White paper

The New Threat: Attackers That Target Healthcare Organizations (And what you can do about it)

Abstract

Healthcare organizations (HCOs) are facing a new threat. They're being targeted by financially motivated attackers that steal and sell valuable data -- including identities -- and computing resources. Armed with sophisticated tools, attackers exploit countless software vulnerabilities that exist in the multitude of systems a provider relies upon, including web-based applications such EHR/EMR systems. The consequences of an attack can include reductions in quality of care, service disruptions, reduced revenues, higher operating costs, and regulatory fines. Current security approaches, including network or perimeter defenses, do not adequately protect against the new threat, and can be bypassed. It is imperative that healthcare organizations conduct a vulnerability assessment of their critical applications, and evaluate intrusion prevention as a key compensating control to mitigate the growing risk.

,

Table of Contents

1. Introduction

It's a typically busy morning at the hospital, with all operating rooms booked to capacity. Down in the ER, doctors are treating a steady stream of emergencies. Over in radiology, several patients are being prepped for MRIs. But at 8:35am, the day's steady rhythm is shattered. Something's wrong. The operating room doors won't open. Shortly after, the nurses in the ICU can't log onto the computers. At 9:05, pagers stop working. And by 11am, the MRI machine has crashed, leaving a waiting room of frustrated, anxious patients. Meanwhile, a thousand miles away, a middle-aged man sits alone at his PC, and smiles to himself, as the wreckage unfolds. A few keystrokes later and he's into the database of the hospital's EHR/EMR system, calmly extracting valuable data from thousands of patients that he'll quickly sell for a tidy profit.

Another Hollywood thriller, set in the distant future? Unfortunately not. Although this perfect storm of events is unlikely to occur in a single morning, this is the reality that healthcare providers operate in today. Healthcare organizations are being targeted by attackers.

2. The New Threat

Until recently, attention-seeking hackers were the main IT security threat to businesses, including healthcare organizations. They would write code, unleash it into cyberspace, and hope for their 15 minutes of fame. These types of mass attacks often had no particular target in mind; they would simply seek out vulnerabilities in a system—typically in operating systems and networks—and exploit them.

But that was when hackers and their motives were less dangerous. Recently though, security intelligence experts have detected "the tell-tale signs of organized crime gangs and government espionage in attacks, and a hacker community much more motivated by financial gain than

personal or political fulfillment." (Forrester, "Increasing Organized Crime Involvement Means More Targeted Attacks", August 2, 2005)

Hackers have now become attackers who target particular organizations or groups or users. Motivated by money, revenge, and perhaps in the future by terror, they take control of computing devices to steal identities and confidential data that can then be sold, to use for illegal purposes like sending spam, or to disrupt operations and the delivery of services. And while some attackers might be faceless strangers on the other side of the world, others lurk within your midst. There is a significant risk from insiders - employees, contractors and consultants -- who easily bypass perimeter security and other traditional IT security solutions.

	The "old" threat	The "new" threat
Description	Hacker	Attacker
Type	Random, indiscriminate acts of vandalism	Targeted attacks on specific organizations or groups of users
Motivation	Attention, fame	Financial gain, revenge
Weapons	Mass worms and viruses with relatively benign payloads	Sophisticated, blended attacks, malicious payloads

Just a few years ago, a targeted attack against a healthcare facility was uncommon. But now healthcare facilities have become prime targets. Hospitals, clinics, and medical group practices all contain large amounts of valuable data. Not just confidential patient information but also financial and personal information about employees, insurance companies, suppliers, and partners—making them very appealing to attackers interested in financial gain. In 2005 alone, Privacy Rights Clearinghouse identified more than ten HCOs that had suffered significant security breaches, including University of Florida Health Sciences Center, Duke University Medical Center, and University of Chicago Hospital.

> The Cleveland Clinic Health System discovered that between 8:00 and 9:00 a.m., on any given morning, they block nearly 40,000 attacks that try to exploit a weakness in an unpatched PC.
>
> *"Locking Intruders Out! Securing Healthcare Data", Presented at HIMSS 2006*

Now that most HCOs have strong perimeter defenses including network firewalls, user authentication, configuration management, and data encryption, attackers have set their sights on the next most vulnerable part of your system: software applications.

