HEALTHCARE WHITEPAPER

source

DEFENSE

SECURING HEALTHCARE AND BIG PHARMA COMPANIES FROM FORMJACKING AND MAGECART ATTACKS

Executive Summary

Web browsers contain a universal flaw that leaves major healthcare and pharmaceutical companies at risk of exposing personally identifiable information, financial details, and account credentials every time a visitor accesses their websites. This flaw prevents website owners from controlling what data can be accessed by their website supply-chain vendors and, when those vendors are compromised, allows hackers unlimited access to their visitors' experience and information.

Every website is susceptible to this attack vector as no component of traditional security programs can prevent client-side attacks perpetrated via JavaScript. Despite the rising threat, the vast majority of hospitals and physicians are unprepared to handle cybersecurity threats, even though they pose a major public health problem. This threat briefing is intended to raise awareness of this universal flaw and introduce preventative measures that may be taken.

8 Reasons Why Cyberattackers Target Healthcare Companies

1. Patient information is worth a lot of money to hackers
2. The potential disruption of implementing new technology clashes with already convenient working practices
3. Medical devices are an easy entry point for hackers
4. Medical staff's access to remote data opens up more potential vulnerabilities
5. Healthcare staff traditionally aren't trained in online threats and risk potential
6. The amount of devices used in hospitals make it difficult to stay on top of security
7. Healthcare data needs to be open and shared
8. Outdated technology means the healthcare industry is unprepared for attacks

When Online Attacks can Threaten Lives

The Healthcare industry is going through a rapid digital transformation which has made organizations extremely vulnerable to data breaches and malicious attacks. A healthcare provider's public website, web services, and self-service portals are critical digital assets that must be secured. Patients use their credentials to access lab results, order and update prescriptions, pay insurance premiums, and more. A breach resulting in compromised patient health information (PHI) has serious ramifications for the organization.

Hospitals and medical facilities have been targets of hackers and ransomware groups for years, in part because of computer storage of **sensitive patient information and lapses in cybersecurity**. Motivated attackers put extra effort into finding new and unexpected ways to infiltrate healthcare companies, and they won't miss any window of opportunity.

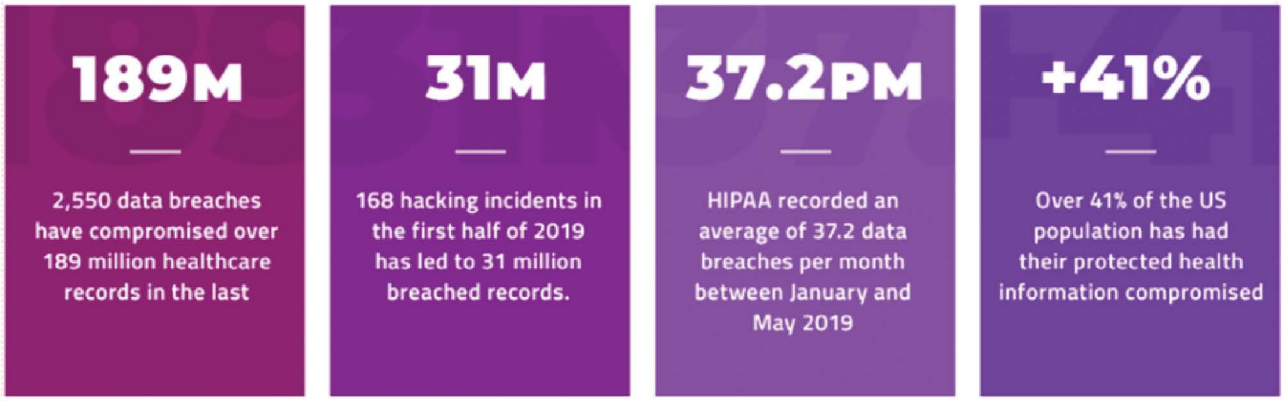
When cyber-attackers infiltrate healthcare-related systems, they may be able to compromise and steal PHI such as patient names, addresses, telephone numbers, medical conditions, treatments, pharmaceutical information, and insurance records. Unlike credit card information, PHI cannot be changed, which may account for its high value.

