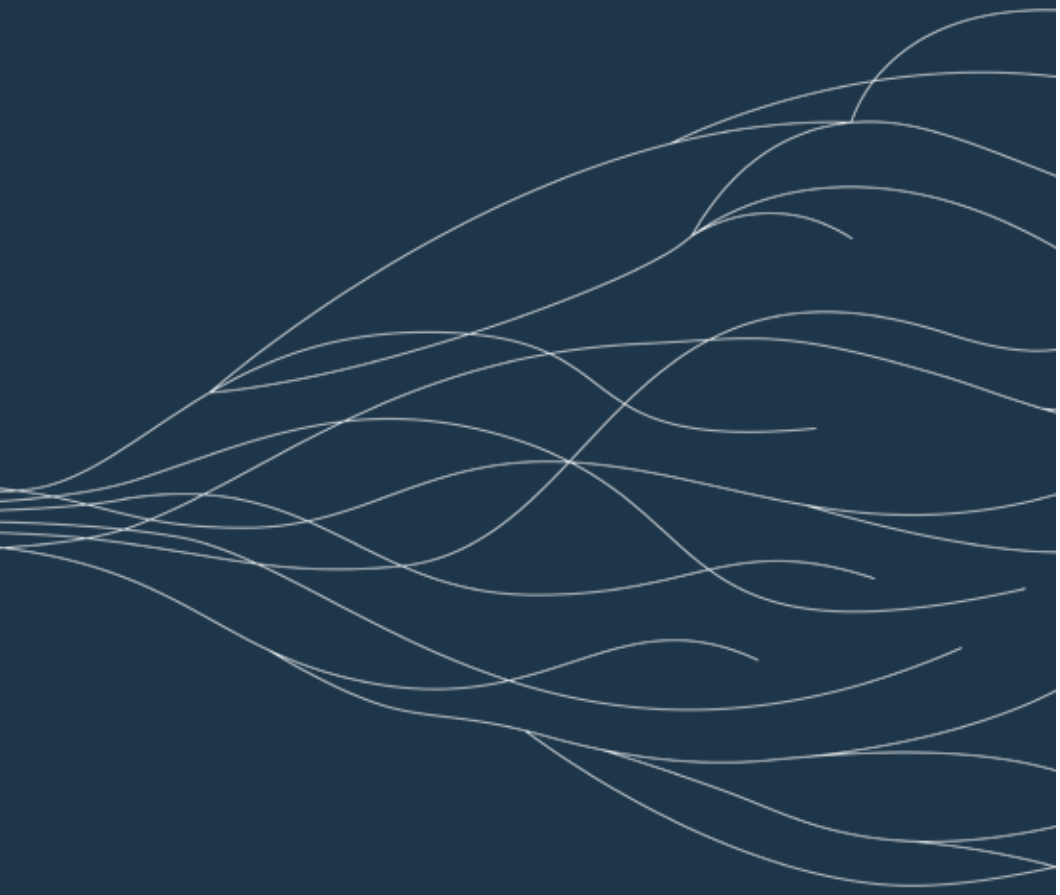

IBM Security

Security trends in the healthcare industry

Data theft and ransomware plague healthcare organizations

IBM X-Force® Research

IBM

Click here to start ►

Contents

Executive Overview

The healthcare industry got a significant wake-up call in 2015. The first six months of that year saw 62 percent of the largest healthcare security breaches—those with more than a million records compromised—of the last five years.[1] In 2016 the volume of compromised records was not as great, but breaches continued to cause operational, financial, and reputational damage to healthcare industry organizations, and in fact the number of breaches rose. A total of 320 breaches involving unsecured protected health information (PHI) were posted by the U.S. Department of Health and Human Services Office for Civil Rights Breach Portal, an increase of 18.5 percent over 2015.[2]

Why are attackers continuing to sharpen their focus on healthcare? It's because the exploitable information in an electronic health record (EHR) brings a high price on the black market. In the past, malicious vendors have touted an EHR as being worth $50,[3] but IBM X-Force researchers have found that these days, with health records often combined for sale in the underground markets with other personal/financial data, the price may be even higher.

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

Contents

Figure 1 shows an ad for such a combination, asking USD69.99 for full payment card data—"Fullz" in fraudster jargon—for an impressive package of document scans including medical and health insurance information. Spear phishing, financial fraud and medical identity theft are just a few of the ways attackers can use such data for monetary gain.

