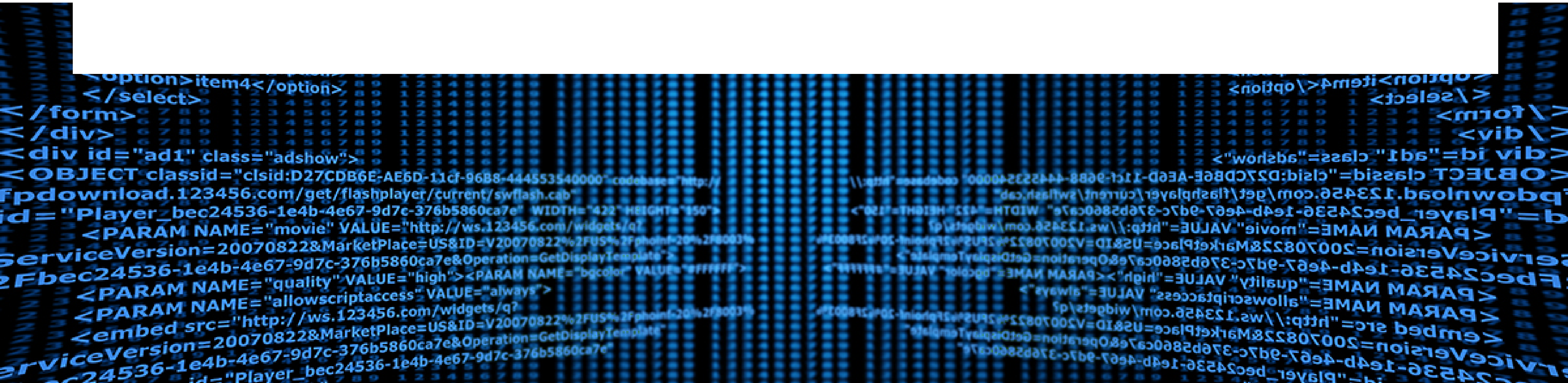
TechTarget | SearchSecurity

E-guide

PRO+ Content

Overcome SSL Security Issues: 7 Key Steps

The latest statistics and key insights on SSL threats



<option>item4</option>
</select>
</form>
</div>
<div id="ad1" class="adshow">
<OBJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://
fpdownload.123456.com/get/flashplayer/current/swflash.cab"
id="Player_bec24536-1e4b-4e67-9d7c-376b5860ca7e" WIDTH="422" HEIGHT="150">
<PARAM NAME="movie" VALUE="http://ws.123456.com/widgets/q?
ServiceVersion=20070822&MarketPlace=US&ID=V20070822%2FUS%2Fphoinf-20%2F8003
2Fbec24536-1e4b-4e67-9d7c-376b5860ca7e&Operation=GetDisplayTemplate">
<PARAM NAME="quality" VALUE="high"><PARAM NAME="bgcolor" VALUE="#FFFFFF">
<PARAM NAME="allowscriptaccess" VALUE="always">
<PARAM NAME="src="http://ws.123456.com/widgets/q?
<embed src="http://ws.123456.com/widgets/q?
ServiceVersion=20070822&MarketPlace=US&ID=V20070822%2FUS%2Fphoinf-20%2F8003
serviceVersion=20070822&MarketPlace=US&ID=V20070822%2FUS%2Fphoinf-20%2F8003
24536-1e4b-4e67-9d7c-376b5860ca7e&Operation=GetDisplayTemplate
id="Player_bec24536-1e4b-4e67-9d7c-376b5860ca7e"

In this e-guide

In this e-guide:

Most companies fall short when it comes to SSL traffic inspection, leaving their organization vulnerable to attacks.

In fact, new research shows lack of SSL/TLS inspection increases the risk encrypted traffic poses to enterprises as malicious actors take advantage of blind spots.

In this guide, uncover the latest statistics and key insights on SSL threats to see how other organizations plan to tackle the security issues hiding in their SSL traffic.

