CareTechSolutions®

Helping extraordinary people
do extraordinary things

Website Security:

How to Avoid a Website Breach

Jeff Bell, CISSP, CPHIMS, ACHE
Director, IT Security and Risk Services
CareTech Solutions

An enterprise's website is now an indispensable asset. It is the public face of the organization, presenting its products or services and increasingly providing a convenient way for users to transact business. Yet it also provides a "window of vulnerability" for sophisticated intruders into the inner workings – and the very infrastructure – of an organization.

In some of the latest findings from WhiteHat Security, 86% of all websites (and 90% of healthcare websites) had at least one "serious vulnerability." A serious vulnerability is defined as one in which "an attacker could take control over all, or some part, of the website, compromise user accounts on the system, access sensitive data, violate compliance requirements, and possibly make headline news."[1]

Who Are Today's Cybercriminals?

Today's "cybercriminals" are trained business people in commercial organizations, intent on carrying out well-designed plans of action, with goals and objectives, as well as with cutting-edge tools. And the trend is only growing with the surge in mobile computing and the cloud, creating more channels of communication and vulnerable entry points – such as the company website.[2]

The number-one reason for cybercrime is simply financial gain.[3] Not surprisingly, certain entities present a fatter target than others, promising a big payoff and little risk of detection. Some of these are also among the most vulnerable.

How Hospitals Are at Risk

The organizations most attractive to cybercriminals are those that use credit cards and other personal information. In addition, those that have old or complex code on their servers that is no longer supported by the manufacturer or is not well-maintained by the usually-understaffed IT department are an easy target. Ironically, the functionality that makes a website most valuable – interaction and engagement with the public – also opens the door to a company's Web and database servers as they respond to user requests.[4]

That closely describes the situation at hospitals and large healthcare systems, many with far-flung subsidiaries and running outdated IT systems at multiple locations with lean staffs. Hospitals make use of credit cards for patients to pay bills through the website, maintain financial records of those transactions, and, of course, house extensive repositories of Protected Health Information (PHI). Healthcare websites have one of the highest rates of serious vulnerabilities – but also were among the slowest industries to respond and fix an issue. [5]

Complicating the issue for the healthcare industry is the need to comply with regulations such as the HITECH Act, Payment Card Industry (PCI) standards, and the HIPAA Security Rule's implementation specifications and stringent documentation requirements.[6] Faced with the necessity of dedicating IT resources toward updating code and systems that do not seem to pose an immediate problem, or dedicating resources to regulatory compliance, hospitals may put compliance first. This very real-world choice, often based on budget constraints, further reduces the likelihood of proactive remediation – and leaves the hospital vulnerable.

The Most Common Vulnerabilities – and What They Can Mean for Your Hospital

The technical names and distinctions of the various weaknesses hackers exploit to invade hospitals through the website mean little in a non-technical context. WhiteHat Security lists its current Top 15 weaknesses[7], including information leakage, cross-site scripting, content spoofing, fingerprinting, session fixation … and many more. OWASP (Open Web Application Security Project) regularly publishes its own Top 10 security issues, such as injection, broken authentication, unvalidated redirects and more.[8] Both lists mention some of the same problems. It's not the purpose of this paper to explore and explain each one. More important is to convey a sense of the damage they can allow, the importance of getting rid of them – and to close the vulnerabilities through which hackers enter a hospital website.

Such access points exploited by sophisticated hackers can allow them to take control of critical functions on a hospital's website, deleting pages or adding unauthorized material. Email addresses of staff or patients can be the same as user names or passwords and can be linked by intruders to find the correct username/password combinations. They can then unlock financial records and personnel information. Potentially controversial correspondence can be stolen and publicized to cause embarrassment and even compromise physical safety, as has been seen repeatedly in the news.

[1]WhiteHat Security: Website Security Statistics Report, May 2013, [2]www.beyondsecurity.com/web-security-and-web-scanning.html, [3]Ponemon Institute: The Impact of Cybercrime on Business, May 2012, [4]www.beyondsecurity.com/web-security-and-web-scanning.html, [5]WhiteHat Security: Website Security Statistics Report, May 2013, [6]HIPAA Security Rule, §164.316. Available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf, [7]WhiteHat Security: Website Security Statistics Report, May 2013, [8]www.owasp.org/index.php/Top_10_2013-Top_10

These and many other intrusions can go unnoticed by a hospital for months or even years. "Malware" (malicious software) can lie dormant or quietly gather information unnoticed until it is suddenly activated and "exfiltrates" (sends elsewhere) the stolen data before anything can be done about it or anyone even knows that it exists.

A recent alarming development has been the formation of efficient cybercriminal enterprises (usually overseas) that make it their business to search out and discover vulnerabilities and sell them to the highest bidder, rather than commit the attack themselves. "All over the world, from South Africa to South Korea, business is booming in what hackers call 'zero days,' the coding flaws in software like Microsoft Windows that can give a buyer unfettered access to a computer and any business, agency or individual dependent on one."[9]

Taking Aim at the Moving Target

Clearly the Web security landscape is changing constantly. Today's defenses are no guarantee of safety for months or even days ahead. But there is still much that can be done, and should be done. Most hospitals remain either unaware of the dangers or not convinced that a significant, proactive push for Web security is needed – until they suffer a major breach and data loss. And for hospitals everywhere, that's just a matter of time.