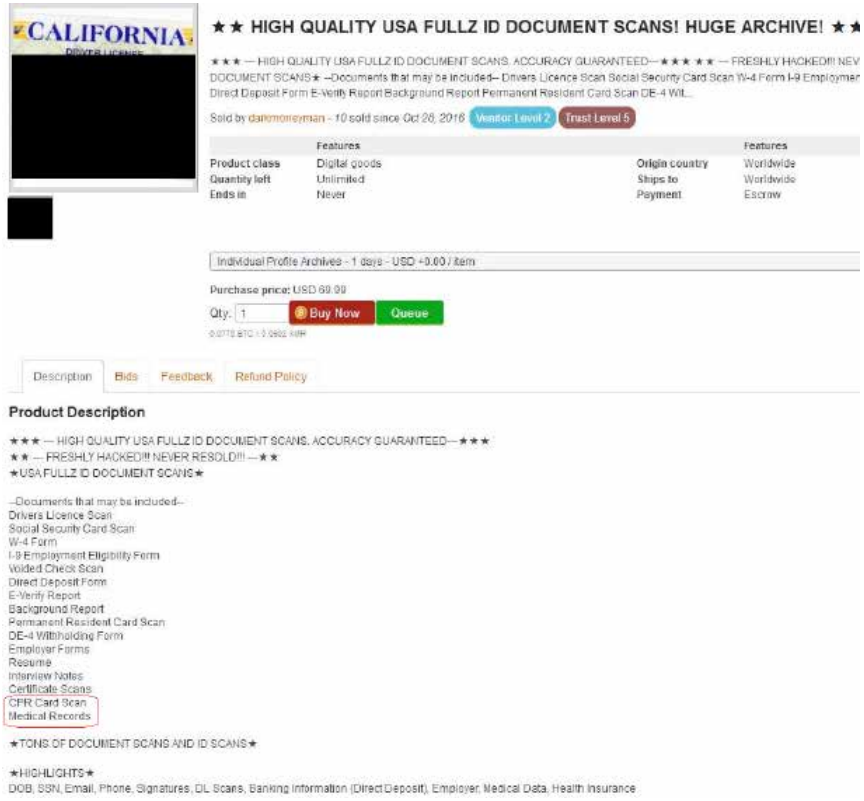

Figure 1. Screenshot of record for sale on the dark web. Source: IBM Security research.

Contents

Healthcare data at rising risk

Attackers' costs may be rising, but for the victim it's much worse. According to the 2016 Cost of a Data Breach Study, the healthcare industry's data breach cost, $355 per record, is more than twice the mean across all industries of $158 per record. Despite being under constant pressure to lower the cost of healthcare to consumers, healthcare organizations simply cannot afford to make cyber security a low business priority and risk multi-million-dollar losses to a hard-hitting attack.

It is safe to say that costs to healthcare organizations will continue to rise as one of the fastest-growing threats, ransomware, successfully wreaks havoc in the industry. An IBM survey released in December 2016 found that 70 percent of business executives with experience of ransomware attacks had paid to get data back, with more than half paying over $10,000 and one in five paying more than $40,000. Ransom demands are likely to increase in 2017.

Ransomware and the cost of breaches aren't the only threats. Another concern, outlined in our 2016 Security trends in the healthcare industry report, is the introduction of risk from the Internet of Things (IoT), mobile health apps and cloud. As the healthcare industry continues to accelerate the transformation of its IT infrastructure, the need for adequate security increases apace. And the pace is dramatic. For example, in just two short years, the number of US hospitals providing patients with the ability to digitally view, download and transmit their health information jumped from just 10 percent in 2013 to 69 percent in 2015.[4]

Between ransomware, data breaches and the risks posed by IoT and consumer access to electronic health information, the healthcare industry is under attack.

Contents

According to one report released in 2015, EHRs had replaced more than 80 percent of paper-based health records in established markets and up to 40 percent in emerging markets.[5] In Canada the availability of digital consumer health services more than doubled in two years,[6] and in Australia the Australian Digital Health Agency was created in July 2016 to drive the development and delivery of the nation's digital health.[7] Those are just a few examples of how technology is increasingly being used to enhance healthcare information accessibility across the globe. Along with the potential benefits of digital EHR implementation, however, come potential risks, many of which can materialize through indirect compromise such as third-party EHR vendor breaches.