In addition, information taken from healthcare services that can be used to forge medical backgrounds go for as much as $500 per listing on the dark web. Cybercriminals will continue to exploit security vulnerabilities in the healthcare industry, as there is a better chance of financial reward and return on their time investment.

Whether their intent is to access patient data or collect a ransom – as long as these organizations remain easy targets, they'll continue to be targeted. PHI is more valuable on the black market than credit card credentials or regular Personally Identifiable Information (PII). Therefore, there is a greater incentive for cyber criminals to target medical databases and sell the PHI or use it for their own personal gain.

In addition to dealing with cybersecurity threats and data breaches, the healthcare industry is also governed by the Health Insurance Portability and Accountability Act (HIPAA). Non-compliance with HIPAA results in significant fines, and compliance with HIPAA and other regulatory mandates is a boardroom issue.

Most hospitals don't have the resources to monitor threats to their systems, and many might not even be aware that they're something to be concerned about. The challenge for the healthcare industry in the years ahead is the drive to digitally transform organizations and increase automation, data, and system interoperability. But this all has to be done securely, otherwise the industry, regulators, and most importantly — patients — could lose their trust in the system.

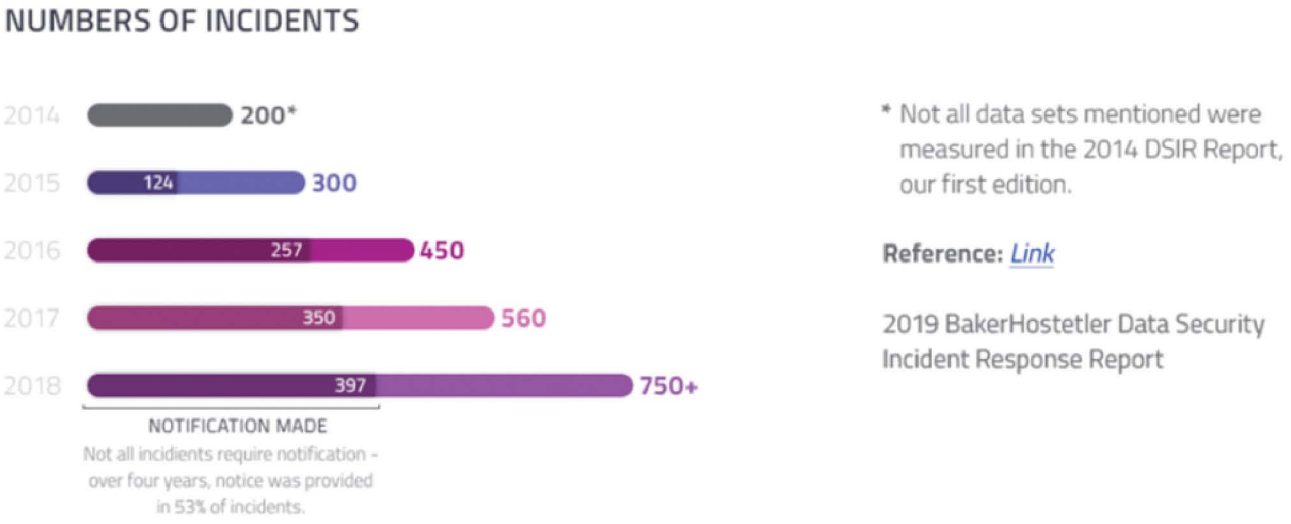


With the use of online healthcare portals and remote technology, online threats and attacks will continue to rise. Healthcare CISOs must prepare now for the challenges of managing security and compliance across a dynamic environment. Protecting PHI, as well as any type of data breach that may potentially expose patients to harm, should be healthcare organizations' top priority.

Healthcare Companies and Unmanaged Risks

Malicious code may be injected into your website and or executed on victims' browsers without their knowledge. The more tools used, the greater the risk healthcare companies expose their visitors to. Evaluating the security perimeter of any website is simply not enough because that perimeter has expanded to include the code provided by the myriad of 3rd party tools in use on every contemporary website, as well as the fourth, fifth, etc. sets of code which those tools rely on to provide functionality.

