THE SIX HIDDEN SSL VULNERABILITES IN EVERY NETWORK

Ensuring that your network is secure from every possible threat can be a full-time job. This challenge is heightened by the fact that many network admins only think about encryption and their SSL Certificates on an irregular basis. This article touches on some of the most common areas that companies inadvertently leave exposed to attackers.

OUT-OF-DATE SERVERS

You can be secure today and get hacked tomorrow if you simply "stand still". Neglected servers quickly become huge security liabilities. Failing to keep on top of operating system updates, patches, and new versions of your software creates new attack vectors for bad actors. This problem is amplified if these vulnerable servers contain the keys used to secure your network. The longer a piece of old software is sitting on your servers, the longer hackers have to find weaknesses in that software. "Keep the target moving" by keeping up-to-date.

Strongly consider decommissioning and unplugging servers on your network that are not providing a specific, important function. Keep on top of the software on your network. Utilities such as DigiCert's free SSL Discovery Tool help you identify certificates that are on the cusp of expiring or that are improperly installed.

You should also subscribe to blogs and newsfeeds detailing the latest exploits. Knowledge is your best defense.

INADEQUATELY-TRAINED OR OVERWORKED STAFF

Even after deploying a complex security plan and properly configuring all of the servers in your network with state-of-the-art SSL encryption, you can still end up with one glaring weak link in your precautions—poorly trained or overworked employees.

Whether these employees are part of your IT staff or are simply end-users scattered around your company, their risky habits and behaviors can quickly poke holes in your otherwise ironclad security. Every employee in your organization needs to be trained on security best practices and what to watch for in common exploits, both software-based and through social engineering. They need to know what "spear phishing*" is, how to spot suspicious activity, how to ensure sites are secured by HTTPS, and how to react when they see something unusual.

**Phishing is an attack on a person or organization where an attacker poses as a trusted entity to gain sensitive login information or even just general details about a network. Spear phishing is a type of phishing attack where the attacker initiates or solicits contact from a specific individual. The personalized nature of the attack increases the success rate, as opposed to typical phishing attacks that cast a wider net.*

Most of all, employees need training on reporting anomalies and to be given confidence that their concerns will be quickly investigated and are appreciated. Maintaining the security of your network is a collaborative team effort that depends on the participation of even the most junior employee.

YOUR INTRANET & MAIL SERVERS

Too many network administrators assume that internal servers behind a firewall are safe and that SSL Certificates are not needed on servers that are not public-facing. The failure to use multiple levels of security leaves your network vulnerable to the first hacker or malware that slips in. Once an attacker is able to sniff your network, the network becomes more susceptible to Man-in-the-Middle (MITM) attacks and attacks that intercept or compromise data on your servers. A hacker with access to your company email, proprietary code, and databases is a worst case scenario that is often preventable.

The best way to prevent these attacks is to deploy SSL Certificates on all external and internally-facing servers, regardless of the sensitivity of the data that resides on it or the traffic it manages.

FILE TRANSFER PROTOCOL (FTP)

First conceived in 1971, File Transfer Protocol (FTP) remains one of the most common ways to transfer large files across the Internet. FTP's low cost and ubiquity make it attractive to admins; a recent poll by Harris Interactive of 1,000 IT decision makers found that 51 percent of organizations use FTP to send and exchange large files.

Unencrypted FTP sites and file transfers are a treasure trove for attackers looking for easy pickings. The simple fact that passwords are passed in the clear is a significant risk. Add to that the fact that credentials and files are sitting in an unprotected server. While FTP is convenient for end-users, related exploits have been responsible for many of the most damaging network hacks in recent years. Even if you are not attacked via FTP connections, security auditors frown on its usage and what is typically inadequate monitoring on the part of the IT team. It's embarrassing when a regulator finds an unsecured FTP connection, let alone when a Google spider stumbles upon it and publishes it to the whole web.

"Unencrypted FTP sites and file transfers are a treasure trove for attackers looking for easy pickings."

Improperly-issued permissions are also a potential problem when limited users or even visitors end up with access to the entire directory, including other people's sensitive data. Avoiding FTP altogether is a safe bet, but if you are determined to implement it in your network environment, always protect your servers with secure transfer protocols. SCP (Secure Copy) and SFTP (Secure File Transfer Protocol) are alternative methods to consider.