Insider threat remains a serious concern, with IBM Managed Security Services (MSS) data for 2016 showing that 68 percent of all network attacks on healthcare organizations were carried out by insiders.

Unsurprisingly, the number one attack vector involved the use of malicious data input from bad actors to attempt to control or disrupt the behavior of target systems. With the increasing black-market value of healthcare records packaged into full individual profiles, attackers will increasingly set their sights on the healthcare industry. Healthy security is now a necessity. More than ever, there is an urgent need for organizations to transform a point product-based set of security solutions into an integrated security immune system.

Contents

Healthcare records up for ransom

Ransomware flourishes. Security incidents involving this malware are expected to continue rising in 2017,[8] and it was one of the top security threats in 2016. For example, the criminals responsible for distributing the now infamous Locky ransomware[9] focused on the healthcare industry early in the year. Numerous reports of incidents involving the malware surfaced globally in February, the targets including a New Zealand health board[10] and several hospitals in Germany.[11] In some cases security prevailed. The German hospitals were able to use backup data without paying the ransom, as was a Canadian hospital targeted by a different ransomware, WinPlock.[12]

Unfortunately, not all incidents have been so easily resolved, and perhaps healthcare organizations are targeted more often than others in this widespread malware epidemic because attackers are experiencing relative success against them. In other words, hospitals and clinics may be more willing than others to pay for the decryption of their critical and sensitive information, especially when such attacks paralyze their operations and affect both patients and staff. In another notable Locky incident, for instance, a US hospital paid attackers 40 Bitcoins (~ USD17,000) to decrypt files on critical servers.[13] The Bitcoin exchange rate has been rather volatile lately, so had the attack happened in January 2017, that 40 Bitcoin ransom would have cost the hospital close to USD40,000.

Many other victims have acted likewise, though often the size of the ransom paid has not been revealed for "security reasons." One US-based health facility notified customers that their electronic medical records and backup copies had all been encrypted by Cryptowall ransomware, and that "seeing no other option" they had paid an undisclosed ransom fee to regain access.[14] In one unlucky twist of fate, a US medical billing and electronic health record service provider paid a ransom and got their customers' data unlocked, but then lost it due to a faulty backup system.[15] Americans aren't the only ones paying. One survey released in August 2016 reported that among respondents from non-US businesses, 40 percent said they too had paid a ransom to recover encrypted data.[16]

Contents

How are healthcare companies being infected by ransomware? Banking Trojans and ransomware use the same infection vectors, and increasingly, cybercriminals are delivering ransomware via spam and phishing emails designed to trick unwitting users into opening an attachment or clicking a link. IBM X-Force has found that the average ransomware attachment rate in spam emails, at 0.6 percent in 2015, ballooned to an average of 40 percent of all spam in 2016—an increase of six *thousand* percent.[17] Drive-by-download is another infection vector.[18] In one incident, a Canadian hospital running an outdated content management system was found to be exposing visitors to the Angler exploit kit—delivering ransomware directly from its compromised website.[19]

Whatever the variant or infection vector, ransomware presents all industries with the clear and costly danger of both data loss and operational impact, and many organizations in the healthcare industry may not be prepared to handle the threat. In fact, an IBM-fielded, US-based consumer and business research study found that businesses lack overall awareness and preparedness in the face of rising ransomware attack risk. The IBM report Ransomware Response Guide, designed to help organizations prepare for or deal with a ransomware attack, is a valuable source in that regard.

Data compromise through third-party vendors

Your security posture is only as strong as your weakest link, and your weakest link may be the third-party vendor with which you do business. The practice of outsourcing the management of EHRs or electronic medical records (EMRs) is growing. Hundreds of vendors are operating in the EHR management space,[20] and any one of them could serve as an attacker's point of entry in a healthcare data breach. The stakes can be high in this area. A breach affecting a company with a large market share could compromise multiple millions of patient records at once.

Unfortunately, such an incident isn't hypothetical. One of the largest healthcare breaches of the last five years was the compromise of a provider of software services to the healthcare industry that exposed data on almost four million individuals.[21] According to the company's statement on the breach, the "sophisticated cyber attack" was detected 19 days after attackers gained unauthorized access to its network. Clients weren't notified until almost a month after the attack began[22]—ample time for cybercriminals to conduct nefarious activities with the unsuspecting patients' information.

Contents

In December 2015 a US-based company offering management software solutions for healthcare providers became aware that it was the victim of a cyberattack that might have occurred many months earlier, as early as January of that year.