Given the digital transformation that the healthcare industry is undergoing, many websites in the industry rely on an ever-expanding ecosystem of 3rd party suppliers to enhance and personalize user experience, increase engagement, track their customers' journey and behaviors, and so on. These 3rd party tools offer great benefits, but also provide attackers with an attractive gateway for malicious activities such as form jacking, magecart, JavaScript skimming and more.



The Rise in Supply Chain Attacks

Websites rely heavily on 3rd party vendors to provide within the browser. Unlike traditional applications, functionality and behavior expected of visitors. 3rd parties however, each piece of JavaScript is accessed in real-time to provide analytics, user behavior analysis, customer engagement, display advertising and, in general, monetization of a website's content and brand. Although 3rd parties provide immense value, they also introduce a broad security risk to the visitor of an organization's web site.

JavaScript, the programming language which enables interactivity on the web and facilitates the functionality of these 3rd party tools has very poor inherent security controls. In fact, it would be fair to say that there are no controls available at all. Every line of JavaScript which is executed by a web

browser has the same level of access, permission to run and interaction with the user that any other line does. The consequence of this is that there is no way to control the behavior of any particular script within any given web session using standards-based approaches.

Each script in a traditional computer programming context may be thought of as its own application running as the visitor requests a web page. There is no concept of compilation, bundling or package delivery within the browser. Each script arrives fresh on each pageview with whatever behavior it contains at that particular moment.

The combination of these factors leads to a serious security flaw, namely, that 3rd parties which drive monetization can and do introduce unintended behavior into the visitor experience. And, if a third party is compromised, that unintended behavior may take the form of malicious exploitation: credit-card skimming, defacement, PII disclosure, etc.

In essence, any enterprise hosting content through a web server is extending unlimited trust to each 3rd party as it relates to the visitor's experience. In the context of modern cybersecurity practice and regulatory requirements this is untenable risk for any organization, let alone those which handle PHI in addition to more commons forms of protected information.

Attacks Aimed at Healthcare Organizations:

- Payment card skimming
- Keylogging
- Form field manipulation
- Web injection
- Phishing
- Content defacement
- Clickjacking
- Malware and ransomware distribution
- Watering hole attacks

Tips to Protect Healthcare Companies from Online Attacks:

1. Prepare a clear description of potential risks: healthcare companies need to assess their vulnerabilities and detail possible attack scenarios
2. Identify best practices: after appropriate cybersecurity solutions are implemented in healthcare institutions, it is necessary to develop best practices and familiarize users to ensure the highest outcome of success in preventing cyber-attacks
3. Simulate attacks and response: all organizations face a constant threat of potential cyber-attacks. Simulations help improve the ability to detect and prevent cyber-attacks along with handling the aftermath of a potential attack
4. Identify the most important and specific data: healthcare organizations need to prioritize data according to the levels of privacy and importance associated with protecting it. The type of data will help determine the level of security and investment required to protect that data

A thorough cybersecurity plan must be implemented to ensure that organizations, employees, and patients are protected. It is important to follow key cybersecurity best practices to help reduce security vulnerabilities. Research has shown that a low level of cyber employee awareness training has caused more than half of the attacks in the healthcare industry.

An Innovative Approach in Securing Healthcare Websites Security Gaps

Source Defense provides an entirely new and unique solution to protect websites and their visitors from attacks that lead to data theft from the live customer web session. Source Defense's VICE solution secures websites, enables secure digital innovation, and ensures customer and payment data privacy via the only real-time prevention solution against website supply chain attacks. By isolating and sandboxing all 3rd party website code, website supply chain partners can be managed and controlled preventing security violations that access unauthorized customer and payment data that are then exploited by hackers.

VICE delivers security without compromising the user experience or burdening your IT staff with unnecessary administration. Source Defense ensures 3rd party website tools only deliver the intended website experience and that these JavaScript tools may not be leveraged for malicious data extraction or website alteration.

About

Source Defense

Source Defense is the market leader in Client-side Web Security, providing real time threat protection against vulnerabilities originating in third-party scripts such as Magecart & Formjacking attacks.

With their patented VICE platform, Source Defense protects web pages from vulnerabilities in third-party scripts. Source Defense's solution isolates those scripts from the web page and allows them to read and write according to a given permission either defined by Source Defense's recommended standards, or specific company policies.

Source Defense extends the traditional security perimeter to protect your customers and fortify your security stack in real-time.