Plus, expert Rob Shapland will help you prepare and strengthen your web security plan with 7 essential steps to overcome these SSL issues.

In this e-guide

Report: Encrypted SSL traffic poses threat to enterprises

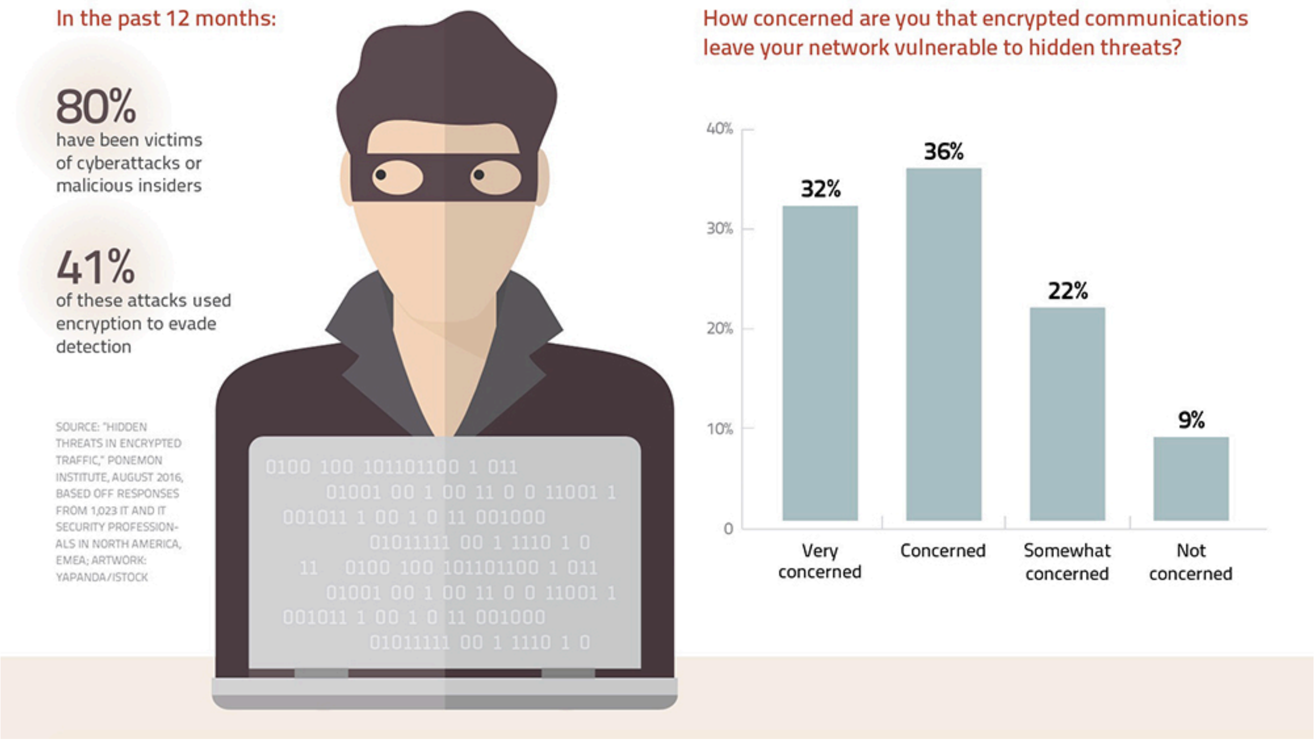
Kathleen Richards, Editor - Information Security

The numbers vary, but by all accounts, encrypted traffic is increasing on the internet. The problem? Most companies fall short when it comes to SSL traffic inspection, which creates a blind spot in inbound and outbound communications that may increase the threat of web-based attacks.

The SSL protocol uses authentication and encryption -- public-key and symmetric-key -- to secure communications between servers and other systems. It is frequently used to encrypt email, web transactions and data in transit, including data used by mobile apps. While the protocol usually works as intended, lack of visibility into SSL traffic is actually putting companies at risk, according to an August 2016 report by the Ponemon Institute.