The weapon of choice may have been credential-stealing malware allowing attackers access to systems and ultimately compromising over a quarter million health care records from more than a dozen organizations (see Figure 2).[23]

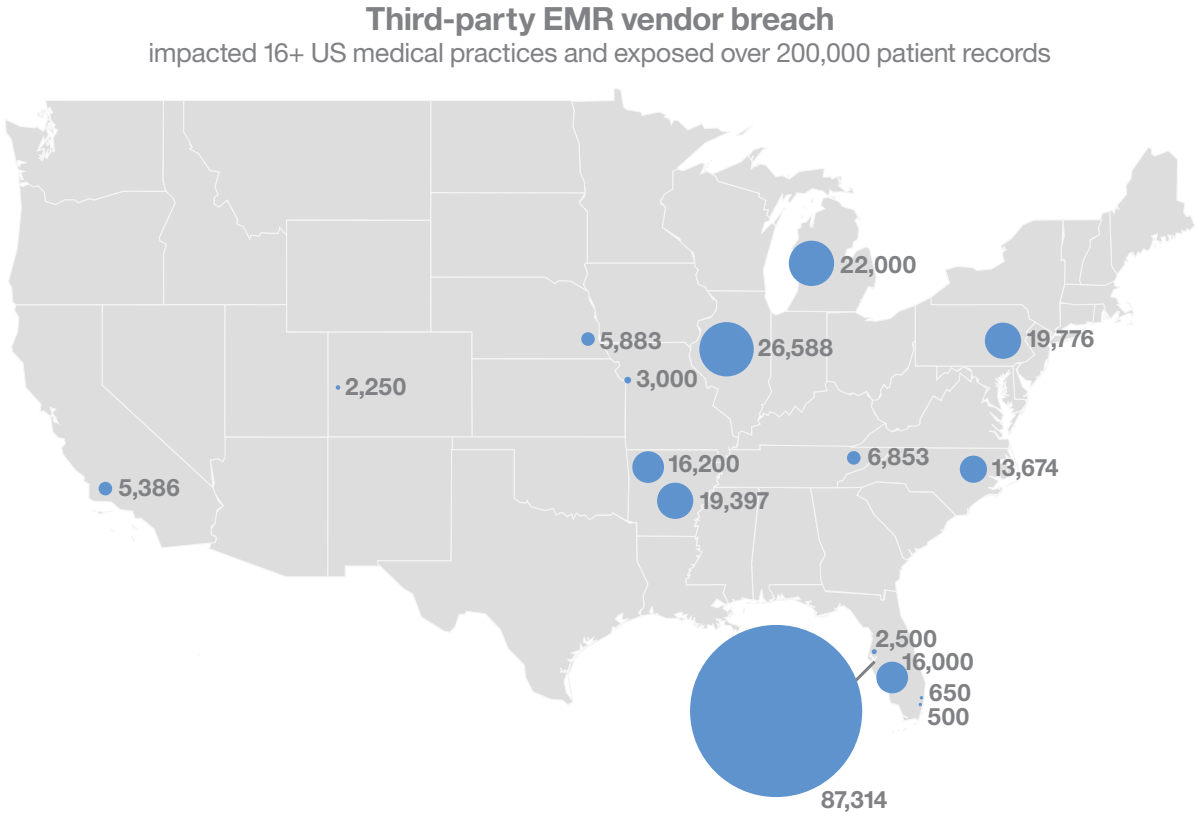

Figure 2. Map of affected companies and number of records compromised resulting from a single third-party incident. Source: IBM X-Force Interactive Security Incidents data.

Contents

Malicious actors aren't the only agents of compromise. Sometimes third-party vendors can open the data of their clients' patients to potential compromise and theft through simple carelessness. In one incident reported in February 2016, patient data from several dental practices in Canada and the United States was exposed due to a misconfigured FTP server at a company that sells management software to dental offices.[24] In another incident, a US health organization notified over 650,000 individuals of an incident involving one of its vendors that unintentionally exposed sensitive information, including social security numbers and partial payment data, to an Internet-facing server for several days.[25]

A healthcare organization's ability to protect its clients' PHI often depends on how quickly its vendors can close the breach-detection gap when an incident occurs—but navigating the world of health EMR and EHR vendors can seem daunting, especially to smaller practices. Healthcare organizations need to ask their third-party vendors the right questions. Did the software developers adhere to the expectations set forth in the HIMSS' EHR Developer Code of Conduct?[26] Is the vendor willing to sign a comprehensive business associate agreement and be audited for compliance with HIPAA privacy and security rules? The answers will show which vendors will fit with the organization's cybersecurity program and minimize its exposure to breaches and the damage they cause.