3. Applications – The Heart of Your Healthcare Facility

HCOs increasingly rely on computerized systems and software applications. Large hospitals often have tens of thousands of computerized devices, ranging from diagnostic systems, like X-ray and MRI machines, to portable bedside monitors, wireless/telemetry monitors, clinical systems, wireless PCs, and enterprise servers. Each of these systems run on software applications, many of which are commercial off-the shelf (COTS) applications, while others are one-off, custom applications, developed for a specific organization. It is not uncommon for an HCO to run 100's of applications including:

- Operating systems
- Databases
- Servers
- Office productivity applications
- Electronic Health Records / Electronic Medical Records (EHR/EMR)
- Patient Health Records (PHR)
- Picture Archiving and Communication System (PACS)
- Diagnostic systems
- Monitoring systems
- Physician and patient portals
- Clinical and health information systems
- e-Prescribing applications
- Finance, payroll, and human resource applications

Without these systems, healthcare facilities simply cannot reliably provide the high-quality services they – and their patients -- have come to expect. And while no one questions the benefits these applications provide, in terms of quality of care, improved communications, operational efficiency and savings, it is important to recognize the risks they introduce into your HCO.

These software applications come with thousands of vulnerabilities that can be exploited by an attacker. The potential consequences of a vulnerability being exploited include an attacker:

- Taking full control of a system
- Installing programs

> "The FBI is investigating unauthorized changes made to a MySQL database that underlies an electronic medical record system at an Indiana-based orthopedics clinic. Orthopedics Northeast noticed significant performance slowdowns in January. The changes were apparently made by an intruder who gained initial access to the system through a back door in WebChart software from Medical Informatics Engineering (MIE). On one occasion, the intruder appended characters to a database query, causing it to crash. On another occasion, the intruder deleted a print-server directory."
>
> *Computerworld, February 10, 2006*

- Viewing, deleting, or changing patient or medical data
- Creating new accounts with full user privileges
- Denying service (i.e., X-ray, MRI, etc.)
- Crashing systems

The more responsible COTS application vendors routinely communicate information about the new vulnerabilities that have been discovered in their software through security bulletins. However, practices vary, and vulnerabilities in custom-built applications are often only discovered once they've been exploited.

4. Why Are Applications Vulnerable?

For one, it's all but impossible to write perfect code. Most software has from 1,000 to 1,500 security defects per million lines of code ("Software Assessments, Benchmarks, and Best Practices", 2000) and sophisticated software applications typically have millions of lines of code. EHR/EMRs, for example, are complex systems that typically consist of an operating system, a database, a web server, an application server, as well as the EHR/EMR application itself. All told, there can be a hundred million lines of code and as many as 150,000 defects that an attacker could attempt to exploit to gain access to the heart of a healthcare organization's systems. Not all of these will be critical vulnerabilities, but the numbers can be staggering.

Last year alone, 1,500 major software vulnerabilities were disclosed (SANS, 2005) and more than 10,800 new virus and worm variants were identified for the Win32 platform, in the first half of 2005. (Secure Computing, March, 2006)

The other reason that applications are vulnerable is that they are increasingly based on Internet Protocols; that is, they are designed to be remotely accessed by system administrators, medical professionals, healthcare partners, and patients, via the web. While web-based applications offer convenience, efficiency, better service, and savings, they also fundamentally increase the vulnerability of your applications, systems, and sensitive data.

5. The Consequences of an Attack

An attacker who successfully exploits an application vulnerability could quickly and significantly affect a healthcare facility in a variety of ways like disrupting services, stealing data and identities, taking control of host computers and using them for illicit purposes. The fallout from these attacks can be devastating.

Quality of care: If an attacker changes patient information, or disrupts hospital services, quality of care can be jeopardized. At Seattle's Northwest Hospital, for example, a 20-year old attacker in California used a computer "bot" that caused computer malfunctions. As a result, doors to the operating room did not open, pagers didn't work, and computers in the intensive care unit shut down. (Computerworld, February 13, 2006)

Financial loss: When the security of an organization is compromised and publicized, the financial impact can also be significant. Security breaches not only reduce revenues because of service disruptions but they also increase costs. Systems now have to be fixed plus there are often penalties, fines, and media relations costs when it comes to announcing security breaches. Customers and patients care a lot about the confidentiality of their data. "In a national survey of more than 1,000 victims of personal data security breaches, nearly 20% said they had already terminated their relationships with companies that maintained their data, while another 40% said they might do so. And nearly 5% of those surveyed said they had hired lawyers to seek legal recourse after their data was put at risk." (ComputerWorld, September 28, 2005)

Compliance and notification: Compliance-related issues are perhaps the biggest headache related to a security breach. In addition to HIPAA, which is now reasonably well-understood by most affected organizations, there are numerous new breach notification laws that are causing severe discomfort. They require HCOs to inform patients if their data has been compromised or exposed by an attack. There is a patchwork of breach notification laws, which are either already in place or proposed, in more than 40 states.

