Making Everything Easier

Symantec Website Security Solutions Special Edition

Website Security

FOR DUMMIES®

A Wiley Brand

Learn to:

- **Make the business case for website security**
- **Explain how SSL forms the foundation of great website security**
- **Choose and implement the right SSL certificates for your website**
- **Follow best practice for maintaining a healthy and trusted website**

Symantec™

Website Security

FOR

DUMMIES®

A Wiley Brand

WILEY

Website Security

FOR

DUMMIES

A Wiley Brand

by Symantec

WILEY

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

For details on how to create a custom *For Dummies* book for your business or organization, contact CorporateDevelopment@wiley.com. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Visit our Home Page on www.customdummies.com

ISBN: 978-1-119-14155-6 (pbk); 978-1-119-14165-5 (ebk)

Printed and bound in the United Kingdom by Page Bros Ltd., Norwich

10 9 8 7 6 5 4 3 2 1

Table of Contents

Introduction

Welcome to *Website Security For Dummies*, your guide to understanding the risks posed by unprotected websites, the value of using SSL certificates, and the what and how of different types of SSL certificates. This book can help you keep your websites and your business safe.

About This Book

Website security is important for every business that has an online presence, but different companies have different needs and compliance requirements.

You don't have to read this book from cover to cover to get the information you need for your particular business. Instead, each chapter is self-contained and you can pick and choose what you need to know.

Website security can seem like a daunting topic, full of jargon and unfathomable workings. This book aims to remove as much of that as possible, and explain things in everyday language. Occasionally a bit of tech speak is necessary, but it's always explained.

So relax and prepare to become your company's expert on website security.

Foolish Assumptions

In writing this book, we've made a few assumptions about you:

- You are responsible for a business website.
- Your specialty is not necessarily IT: for example, you might be in marketing or you might be the CEO of a startup.
- You have some basic IT knowledge: for example you know what a server is, and you are familiar with ecommerce and other online transactions.

How This Book is Organized

Website Security For Dummies is a reference book, meaning you can dip in and out, but it is still arranged in a helpful order.

The first couple of chapters deal with the business side of website security. If you need to make a case to your boss, or even just figure out why website security is so important, these are the chapters for you.

Chapters 3–6 then cover SSL certificates, which are the foundation of website security. We cover the basics of how they work, what different types you can get and why you might need them, and how to manage your SSL certificates.

Chapters 7 and 8 cover other best practices for maintaining a secure and trusted website. Think of it as good hygiene.

Finally, Chapter 9 offers you some great sources for more information depending on your area of interest and tells you about some of the leading organizations that promote good website security.

Icons Used in This Book

To make it even easier to navigate to the most useful information, these icons highlight key text:

This icon is used to highlight a particularly useful bit of information or way of protecting your website.

These are points that you need to make sure you take away with you. They're necessary rather than optional.

Warnings indicate information that could seriously affect your site or business. You need to pay careful attention when you see this.

This tells you that some techy speak is coming up and you may want to avert your eyes or get a cup of coffee before you read them.

Where to Go from Here

To get to grips with the why and what of website security, start the conventional way at Chapter 1 and go from there. If you want to get straight down to practicalities then you probably want to start at Chapter 3 to get the low down on SSL. Then check out Chapter 4 and 5 to check which kind you need.

Other than that just dip in for what you need. Of course if you want to make sure you're fully covered when it comes to website security then read this guide from cover to cover.

Chapter 1

Building the Business Case for Website Security

In This Chapter

- Calculating the cost of ignorance
- Understanding the core principles of website security
- Using security to boost your bottom line

What's the first thing you do when you're looking for a new product or service? If your immediate response wasn't to say "Google it" then you're weird. Customers are savvy creatures and they don't just use websites to find out what you do; they also use them to figure out who you are and if you're trustworthy enough for them to hand over their hard-earned money to.

Whether you're in ecommerce or electricals; holiday rentals or hedge funds, your website is one of your most important business assets. It's your 24 by 7 shop front, and you need to make sure it's secure and working at its best.

You wouldn't leave your laptop behind when you leave a coffee shop or your stockroom door wide open, so why would you take chances with website security?

This chapter looks at the risks of ignoring website security and just how badly it can harm your business. We also explain the basics of what website security means in a way that you can pitch it to whoever controls the purse strings. And of course a business case wouldn't be complete without a look at the added benefits and return on investment that good website security can offer.