Healthcare organizations should secure assurance that third-party providers handling patient data meet industry requirements for data privacy and security.

Contents

Insider threat

Healthcare organizations continue to be victimized by insiders, both malicious and inadvertent. According to IBM Managed Security Services data, 68 percent of all network attacks targeting healthcare organizations in 2016 were carried out by insiders and more than one-third of those attacks involved malicious actors. A notable incident from April 2016 highlights the danger from individuals motivated by malice. Reportedly, the personal information of children vaccinated at Chinese hospitals was obtained partly through unauthorized access and partly by malicious insiders collaborating with attackers who subsequently posted the information for sale.[27]

Malicious insiders are certainly a concern, but others who inadvertently or unwittingly introduce threats to your environment can cause just as much damage. From falling victim to phishing scams to misconfiguring servers to losing laptops, the mistakes and failings of an organization's otherwise loyal insiders can often give attackers a wide-open gateway into its networks. Most such users are employees, but they can also be trusted third parties—partners, clients, maintenance contractors—with whom an organization conducts business.

The compromise of hundreds of thousands of healthcare records doesn't have to be the result of a complicated scheme. In one incident from February 2016, an unencrypted password-protected laptop containing the PHI of 400,000 individuals was stolen from an employee's car.[28] Beyond the immediate access it can open to internal networks and file shares, a stolen laptop can be easily booted to reveal passwords, stored temporary files, access to VPN connections, remote desktops, wireless encryption keys and more. And while lost laptops are a problem in all industries, the rate of reported loss in healthcare and pharmaceutical companies is unusually high, second to the top across all industries.[29] But how well does that fact reflect the real world? How many laptop thefts go unreported? How much data really ends up in the wrong hands this way? Tracking such statistics remains nearly impossible.

Contents

And more questions. Does poor security education play a role in inadvertent incidents? One report released in September 2016 rated healthcare employees as one of lowest-performing groups on questions asked about safe password practices.[30] How does that trickle down to other areas of basic cybersecurity hygiene? If staff is failing to apply security updates, downloading unauthorized software, or indulging in other risky and forbidden behaviors, they could easily end up being the reason malware is running rampant on the network or ransomware is locking the patients' data.

Prevalent mechanisms of attack targeting the healthcare industry

IBM Managed Security Services, which monitors billions of events reported every year by client devices in over 130 countries, analyzed the aggregate data we accumulated between January 1, 2016 and December 31, 2016. This data provides insight into the healthcare industry's daily cyber experience.

In this section we define an attack as a security event observed in a system or network that has been identified by correlation and analytics tools as malicious activity attempting to collect, disrupt, deny, degrade, falsify or destroy information system resources, or the information itself.

We have grouped the attack types listed below according to the standard set forth by the MITRE Corporation's Common Attack Pattern Enumeration and Classification (CAPEC™) effort, which "organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability."[31] The only exception is the "Indicator" category.

Inject unexpected items

According to our analysis of the 2016 data, the number one attack vector targeting healthcare organizations, at 47 percent of attacks, involves those attacks that use malicious data input to attempt to control or disrupt the behavior of a target system. Command injection, which includes operating system (OS) command and SQL injection, belongs in this category. OS command injection is also known as shell command injection, for which the now infamous and widely prevalent Shellshock vulnerability is named. Shellshock attack activity surged across all industries prior to its two-year anniversary in September 2016 and made up just over one-third of all attacks targeting healthcare in 2016.

Contents

Manipulate data structures

The number two attack vector, accounting for 19 percent of attacks, was attempting to gain unauthorized access through the manipulation of system data structures. As CAPEC states, "Often, vulnerabilities [such as buffer overflow vulnerabilities], and therefore exploitability of these data structures, exist due to ambiguity and assumption in their design and prescribed handling."[32]

Manipulate system resources

Attacks attempting to manipulate some aspect of a resource's state or availability accounted for nine percent of all attacks. Resources include files, applications, libraries and infrastructure and configuration information. Successful attacks in this category could allow the attacker to cause a denial of service as well as execute arbitrary code on the target machine.