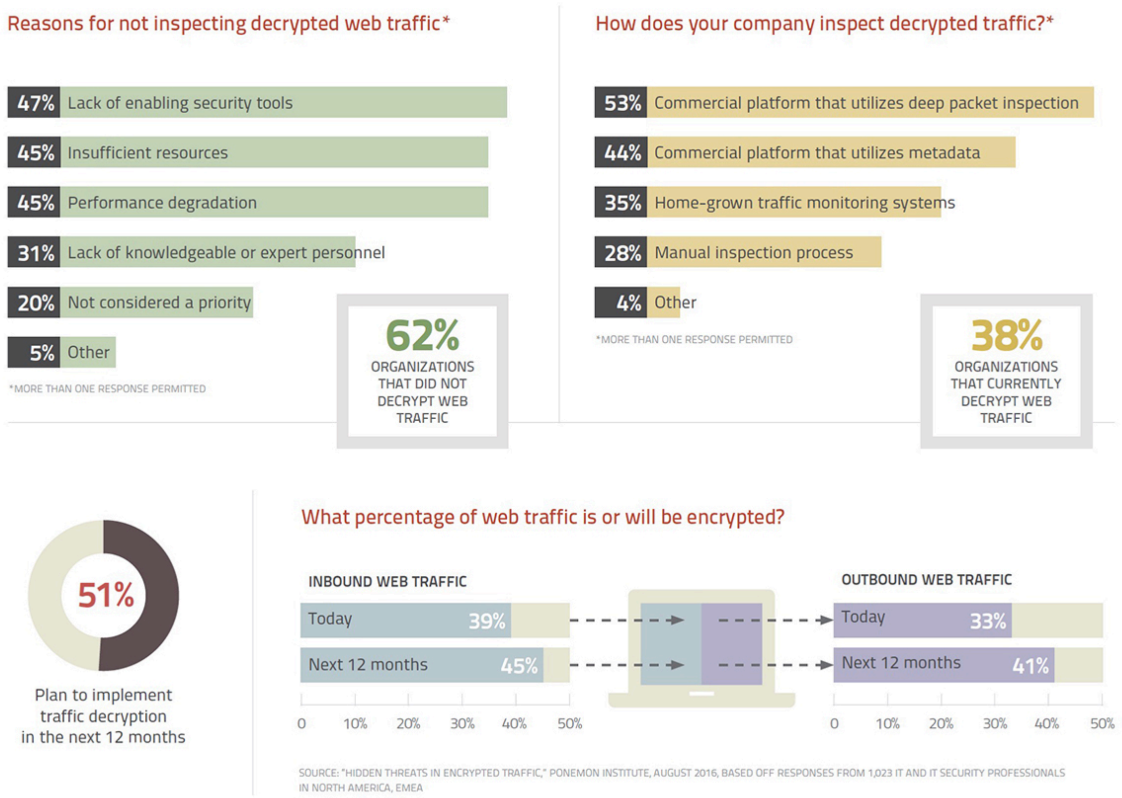
For the "Hidden Threats in Encrypted Traffic: A Study of North America and EMEA" report, sponsored by A10 Networks, Ponemon researchers independently surveyed 1,023 IT and security professionals. According to survey respondents, 80% of organizations have been victims of cyberattacks or malicious insiders in the past 12 months, and 41% of those attacks used encryption to evade detection.

In this e-guide



SOURCE: "HIDDEN THREATS IN ENCRYPTED TRAFFIC," PONEMON INSTITUTE, AUGUST 2016, BASED OFF RESPONSES FROM 1,023 IT AND IT SECURITY PROFESSIONALS IN NORTH AMERICA, EMEA; ARTWORK: YAPANDA/ISTOCK

The majority of those surveyed expect the potential dangers hiding in SSL traffic, such as malware and other intrusions that threaten to bypass security controls, to get worse in the next 12 months, the report found. While 51% of those surveyed indicated that their companies plan to install some form of traffic decryption in the next 12 months, 62% said they did not inspect decrypted web traffic.