Calculating the Cost of Ignoring Website Security

Studies, surveys, and questionnaires galore have shown that an unhappy customer is much more vocal than a happy one. If your site triggers a security warning in the web browser of the visiting user or worse, it infects a customer's computer, that customer is going to tell all their friends and colleagues, and thanks to social media perhaps even the wider world. Ouch.

And it's not just your reputation that you have to worry about. If you have an ecommerce site, warnings and poor security will mean abandoned carts and lost customers.

In a recent Symantec, online consumer study, 56 percent of respondents go to a competitor's website to complete their purchase, and only 11 percent go back to the first website after seeing a security warning (Symantec Online Consumer Study, March 2011).

What you stand to lose

The potential costs of a data breach or a malware infection on your website go beyond the immediate cost of a lost sale or good-will payment. Your business stands to lose a lot more:

Money

Most customers, who don't see a visual clue proving your site is secure, won't trust you and you won't win their business. For the few that give you the benefit of the doubt, if they see a browser or security warning (see Chapter 3, 'Understanding Basic SSL Certificates' for more on browser warnings) then that's it: no interest, no purchase, no revenue.

If things get worse, and your site is blacklisted by search engines (Google alone identifies and flags some 10,000 unsafe sites daily according to their own website: `http://www.google.com/intl/en/goodtoknow/protection/internet/` the effect is almost the same as shutting down your site altogether. People won't be able to find you, and even once you're off the blacklist, your search rankings could be severely damaged. Lost visitors means lost revenue.

If you suffer a data breach there may be fines to pay or customers to compensate. A severe infection could mean you have to hire specialists to fix it. None of these things are cheap.

Then of course, there are the person-hours spent responding to website security breaches: you have to track down malware, search for vulnerabilities, renew or apply for SSL certificates, investigate any data loss, and update your systems and passwords.

The average recovery time from a cyber attack in 2012, according to Ponemon Institute's 2012 Cost of Cyber Crime Study sponsored by HP (`www.symantec.com/connect/blogs/cost-cybercrime-2012`), was 24 days, and the average cost was a staggering $591,780. That's time and money that could've been better spent on sales or development.

Reputation and trust

Once people see a browser warning or hear a news report about a security breach or malware infection that's your reputation blown. The general public is surprisingly well informed about online threats, and if there is any hint that their data won't be safe with you, then you can kiss their credit cards goodbye.

An expired SSL certificate warning, for example, suggests that you either don't care about security or that you've gone out of business. At the very least it suggests poor organization and if you can't keep your SSL certificates in order, what kind of customer experience are you likely to provide?

Search engine ranking

It can take up to six weeks to get off a search engine blacklist. During that time, when people search for your product or service, no matter how much lovely search engine optimization you've done, no one will find you.

Even without being blacklisted, browser warnings can damage your search ranking. If a visitor sees an indication that your site might not be safe they'll likely click away. The more often people click away after trying to access your site, the lower your search engine ranking goes.

Regulations and compliance

Website security isn't always optional. There are rules and regulations affecting processes such as data collection and storage, and payment transactions. Fall short of these and poor website security will cost you dearly.

Data protection is a vast topic and not one that can be covered in detail in this book. That said, there are some key points that you should be aware of. After all, when it comes to compliance, it's much easier to be proactive than reactive.

US data protection law

The US doesn't have one, single federal law relating to data protection. Instead there are several overlapping federal and state laws that relate to data protection, and how you handle your website visitors' and customers' personal information.

The Federal Trade Commission (FTC) is the main body that regulates ecommerce activities. They make sure you are sticking to your privacy policies – the promises you make to customers about how you collect, secure, and use their personal information. If you fail to meet their standards, you could face penalties or punishments. In 2013-14, for example, the FTC:

- Charged a free flashlight mobile app with sharing users' geolocation and unique device identification with advertisers without providing notice, or obtaining consent.
- Settled with a medical billing company over allegations that it failed to provide reasonable and appropriate security measures and procedures to protect consumers' personal information, including sensitive personal health information.

Working out what other agencies regulate your business and its website depends on your industry, where your customers are based, and how you use your website. For example, do you collect highly sensitive medical information? Who has access to the data you collect? Do you trade overseas?

