HealthManagement
Promoting Management and Leadership

Volume 2 / Issue 1 Spring 2007 - Features

Reducing Security Risk to E-Health

Author

Blake Suthherland

is vice president of

product management

at Third Brigade.

The New Threat

Until recently, attention-seeking hackers were the main IT security threat to businesses, including healthcare organisations. These types of mass attacks often had no particular target in mind; they would simply seek out vulnerabilities in one system, exploit them – and move on to the next.

Today's attackers, however, increasingly target specific organisations. Motivated by profit, revenge, and perhaps terror, they have the potential to seriously disrupt operations. While some attackers may be faraway, faceless strangers, others may lurk in your midst. There is a significant risk from insiders—employees, contractors, and consultants— who easily bypass perimeter security and other traditional solutions. Just a few years ago, healthcare facilities were rarely objects of attacks, but have recently 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 data about employees, insurance companies, suppliers, and partners—making them appealing to attackers interested in financial gain. A new form of fraud called medical identity theft is on the rise, with 250,000-500,000 victims in the US alone, according to a November 2006 Readers Digest report.

Now that most healthcare organisations 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 the system: software applications.

Applications — At the Core of Modern Healthcare

Healthcare organisations increasingly rely on computerised e-Health systems and software applications. Large hospitals often have tens of thousands of such systems, ranging from X-Ray and magnetic resonance imaging (MRI) machines to portable bedside monitors, wireless/telemetry monitors, clinical systems, wireless PCs, and enterprise servers. Each system contains custom software applications, which in turn rely on common commercial off-the-shelf (COTS) operating systems and applications.

Without these systems, healthcare facilities cannot reliably provide the high-quality services they and their patients have come to expect. And yet it is also important to recognise the risks they introduce.

Why are Applications Vulnerable?

When dealing with applications of any complexity, it's all but impossible to write perfect code. Electronic health or medical records (EHRs/EMRs), for example, are complex systems that typically consist of an operating system, a database, a Web server, an application server, and the EHR/EMR application itself.

All told, there can be a hundred million lines of code and as many as 150,000 defects open to exploitation by an attacker. While not all will be critical vulnerabilities in environments employing sound security practices and procedures, the final count of numbers can still be staggering. Another reason for the vulnerability of applications is that they are increasingly 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 risk because of their accessibility.

The Consequences of an Attack

An attacker who successfully exploits a vulnerability in an application can quickly and significantly affect a healthcare facility in various ways, including disrupting critical services (such as, for example, an operating room), stealing data and identities and using them for illicit purposes. The fallout from these attacks could be devastating, in terms of quality of care, financial losses and legal consequences – above all, in terms of compliance and notification.

Current Security Approaches are not Adequate

Although healthcare organisations have done much to strengthen their security with numerous perimeter defences, many such measures do not provide adequate protection because application vulnerabilities allow them to be readily bypassed. Attackers have set their sights on applications (or vulnerabilities within the applications) and have repeatedly proven that they are an effective way of compromising a system.

While patching software vulnerabilities remains a key security priority, it’s a race that can’t be won. Beyond perimeter defences, many healthcare organisations rely on patches— fixes provided by software vendors that address specific vulnerabilities. However, the time between publication of a vulnerability and the malicious code that exploits it has narrowed sharply—from months and weeks to days. In some cases, attacks occur before the vulnerability is even discovered or 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, installed, and scheduled to minimise disruption. Because deploying patches can affect manufacturer warranties, many medical devices are left unpatched for long periods of time.

It is all About Risk Management

Unfortunately, it is not possible to eliminate all sources of risk. The key is to determine what level of risk is acceptable and then manage the risks through costeffectively implementing security processes and technology. With respect to risks posed by software vulnerabilities in e-Health systems, organisations should ensure they incorporate the following into their risk management strategy:

1. Application Vulnerability Assessments

An application vulnerability assessment helps determine system vulnerabilities. It can require as little as a day using special software to systematically test for thousands of known vulnerabilities - or up to several weeks involving a qualified security tester. Findings are categorised and prioritised by degree of severity and assessments repeated periodically to look for new vulnerabilities.

2. Better Accountability From System Vendors Reporting results of the above assessments and asking vendors to disclose vulnerability information provides information to better protect assets; it also causes vendors to acknowledge awareness of potential flaws and compels them to take more care to reduce vulnerabilities in their products.

Healthcare IT managers should consider participating in initiatives like the e-Health Vulnerability Reporting Program (www.ehvrp.org) which strive to ensure greater security of e-Health systems.

3. Hardening Systems

Ask software and system vendors to provide application hardening recommendations and take steps to implement them. This could be as simple as changing the default configuration on “black-box” systems before they are deployed or be more involved when applications are installed on commercial hardware, to identify and disable unnecessary services.

4. Security Patches Since attackers regularly attempt to exploit known vulnerabilities, ensure the deployment of vendor approved security patches in a timely manner. Also ensure your software and system vendors provide appropriate vulnerability/ patch information so that you can make informed decisions based on risk.

5. Defence-in-Depth Strategy Defence-in-depth is a common security strategy that promotes the use of multiple protection techniques to mitigate the risk of one component being compromised or rendered ineffective. When vulnerabilities exist and patching is not an immediate option, utilising security control technology, such as Host-based intrusion prevention, will shield the application until it is patched.

While the complexity of e-Health systems, software, and applications will continue to present a daunting security challenge for many, following these security guidelines will help healthcare providers significantly reduce the risk of an attack, enabling hospitals and medical centres to deliver on the promise of lower costs and higher quality care.

Published on : Sat, 21 Apr 2007