Many of those state laws specify different triggers for notifications and set varying requirements on what must be disclosed, to whom and when. California, for instance, uses an "acquisition standard" that requires companies to notify consumers each time their data has been acquired by an unauthorized person. Other states, including Delaware, Arkansas and Florida, require companies to notify consumers of breaches only if the companies believe there's a reasonable risk of harm. Some states exempt companies that encrypt their data from disclosures; others don't. To make things more complicated, breach notification is extra-territorial. This means that a healthcare provider who treats an out-of-state resident must adhere to the breach notification laws of the patient's home state, if their data is compromised.

> "Despite the compliance headaches caused by such disparities, the laws appear to be forcing companies to pay more attention to how they handle confidential data,"
>
> *John Pescatore, Gartner Inc.*

6. Current Security Approaches Are Not Adequate

Healthcare organizations have done a lot to strengthen their security with perimeter defenses, network firewalls, user authentication, configuration management, and data encryption. But now that attackers have set their sights on applications, these measures do not provide adequate protection because they can be readily bypassed by attackers, for these reasons:

- ***WiFi:*** Wireless networks provide alternate paths into the organization that often circumvent perimeter security defenses.

- ***Mobile PCs***: One of the major tools that attackers target as a means of launching an attack are individual PCs. Given today's flexible work environment, many of the PCs that attach to the network are mobile and travel outside the protection provided by the network or are home machines that permanently reside outside the control of the IT department. While outside the defensive perimeter, these machines are easily compromised and can be used as launching points for more sophisticated attacks against the organization the next time they connect to the network.

- ***Tunneling:*** Tunneling is often used to create private networks on public systems by encrypting data between end points. Ironically, the increasing trend towards encrypting data in transit or storage means malicious code can 'hide' from network-based intrusion detection and prevention systems and other safeguards until it reaches its end point on a server. Attacks can utilize SSL/TLS or IPSec as a means of tunneling the attack all the way to the host – depending on the target of interest. In many states, encryption is no longer considered a "safe harbour". That is, even if data is encrypted, if it is stolen, you can still be penalized.

Beyond perimeter defenses, many HCOs rely on patches – fixes provided by software vendors that address specific vulnerabilities. However, while patching software vulnerabilities remains a key security priority, it's a race that can't be won. The time between the publication of a vulnerability and the malicious code that exploits it has been narrowing sharply – from months and weeks down to days. In some cases, attacks occur before the vulnerability is even announced (so-called Zero-day attacks). Meanwhile, the time to create patches and distribute them remains relatively fixed and dangerously long because they need to be tested and installed, and scheduled to minimize disruption. And because deploying patches can affect manufacturer warranties, many medical devices are left unpatched for long periods of time.

Additionally, patching cannot protect organizations against vulnerabilities they are unaware of. Often referred to as unknown vulnerabilities – this type of risk is the result of an attacker becoming aware of a vulnerability and generating an exploit for it, before either the application vendor is aware of the issue or has created a patch and notified its customers.

> "As cyber attackers become more efficient at quickly exploiting software vulnerabilities, IT security managers will not be able to patch faster than all cyber attacks."
>
> *"Gartner Predicts 2005: Security Focuses on Attack Prevention", John Pescatore et al*

7. Steps You Can Take To Reduce Your Risk

It is impossible to remove every possible security risk to any business. So it's important to determine what level of risk you are willing to assume, and then cost-effectively implement security processes and technology that reduce the risk to an acceptable level. In addition to arming yourself with relevant and timely threat information, educating staff about security, and imposing security requirements with healthcare partners, there are a number of other important first steps you can take to determine how vulnerable your HCO is, and to prevent attackers from exploiting the applications you rely on.

Step 1: Perform an application vulnerability assessment

An application vulnerability assessment will help you determine what vulnerabilities your systems have. An application assessment can take as little as a day, and uses special software to systematically test for thousands of known vulnerabilities. It then categorizes the vulnerabilities by degree of severity. HCOs can prioritize these vulnerabilities for further action, and decide whether they are prepared to accept the medical, business, and legal risks associated with these vulnerabilities.