While far from comprehensive this list is a good place to start to check what obligations you have beyond the FTC:

- **The Financial Services Modernization Act (Gramm-Leach-Bliley Act (GLB)):** This regulates the collection, use, and disclosure of financial information. It can apply broadly to financial institutions such as banks, securities firms and insurance companies, and to other businesses that provide financial services and products.
- **The Health Insurance Portability and Accountability Act (HIPAA):** HIPAA regulates medical information. It can apply broadly to health care providers, data processors, pharmacies, and other entities that come into contact with medical information.
- **State legislation:** There are also a lot of state laws that regulate the collection and use of personal data. Sometimes federal privacy laws on the same topic pre-empt state laws. For example, the federal law regulating commercial e-mail and the sharing of e-mail addresses pre-empts most state laws regulating the same activities. On the other hand, there are many federal privacy laws that don't pre-empt state laws, which means you might need to comply with both federal and state privacy laws that regulate the same types of data or types of activity.

We give you details on websites and organizations that can tell you more about laws that might affect your business's website in Chapter 9.

PCI compliance for sites that take card payments

If you accept credit cards on your site, the chances are that you'll have to be PCI-compliant. The PCI Security Standards Council is an open, global forum that sets standards for processing credit card payments. The council includes the five major payment brands—American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.

There are three key steps to complying with the Payment Card Industry Data Security Standard (PCI DSS): Assess, Remediate, Report.

Assess is where you 'identify all technology and process vulnerabilities that pose risks to the security of cardholder data that is transmitted, processed or stored by your business.' For an ecommerce site this means checking for vulnerabilities

in your site and the encryption of data that's passed between the site and the payment processing systems. In fact in the PCI eCommerce guidelines specifically call out that SSL should be used when transmitting cardholder data and they go further, advising all technical staff be trained to manage all security products including SSL. See `www.pcisecuritystandards.org/security_standards/documents.php?document=dss_ecommerce_guidelines_v2`

You also need to assess your processes. For example, protecting your private encryption keys, which we cover in Chapter 6, 'Managing Your SSL Certificates'.

Remediate and report are the fixing and confirmation stages, which prove you're being proactive about your security. To remain compliant you have to continually repeat this process, always being vigilant for vulnerabilities.

Understanding the Basics of Website Security

Making a business case isn't about confusing people with technicalities and long names: it's about conveying basic principles and arguments. This section looks at the two core features of website security provided by SSL certificates, and tells you what you're getting for your money in a way your manager will understand.

Authentication

When you apply for an SSL certificate you have to go through a business identity check. How rigorous this check is depends on the type of certificate you are buying, which is covered in subsequent chapters.

The more thorough the check, the more visual clues of authenticity your website visitors get, such as green address bars and padlock symbols.

These checks are done by whichever Certificate Authority (CA) you choose for your SSL certificate. They are third-party bodies. The best CAs are highly reputable and give you the credibility that customers are looking for when assessing your website. It is this validation and checking that is the bedrock of trust behind an SSL certificate.

Encryption

What SSL certificates actually do is enable encryption. This means that sensitive information exchanged via your website or between internal servers can't be read by anyone other than you. If hackers are able to eavesdrop they can't steal credit card details, name, email addresses, or other data such as intellectual property assets. It also means that data isn't modified in transit between servers and computers: so hackers can't insert malicious code into the messages and data.

In other words, SSL certificates are what keep data safe and help you comply with regulations, while enhancing your reputation and helping to increase your website conversions.

Using Security to Boost the Bottom Line

Used right, SSL certificates can help you to attract more visitors to your website, drive adoption of online tools, increase conversions and achieve greater online sales.

Different SSL certificates tell customers different things about how you are protecting their data, and earning their trust and custom. They also come with different additional features and layers of security. We explain the technical differences between these SSL certificates in Chapter 3, 'Understanding Basic SSL Certificates'.

In this section, however, we look at the business perspective, and explain how different visual clues and protection can help boost confidence in your business, and add value to your website.

Psychological comfort of privacy

People are becoming more and more conscious of the value of the data that companies can collect from them. It's not just about credit card numbers or email addresses, but behavior such as search terms and click-throughs.

Then there are all the news stories about prying spies and mass hacks by cybercriminals. People want privacy.

If your site uses Always-On SSL (which we explain in more detail in Chapter 5, 'Switching to Always-On SSL') site visitors will see 'https' in their address bar for the entire time they are on the site. This tells them that all their interactions with your site are encrypted, from the moment they arrive to the moment they leave. It gives them the comfort they want.

On top of that, visual signs of advanced SSL security, such as the green address bar, which is activated when a site uses Extended Validation SSL certificates, indicate that you are a legitimate business that underwent advanced validation in order to qualify for such a certificate. If you do this, it shows that you value your customers' and prospects' security as much as you value their business. If you do the same, it proves your company belongs with the big guys.