The Necessary First Step

In order to begin the journey to Web security, a hospital must start with a Web risk assessment. As part of that, a website should have a complete audit that evaluates the infrastructure code behind the website and in the applications themselves, particularly if a website is "home-built" (by the hospital's own IT department) and has never been audited. The Web risk assessment should be done by a third party.

You have to find out what your vulnerabilities are and how to address them. For example, CareTech Solutions, a healthcare IT and Web services provider, offers a thorough assessment that evaluates a website using both automated scanning tools and methodical "manual" investigation. The resulting report details how susceptible the website is to potential problems and documents what needs to be done.

There should be two critical components to any Web security assessment, both of which CareTech employs:

Part 1 - Automated Scanning Tools

Diagnostic scanning tools are run on the website that automatically check "mechanical" issues, such as: are there any open ports that might allow unauthorized entry; are the servers configured correctly and have they been patched as necessary; is there an open FTP site somewhere that's been overlooked? And many more. In addition, the latest scanning tools are aware of current and known "exploits" (attacks that take advantage of a vulnerability) and can test for them, past and present. Such tools can detect 70-80% of potential trouble spots. But more is needed.

Part 2 – Hands-On Evaluation

An indispensable part of the risk assessment of a website is for an experienced expert to also do a real-world, "human" review. Automated diagnostic scanners can locate and flag missing pieces, mistakes or inadequacies – but it takes a practiced professional who understands the business environment to check for the intangibles, by asking questions such as why a critical process is not doing its specific job. Using the analogy of a house, scanners can check whether you have locks on all the doors – but a real person has to ask if you actually take the time to lock them. Websites can have the latest security technologies, but administrators may still fail to use them or may bypass them for temporary convenience. So a proper assessment has to look at and understand downstream processes as well as what is apparent up front, and only the human factor has the intuition and flexibility for the final evaluation.

Too Much Information Leads to Risk

A common mistake that leads to unnecessary risk is asking for too much information from users. One of the most active areas of a hospital website is the employment section – people looking for jobs. The assessment may note that the request form on the site is configured properly and is secure, but is asking for more personal information, such as a Social Security number, than is actually needed for a preliminary interview. As a general rule, in all areas, a website is more secure if you only collect personal and protected information that you really need. If you're not going to use it, don't ask for it. And when you don't need it any more, delete it. Unnecessary information is data that does not have to be stored and therefore can't be stolen.

[9]The New York Times, "Nations Buying as Hackers Sell Computer Flaws," 7/14/2013, Vol. CLXII, No. 56,197

Fixing the Holes

It cannot be stressed enough that an expert third-party company should be part of the assessment and remediation mix. A hospital's own developers and programmers should not be counted upon to assess – and then fix – the security flaws in its website and applications that they themselves may have constructed. Without specific information, security training and certifications, a developer may not recognize weaknesses or know the latest remediation techniques.

The temptation is often to simply purchase a budget-friendly out-of-the-box Web application firewall that sits in front of a website and tries to monitor transactions coming to the website that have malicious intent. These "fixes" typically have little effect overall and can, in fact, delay getting to the root of a problem since they provide a false sense of security about the integrity of the applications themselves.

A Certified-Secure Content Management System

A hospital website is way ahead in the information security game if it is built upon a secure content management system (CMS) in the first place. When a CMS has been thoroughly tested and has been submitted to rigorous quality assurance and certification processes, there is much less chance of risk though the applications themselves. CareTech Solutions' CareTech CMS is such a system. CareTech was designed and built for hospitals. Fully PCI-compliant (Payment Card Industry), the "gold standard" of Web security certifications, CareTech CMS provides security integrated into the code that can't be supplied by an overlay like a firewall.

Security Equals Trust

On the positive side, there is an increasing awareness of the need for website security, especially as instances of major data breaches reach the news and create public outrage. As more and more people transact business of all kinds on the Web, they have to think about how the critical information they are providing is handled by the organizations with an online presence – especially hospitals – to which they are entrusting it. As that data is lost or mishandled, the public trust in the institution that allowed it to happen will certainly diminish, along with revenue. Website security has to move to the forefront of any responsible organization's concerns.

Additional Resources

Microsoft Security Intelligence Report, Vol. 14, July through December, 2012

Verizon 2012 Data Breach Investigations Report (DBIR)

Trustwave Global Security Report 2013

2012 HIMSS Analytics Report: Security of Patient Data

If you are interested in finding out more about how CareTech Solutions can support your website security needs, call us at (877) 700-8324 or visit our website at www.caretech.com.

Best in KLAS
Partial IT Outsourcing 2012
Extensive IT Outsourcing
2008, 2009, 2010 and 2011
Best in KLAS Awards:
Software & Services
www.KLASresearch.com

CareTech Solutions
901 Wilshire Drive
Troy, MI 48084
877.700.8324
www.caretech.com

CareTechSolutions®
Helping extraordinary people
do extraordinary things