Employ probabilistic techniques

The fourth most prevalent mechanism of attack, at six percent, involved an attacker "using probabilistic techniques to explore and overcome security properties of the target."[33] Most of the activity involved brute-force password attacks, a tactic in which an intruder tries to guess a username and password combination to gain unauthorized access to a system or data. Most of the attacks observed targeted the Secure Shell (SSH) service. Attackers favor SSH because it provides shell account access across the network.

Indicator

A cyber threat indicator consists of certain observable conditions as well as contextual information about the condition or pattern. These events, which accounted for six percent of the total in the data analyzed, could indicate either a compromise or an attempted attack on the target system. A large percentage of the activity involved targeted systems experiencing many (100-plus) external destinations in a short time, which might indicate a compromised internal host. If compromised, a host could be attacking other targets or communicating with other compromised hosts.

Contents

Abuse existing functionality

Four percent of attacks involved those attempting to abuse or manipulate "one or more functions of an application in order to achieve a malicious objective not originally intended by the application, or to deplete a resource to the point that the target's functionality is affected."[34] Successful attacks in this category could allow the attacker to obtain sensitive information or cause a denial of service, as well as execute arbitrary code on the target machine.

Collect and analyze information

Attacks focused on the gathering, collection and theft of information made up four percent of attack attempts targeting client devices. Most of these attacks involved fingerprinting, often viewed as a kind of pre-attack to gather information on potential targets and discover existing weaknesses in them. Essentially, an 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 application. Attackers can use the information to exploit known vulnerabilities in the target organization's IT infrastructure.

Engage in deceptive interaction

Accounting for three percent of attacks, attempts to fool victims into opening malicious documents or clicking on links to malicious sites are proving very successful in the healthcare industry. The suspect documents and links are often delivered via phishing campaigns. One of the most devastating healthcare breaches reported to date, which compromised the information of nearly 80 million individuals, is suspected to have been initiated via phishing, which led to the attacker's obtaining employee credentials.[35]

Subvert access control

Attacks attempting to subvert access control through the "exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage identity and authentication"[36] accounted for two percent of attacks. Most of the attacks observed in this category involved the exploitation of vulnerabilities in the target's client/server communication channel for authentication and data integrity by leveraging the implicit trust a server places in what it believes to be a valid client.

Contents

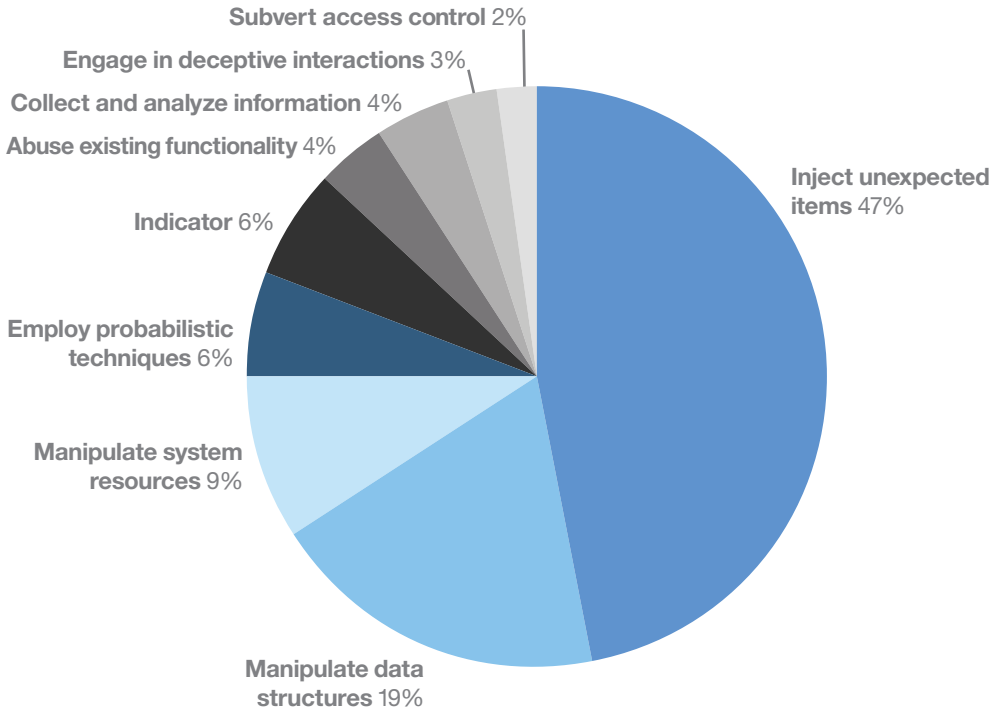

Figure 3. Prevalent mechanisms of attack targeting healthcare industry. Source: IBM Managed Security Services data (January 1, 2016 – December 31, 2016).