Secure before you click

People are not trusting. It's in our nature to be wary; it probably helped us not get eaten by lions in some bygone era. What it means today is when people are searching for information and products online, their default position is to assume a new site could be dangerous.

To help combat this, leading security software vendors have developed trust signals that show up directly in search results.

It starts before people even reach your site. If someone has the right security software and searches for 'costume jewelry', a list of sites will come up, but only those trusted by a particular Certificate Authority will display a symbol, like a trust mark, next to their name in the search engine results to prove their security and authenticity.

Figure 1-1: Example Symantec Seal-in-Search.

When people can verify the safety of a site before visiting it and without any risk on their part, they are more likely to click through, which not only increases your organic search traffic, but also improves your search engine ranking.

Trust marks

Trust marks are the symbols or logos that Certificate Authorities give you access to when you successfully deploy an SSL certificate. It's the visual stamp of approval, which indicates that a particular Certificate Authority trusts your site.

These trust marks encourage visitors to trust your business and your site. This translates into more conversions. And for ecommerce sites, tests carried out by ConversionIQ have shown that the revenue per customer (RPV) also increases when there is a trust mark present. See `www.cpcstrategy.com/blog/2013/01/case-study-symantecs-norton-ssl-and-mcafee-secure-trust-marks-increase-new-visitor-conversion-rates/`

This raises another important point for trust marks—where you put them. If people don't see the trust mark, they can't feel the trust. So it's worth displaying them prominently and at the right time—for example on your checkout page. It's also worth experimenting with A/B tests for different locations to find the best place.

Symantec's signs of security

Symantec is a well-known provider of internet security and a trusted Certificate Authority. Consumers might know them as Norton, but their products for businesses come under the Symantec brand.

Symantec secures more than one million web servers worldwide and Symantec SSL secures 91 percent of the 2013 Fortune 500 companies.

When you buy an SSL certificate with Symantec you also get:

- The Norton Secured Seal, which is the most recognized trust mark on the internet according to an International Online Consumer Research Study of November 2013, conducted by Symantec.
- Symantec Seal-in-Search, which puts the Norton Secured Seal next to your search results on enabled browsers and partnering websites.

Chapter 2

Recognizing Threats to Your Website

In This Chapter

- Who is most at risk from cyber attacks
- The different threats that businesses face
- Why authentication is just as important as encryption

Cyber criminals' best weapon is their victim's ignorance. Most companies simply don't understand how they attack websites. If you don't know where and how criminals attack, how can you know what a vulnerability looks like? Let alone begin to patch or remedy it?

This huge blind spot exposes vast numbers of businesses to easy exploitation: 77 percent of legitimate websites had exploitable vulnerabilities in 2013, according to Symantec's 2014 Website Security Threat Report, and one in eight of all websites had a critical vulnerability. Companies are basically going down to the local bar and leaving their back door wide open.

This chapter looks at the reasons criminals might target your business and your site and the most common attacks. We also discuss *watering hole attacks,* which make the need to authenticate your business more important than ever.

Assessing Your Risk Level

How much risk you face depends on a number of factors. The first step in figuring out what security you need is thinking about what the criminals might be after.

Consider the following to figure how much danger you're really in:

- **Company size**. No matter how big or small you are, you're at risk. Large companies have large revenues and vast quantities of data worth stealing, but they often have advanced security too. Small businesses, on the other hand, still collect valuable data, attract potentially lucrative visitors and have connections with larger vendors or buyers that could be exploited. At the same time, small businesses tend to have weaker website security and people often use the same password for all sites, making them easy targets.
- **Type of information you collect**. Credit card details, addresses, email addresses and password-reset hints are all considered juicy prizes by cybercriminals. Identity theft is very profitable. The more you gather, the more they have to go after. Identity thieves often seek three important data points; government ID information, date of birth and address. Having access to all three usually allows them to steal an identity.
- **Popularity of your site.** If you get a lot of visitors you could be a prime target for malware distribution. Criminals want to get their malware on to as many devices as possible. High-traffic websites make this quicker and easier.
- **The type of visitors you attract.** Business-to-business websites, for example, might attract potential customers from larger or more lucrative organizations. If criminals know their targets frequent your site, they'll look to exploit it.

Most Common Threats to Watch For

Different threats require different defenses, and to have a fully secure website you need multiple, overlapping layers of security.

It's like your home: you might have two locks on the front door, window locks and a burglar alarm. You need to figure out where you're most likely to get hit, and what will cause

the most damage in order to start building up effective, multi-layered protection.