SELF-SIGNED CERTIFICATES

Self-signed SSL Certificates are commonly used in development and testing environments and often on internal servers accessed by small groups of users. These certificates have a couple attractive benefits—they are fast and free! Unfortunately those benefits come with a big hidden cost. Namely, using self-signed SSL Certificates on your network is dangerous.

The problem is that, because self-signed certificates are not signed by a public CA, browsers encountering the certificate display a series of critical messages, causing confusion and alarm. Your users become conditioned to ignore vital warning messages. Once they adopt this behavior, your network loses an important deterrent—the vigilance of your employees.

To protect your network, you should issue publicly-trusted certificates for every site and server you manage, including internal resources. Wildcard SSL Certificates and Unified Communications certificates from Certificate Authorities (CAs), like DigiCert®, provide an easy and cost-effective means of protecting a complex environment without requiring a large number of single-name certificates.

An alternative, used by some enterprises, is to manage an internal CA that issues single SSL Certificate for internal sites. This is a headache for administrators as they need to configure every single browser and device to use the correct trust anchor. This approach is both costly and time consuming. In addition, an internal CA presents another attack surface to worry about in the security of your network. The high cost in obtaining and managing the additional infrastructure and expertise required to manage an internal CA makes using publicly-trusted certificates cheaper and more secure. Self-signed certificates are only "free" if you don't value your time.

FAILURE TO CONDUCT PENETRATION TESTING

Your network is a complex environment with potentially hundreds of exposed attack surfaces. A good penetration test (pentest) will help uncover potential holes in your network, helping you to seal them before they are discovered by an attacker. As you know, your network connections are constantly being probed; you can be sure that even if you aren't regularly conducting pentests on your network, the bad guys are.

The security requirements of your site dictate how often you run a pentest, but you certainly need to run one for any

major updates. Keep in mind that invasive pentests can cause bandwidth issues or otherwise break parts of your network. However, when you are the one conducting the pentest you can dictate when the testing takes place, and quickly diagnose the problems as they crop up. Avoid the urge to exclude big parts of your network during the testing—you can be sure that attackers aren't going to give you the same courtesy. If necessary, a pentest of your dev site can reveal most of the vulnerabilities on your sites.

There's no way to make your network 100% bulletproof, but tightening up or closing these common vulnerabilities will remove the low-hanging fruit that hackers are looking for.

USING THE RIGHT SSL VENDOR

Selecting the right Certificate Authority (CA) can greatly impact ease-of-use, speed of issuance, uptime, OCSP/ CRL latency, and a variety of features that make your network more secure and simple to manage. Using DigiCert® as your CA ensures both experience and leadership. DigiCert has been providing SSL Certificates and SSL management tools for nearly a decade. DigiCert assisted in developing the Extended Validation Certificate and worked with Microsoft to develop and promote the use of Subject Alternate Names in SSL Certificates. Unlike other CAs, that sometimes offer dozens or even hundreds of products unrelated to SSL encryption, creating and supporting top-shelf digital certificates is DigiCert's core business. This focused energy results in better products and unmatched service and support.

DigiCert has an award-winning in-house technical support team and has some of the fastest certificate issuance times out of any CA—with EV certificates typically issued in a matter of hours! DigiCert doesn't outsource customer support or have phone queues. Experience the "DigiCert difference" for yourself by calling 1-855-800-3444 or visiting *www.digicert.com*.

About DigiCert, Inc.

DigiCert is a premier online trust provider of enterprise security solutions with an emphasis on authentication, PKI and high-assurance digital certificates. Headquartered in Lindon, Utah, DigiCert is trusted by a continually growing clientele of more than 60,000 of the world's leading government, finance, education and Fortune 500® organizations. DigiCert has been recognized for its excellence in customer support and the workplace, and was applauded for its value-added product features with the 2011 Frost & Sullivan Customer Value Enhancement Award for SSL Certificates.

DigiCert, Inc.
2600 West Executive Parkway Suite 500
Lehi, UT 84043 USA
+1 (801) 701-9600
www.digicert.com