Step 2: Demand better accountability from your application software vendors

Ask your software and system vendors to disclose application vulnerability information. Not only does it give you the information you need to better protect yourself, but it also shows them you're aware of potential flaws in their software. The more that HCOs demand accountability from vendors, the more care vendors will take to reduce vulnerabilities in their products. HCOs should consider participating in vulnerability reporting programs such as the recently announced e-Health Vulnerability Reporting Program **(**www.ehvrp.org**)** that strive to ensure greater security of e-Health systems.

Step 3: Implement a defense-in-depth strategy

Defense-in-depth assumes that no single component, policy, or process can assure security. The modern computing environment is too complex and diverse. Attackers have access to the same vulnerability bulletins as everyone else, and a growing range of automated tools with which to exploit them. The potential risk of failure and regulatory penalties requires that security managers not just arm themselves against a minimum standard of documented threats but to anticipate the unknown: in effect, to 'prove a negative', and show they are not insecure. Intrusion prevention systems (IPS) are an integral part of a comprehensive defense-in-depth strategy.

8. Intrusion Prevention—Your Best, Last Line of Defense

An advanced, IPS prevents attacks that exploit vulnerabilities in commercial and custom software, including e-Health applications. It can be deployed on or near the host, and provides HCOs with the ability to triage their applications and apply security to those that need it the most.

It stops attacks before they impact critical data, applications, and hosts by:

- Reducing the attack surface so that communication is restricted to authorized hosts and services. This eliminates an attacker's access to many software vulnerabilities.
- Monitoring incoming and outgoing network traffic for protocol deviations or content that might signal an attack. When necessary, it intervenes and neutralizes the threat by either blocking or correcting this traffic.
- Reducing the risk of security configuration inconsistencies that leave hosts vulnerable.

It helps ensure compliance with industry regulations such as Sarbanes-Oxley, HIPAA, PCI Data Security Standard, breach notification laws, and corporate policies by:

- Preventing unauthorized access to hosts, and confidential data and information from leaving hosts.
- Providing an auditable history of security configurations and changes, and reports that document prevented attacks.

It maximizes the performance and efficiency of your organization by:

- Automating the process of configuring and deploying appropriate security policies to thousands of hosts.
- Shielding software vulnerabilities from attacks, allowing patches to be deployed on a scheduled basis, rather than reactively.
- Blocking malware before it reaches a host, thus eliminating the process of host remediation.
- Dramatically reducing the number of false positives, and the time spent investigating them.

- Reducing the preparation time required to support audits, and the fines resulting from security breaches.

It protects and enhances revenues, patient safety, quality of care, and brand equity by ensuring:

- The availability and continuity of medical services.
- The confidentiality of information.
- The integrity of business transactions.

About Third Brigade

Third Brigade (www.thirdbrigade.com) specializes in providing intrusion prevention systems to healthcare providers and payers, and other organizations that need to prevent attacks that exploit vulnerabilities in commercial and custom software, including web applications. It enables you to create and enforce comprehensive security policies that proactively protect critical applications, sensitive data and hosts, ensure regulatory compliance, and maximize the performance of your people, processes, and hosts. Unlike other intrusion prevention systems, Third Brigade's is not intrusive. It has been architected from the ground-up for intrusion prevention, and is smaller, faster, and simpler. Third Brigade. That's control.

For more information, please visit **www.thirdbrigade.com**, or contact us at:

Corporate Headquarters
40 Hines Road
Suite 200
Ottawa, Ontario, Canada
K2K 2M5
Toll free: +1.866.684.7332
Local: +1.613.599.4505
Fax: +1.613.599.8191

United States Headquarters
11710 Plaza America Drive
Suite 2000
Reston, Virginia, USA
20190
Toll free: +1.866.684.7332
Local: +1.703.903.4479
Fax: +1.613.599.8191

Author Profile

Blake Sutherland, Vice President, Product Management, Third Brigade

Blake is responsible for managing the product life-cycle of Third Brigade's advanced intrusion prevention software. He works closely with customers, prospects, partners and industry to understand market requirements, and incorporate them into the product. Prior to joining Third Brigade, Blake was at Entrust, a leading Internet security company. Blake is a Professional Engineer in the Province of Ontario, as well as a Certified Information Systems Security Professional (CISSP), and holds a Bachelor of Applied Science degree in Engineering Physics from Queen's University.