See Table 2-1 for some of the most common vulnerabilities that cyber criminals look to exploit on your website. Using these vulnerabilities, criminals look to log keystrokes, steal data, distribute malware or even gather information for blackmail.

Table 2-1: Some of the ways criminals exploit unprotected websites

Vulnerability	*What it is?*
Unpatched servers	Attacks from compromised websites increased by 30 percent in 2012, according to Symantec's Internet Security Threat Report, Volume 18. Criminals mainly take advantage of well-known vulnerabilities in servers to infect them. There are published updates and patches for the majority of vulnerabilities used by hackers.
Authorization vulnerabilities	Weak passwords, compromised administrator user names, unchanged default settings on network hardware, and common software leave systems open to attack by people masquerading as legitimate users.
Cross-site scripting	Cross-site scripting (sometimes called XSS) means injecting code from one site (belonging to the bad guys) into another site (belonging to you). This lets internet criminals run their own code on your site to attack or infect visitors, or trick them into revealing valuable information, such as passwords.
Brute force attacks	Just like it sounds, these attacks simply power their way through all possible password and encryption possibilities until they crack the code to get into your site.

(continued)

Table 2-1:

Zero-day exploits	These are vulnerabilities that no one knows about until a criminal starts to exploit them. The attack begins on 'day zero' of awareness about the risk, and the numbers grew in 2013 as 23 new zero-day vulnerabilities were exposed, according to Symantec's Website Security Threat Report 2014.

Why Credibility is Crucial

The rise in cybercrime, in particular *watering hole attacks* and *spear phishing,* means that proving that you are who you say you are is more important than ever.

Watering hole attacks can take different forms, but the principle is the same. If criminals want to target a particular group, such as people in a particular company, they find out which sites they visit and then hack those sites with the aim of infecting the targeted visitors the next time they browse that particular site. You very definitely don't want to be one of the hacked sites.

Spear phishing is one technique that criminals use to get people to visit infected and fake websites. They gather information about the targets and then send them emails, social media messages or even sometimes phone calls to encourage them to visit a particular site. Sometimes the phishing sites are very sophisticated forgeries of real, trusted sites. This makes authentication—proving your identity—very important.

Businesses and individuals alike are therefore becoming particularly vigilant to the authenticity of websites. SSL certificates (especially Extended Validation certificates, discussed in Chapter 4) offer third-party proof that your site belongs to you and isn't a malicious clone.

Chapter 3

Understanding Basic SSL Certificates

In This Chapter

- What SSL certificates do and how they do it
- Choosing the right level of validation
- Choosing the right Certificate Authority

SSL certificates, or Secure Sockets Layer certificates, are the foundation of website security. They provide the technology to encrypt data and the third-party verification of your business identity.

This chapter looks at how SSL certificates work and how they should be used for your website. Understanding what SSL does will help you decide where it's applicable and what kind of SSL certificates you need.

This chapter also covers applying for a basic SSL certificate and what to look for when choosing a Certificate Authority.

Understanding How SSL Works With Your Website

SSL certificates aren't just for ecommerce sites—if you think about it, almost every site has some form of interaction or data exchange with visitors. It might be contact forms, social interactions, and blog comments, login details for an online application, or landing pages.

Pretty much every website, and certainly every business website will need at least one SSL certificate, and probably more.

Encryption in action

In order to understand how SSL works, you need to understand a few terms:

- **Browser:** This is the application you use to access the internet. Google Chrome, Microsoft Internet Explorer and Mozilla Firefox are all examples of browsers—there are of course many more than we can list here.
- **Server:** This is the engine that runs your website. Servers aren't just for websites (as you most likely know), but in this context it refers to the machine (or machines) that are connected to the internet, and that host your website.
- **Domain name.** This is the unique 'name' of your website, as it's registered. For example, google.com is a domain; google.co.uk is a different domain. The top-level domain is the last part, .com, .org etc. and the second-level domain is the website's actual name, for example, Google, Facebook etc.
- **Subdomain name.** Companies often use subdomains to offer different services with the same basic identity. For example, maps.google.com is a subdomain of Google.com. Hackers often use subdomains to trick their targets. For instance, google.hackahz.com has no relationship to Google.com
- **Cryptographic keys.** SSL encryption is based on a pair of cryptographic keys. These are pieces of information that actually encrypt and decrypt the information. Cryptographic keys are essential in any public key infrastructure (PKI)-based security.