SOURCE: "HIDDEN THREATS IN ENCRYPTED TRAFFIC," PONEMON INSTITUTE, AUGUST 2016, BASED OFF RESPONSES FROM 1,023 IT AND IT SECURITY PROFESSIONALS IN NORTH AMERICA, EMEA

The reasons range from lack of tooling and skilled personnel to network performance degradation and it not being a priority. The speed of SSL traffic inspection, its use of bandwidth and SSL key lengths also pose challenges, researchers said.

How to address key SSL security issues and vulnerabilities

Rob Shapland, Senior Penetration Tester - First Base Technologies LLP

Secure socket layer (SSL) technology has changed in recent years, and new vulnerabilities have also been discovered. This article explores the new SSL security landscape and outlines emerging security issues. Read on to learn the latest on these SSL security issues and the seven steps infosec pros can take to overcome them and implement SSL securely.

Step 1: The SSL certificate

The SSL certificate is a key component of SSL security and indicates to users that the website can be trusted. With this in mind, it must be obtained from a reliable certificate authority (CA) -- the larger the market share the better, as that means there is less chance the certificate will be revoked. Organizations should not rely on self-signed certificates. The certificate should ideally use the SHA-2 hashing algorithm, as there are currently no known vulnerabilities in this algorithm.

Extended validation (EV) certificates provide another means of increasing trust in the security of the website. Most browsers show websites that have EV certificates in a safe green color, providing a strong visual clue to end users that the website can be considered safe to use.

Step 2: Disable outdated SSL versions

Older versions of the protocol are a contributing factor to SSL security issues. SSL 2.0 has been compromised for a number of years and should be disabled. SSL 3.0, with the discovery of the POODLE attack, is now considered broken and should not be supported. The web server should be configured to prefer TLS v1.2 in the first instance, as this provides the most security. Modern browsers all support this protocol. TLS 1.1 and 1.0 support can be enabled for users running legacy browsers.

Step 3: Disable weak ciphers

Ciphers of less than 128 bits should be disabled, as they do not provide sufficient encryption strength. This will satisfy the requirement of disabling export ciphers too. The RC4 cipher should be disabled because of vulnerabilities that make it susceptible to attack.

Ideally, the web server should be configured to prefer ECDHE ciphers with forward secrecy enabled. This option means that, even if the server's private key was compromised, attackers would not be able decrypt previously intercepted communications.

Step 4: Disable client renegotiation

Renegotiation allows the client and server to stop an SSL exchange in order to renegotiate the parameters of the connection. Client-initiated renegotiation can lead to denial-of-service attacks, a serious SSL security issue, because the process requires far more processing power on the server than it does for the client.

Step 5: Disable TLS compression

The CRIME attack can be used to decrypt parts of a secure connection by exploiting flaws in the compression process. Disable TLS compression to prevent this attack. Also be aware that HTTP compression can potentially be exploited by the TIME and BREACH attacks; however, these are extremely difficult attacks to accomplish.

Step 6: Avoid mixed content

Encryption should be enabled on all areas of a website. Any mixed content -- where part of a page is encrypted and part is not -- can lead to the compromise of the entire user session.

Step 7: Secure cookies and HTTP Strict Transport Security (HSTS)

Ensure all cookies that control user sessions are set with the secure attribute; this prevents the cookie from being forced over an insecure connection and intercepted. In a similar vein, HSTS should be enabled to prevent any unencrypted communication to the website.

Follow these steps and the SSL implementation will be considered secure. However, be aware that dealing with SSL security issues is only one part of website security -- regular vulnerability scanning and penetration testing should be conducted to ensure that vulnerabilities elsewhere in the website are not compromising security.

Next article

In this e-guide

About SearchSecurity

IT security pros turn to SearchSecurity.com for the information they require to keep their corporate data, systems and assets secure.

We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security certification training resources, security standard compliance, webcasts, white papers, podcasts, Security Schools, a selection of highly focused security newsletters and more -- all at no cost.

For further reading, visit us at http://SearchSecurity.com/

Images; Fotalia