Contents

Fortify your cybersecurity immune system

The risk factors and data on actual attacks make it very clear. The time for healthcare organizations to strengthen their information security posture from top to bottom—employee training, third party control, proper technological solutions, the works—is now. The guidance provided in the 2016 Security trends in the healthcare industry report still holds true. First and foremost, cyber security has to be a business priority. If so, there will be adequate budgetary allocations, a dedicated information security person to run the show, and an incident response plan, or IRP, to help you comply with HIPAA and other regulations. You may also be reviewing medical devices for security issues and applying essential data protection methods. Those are the basics. What else can your healthcare organization do to fortify its cybersecurity immune system?

Backup your data with the threat in mind

Ransomware is a growing and significant trend. If ransomware defeats your protection strategy and renders your data encrypted and unrecoverable, your next best strategy is to have a regularly updated backup. You're still bound to lose some data—how much depends on how long it's been since your last backup—but the loss will be far less devastating than it would be without any backup at all. Services such as IBM Resiliency Backup as a Service can protect your data with fast, flexible cloud-based backup and recovery.

Just having backups isn't enough. You also need to test them. In several cases seen by IBM X-Force Incident Response and Intelligence Services, companies that had never tested their backups found they didn't work when they tried to restore their data.

Contents

Mitigate internal threats

Insiders who compromise sensitive data often act undetected. Their legitimate access to the information makes it difficult to spot a breach: they could interact with that data every day in order to do their jobs, and then one day access it for nefarious ends. For this reason, it is important for security teams to take an integrated approach across several technology and business areas to both reduce their exposure to these types of threats, and better detect them when they do occur.

To reduce exposure, companies must combine data security and identity and access management solutions to protect their sensitive data and govern the access of all legitimate users. The more end users have access to sensitive information, the greater the chance that someone will put it at risk, either maliciously or by mistake. Companies must ensure they are limiting access to only those users that absolutely need it, and that controls stay current as the user population changes and evolves over time. Similarly, the easier the information is to access, and the more places it resides, the higher the chances that an insider, or an outsider with stolen credentials, will be able to gain access for the wrong reasons.

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. Solutions like IBM Security® Guardium® can help ensure sensitive data is appropriately protected.

To detect threatening or suspicious insider behaviors, 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.

Contents

For these technologies to work well together and protect an organization from insider threats, they must be coupled with the right security expertise to address any security gaps insiders might exploit. For organizations that don't have the skills in-house, or for those who want to find a manageable way to get started, an IBM Security Services engagement, such as IBM identity and access management services for insider threat protection, can provide the business and security experience to help evaluate intelligence, draw more meaningful conclusions and prepare for next steps.

Recent merger or acquisition? Penetration testing services may be needed

According to one report, "the number of hospital transactions announced in 2015 grew 18 percent compared with 2014 and 70 percent compared with 2010."[37] Challenges resulting from mergers and acquisitions go beyond integrating leadership and aligning operational efficiencies. One that may be overlooked is proper consideration of the safety and security of record storage strategies during integration of the merged organizations' EHRs and information systems. In one incident, a security breach in a practice went undiscovered until after the sale, when the new owners' IT personnel discovered the unauthorized access.[38] From small private practice acquisitions to large hospital mergers, IT security must be part of the process.

A safer future for healthcare

We have seen that the healthcare industry is a leaky vessel in a stormy sea. Change and expansion are moving faster than protection and security, and attacks are far outpacing defense. That must change, because the threat is extreme. Putting it one way, making your healthcare organization compliant and secure can help minimize your risk exposure and reduce the potential impact from all threats. Putting it another way, your inattention to cybersecurity is dangerous to your patients' financial health and physical welfare, even their lives.

Contents

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. With IBM X-Force Incident Response and Intelligence Services, IBM experts proactively hunt and respond to threats, and apply the latest threat intelligence before breaches occur. 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, 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, holding more than 3,500 security patents and processing upwards of 1 trillion security events every month for more than 4,500 clients across 133 countries.

Contents

About the author

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

Contributors

Scott Craig – Threat Researcher, IBM Security

Limor S. Kessem – Executive Security Advisor, IBM Security

Jason Kravitz – X-Force Research and Techline Pre-Sales Support

Laurène Hummer – Global Portfolio Marketing, Security Services, Identity and Access Management

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

References

[1] https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-4574&S_PKG=ov39959

[2] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[3] http://www.medicalpracticeinsider.com/news/medical-identity-fraud-hammers-healthcare

[4] https://dashboard.healthit.gov/evaluations/data-briefs/hospitals-patient-engagement-electronic-capabilities-2015.php

[5] http://www.clinicalleader.com/doc/overview-of-ehr-systems-in-bric-nations-0001

[6] https://www.infoway-inforoute.ca/en/component/edocman/3152-connecting-patients-for-better-health-2016/view-document?Itemid=101

[7] http://www.digitalhealth.gov.au/news-and-events/news/1180-launch-of-the-national-digital-health-strategy-consultation

[8] https://securityintelligence.com/ransomware-top-security-threat-expected-to-continue-rising-in-2017/

[9] https://securityintelligence.com/news/locky-ransomware-cute-name-ugly-consequences/

[10] http://www.nzherald.co.nz/wanganui-chronicle/news/article.cfm?c_id=1503426&objectid=11594628

[11] https://www.helpnetsecurity.com/2016/02/26/crypto-ransomware-hits-german-hospitals/

[12] http://www.archersecuritygroup.com/we-would-never-pay-a-ransom-hospital-escapes-ransomware/

[13] https://www.tripwire.com/state-of-security/latest-security-news/hollywood-hospital-pays-17000-to-ransomware-attackers/

[14] https://www.databreaches.net/nj-spine-center-saw-no-other-option-but-to-pay-ransom/

[15] http://www.marinij.com/health/20160929/marin-patients-medical-data-lost-after-cyber-attack

[16] https://www.malwarebytes.com/pdf/white-papers/UnderstandingTheDepthOfRansomwareIntheUS.pdf

[17] https://exchange.xforce.ibmcloud.com/collection/Ransomware-tops-the-spam-charts-in-2016-1332816b2536befc46fb600ab51613da

[18] https://securityintelligence.com/an-evolving-threat-ransomware-in-2017/

[19] https://blog.malwarebytes.org/security-world/2016/03/canadian-hospital-serves-ransomware-via-hacked-website/

[20] https://dashboard.healthit.gov/quickstats/pages/FIG-Vendors-of-EHRs-to-Participating-Professionals.php

[21] http://www.nbcnews.com/tech/security/medical-informatics-engineering-hack-exposed-data-3-9-million-people-n403351

[22] https://www.mieweb.com/notice

[23] https://www.databreaches.net/264000-and-counting-hack-of-ehremr-vendor-leaves-clients-scrambling/

[24] http://www.databreaches.net/22000-dental-patients-info-exposed-on-unsecured-eaglesoft-ftp-server/

[25] https://www.databreaches.net/bon-secours-notifies-655000-patients-that-vendor-error-exposed-patient-info-on-internet/

[26] http://www.himssehra.org/ASP/codeofconduct.asp

[27] http://www.globaltimes.cn/content/977702.shtml

[28] http://www.careersinfosecurity.com/laptop-breach-may-affect-400000-prisoners-a-9173

[29] http://www.intelligenceinsoftware.com/featur/feature/it_software_strategy/lost_laptop/index.html#.WG_OBH2WLmM

[30] http://www.prnewswire.com/news-releases/cyber-security-awareness-report-from-wombat-security-reveals-knowledge-gaps-that-pose-major-enterprise-end-user-security-risks-300321366.html

[31] https://capec.mitre.org/data/definitions/1000.html

[32] http://capec.mitre.org/data/definitions/255.html

[33] http://capec.mitre.org/data/definitions/223.html

[34] http://capec.mitre.org/data/definitions/210.html

[35] http://www.insurancejournal.com/news/national/2015/02/10/357051.htm

[36] http://capec.mitre.org/data/definitions/225.html

[37] https://www.kaufmanhall.com/software/news-detail/hospital-merger-and-acquisition-activity-up-sharply-in-2015-according-to-kaufman-hall-analysis

[38] https://www.databreaches.net/laser-dermatologic-surgery-center-notifies-31000-of-possible-phi-compromise/

Contents

IBM Security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2017

IBM

SEL03123-USEN-01