So, this is—in simplified terms—what happens when a visitor visits a website that is secured with a trusted and up-to-date SSL certificate (this of course all happens within a matter of milliseconds):

1. **The visitor's browser attempts to connect to the website secured with SSL.**
2. **The browser requests that the web server identify itself.**

3. **The server sends the browser a copy of its SSL Certificate.**
4. **The browser checks whether it trusts the SSL Certificate.** It does this by checking if it trusts the Certificate Authority that issued the certificate. All major browsers come pre-installed with a trusted *root store with vetted public roots* from approved Certificate Authorities. This way a customer's browser automatically knows who to trust. If the browser trusts the Certificate Authority, it extends that trust to the website and sends a message to the server confirming that.
5. **The browser also checks the certificate status to see if the certificate is still valid, or if it has been revoked. This is generally done by one of two methods:**
   - Certificate Revocation List (CRL), a list of serial numbers of all revoked certificates that were issued by a particular CA certificate. The entire CRL is signed by the Certificate Authority so the browser can be assured that it's authentic and hasn't been tampered with.
   - Online Certificate Status Protocol (OCSP), in which a request is made for a specific SSL certificate and a response is returned that indicates whether that certificate is valid or revoked. The OCSP response is signed by the Certificate Authority so the browser can be assured that it's authentic and hasn't been tampered with. Most modern browsers rely on OCSP instead of CRLs.

   Certificates are revoked for various reasons, for example if they are improperly issued, or if the website owner has published false documents, or suffered a security breach that exposed private keys.
6. **Your server shares the public key with the browser. They use that key to securely agree on another key, the session key, that is used to set up a secure and encrypted channel to exchange data through.**
7. **Once a secure, encrypted connection is established, the visitor will see the website address begins 'https' rather than just 'http'.**

This process is known as the 'SSL handshake', and it's how SSL certificates work to prevent criminals eavesdropping and stealing information exchanged between websites and visitors.

Why visitors get browser warnings

The 'SSL handshake' will only work if the website in question has an up-to-date SSL certificate that has been issued from a trusted Certificate Authority. If any of these criteria are not met, the browser will interrupt the process and present the website visitor with a browser warning.

'Alice in Warningland', a study conducted by Google and the University of California, Berkeley, shows, for example, that two thirds of users will not click past an SSL warning of any kind. So it's important to avoid these warnings. See `www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe`.

These look different depending on the browser but usually give a brief explanation of why there is a warning and ask the visitor if they want to proceed. There are some examples in Figure 3-1.

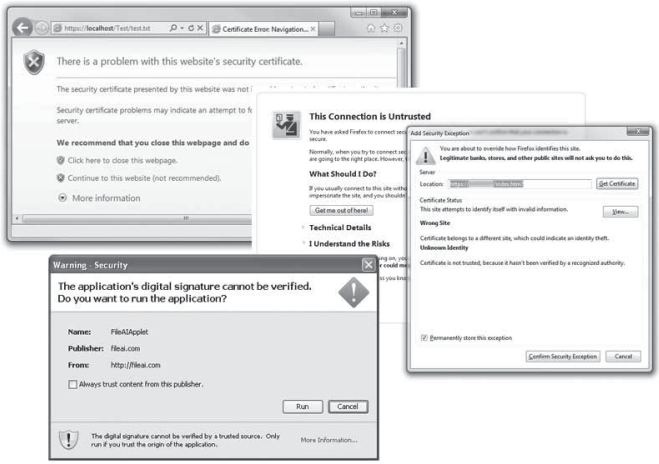

Figure 3-1. Browser warnings generated by different browsers that visitors would see if an SSL certificate is not trusted, is out of date, or does not match the domain name that the visitor is trying to access.

These are all pretty scary. You want to keep everything in order so that visitors to your site never see these warnings.

Figuring out how many certificates you need

You could get a certificate for each domain you want to secure, or you may be able to put multiple domain names in a single certificate. SSL certificates are based on what is called the website's *common name.* This is the host and the domain name. This means if you can access your website by typing 'www.example.com', and by typing 'example.com' you will need a separate SSL certificate for each. You may also need multiple certificates if you have multiple servers.

Some Certificate Authorities offer SSL certificates that cover a range of subdomains, known as Wildcard certificates, which are hosted on the same server, all on the same certificate. This means the top-level domain is the same, but you have different versions of the subdomain, for example, uk.example.com and us.example.com.

Getting the Right Level of Validation

There are many types of SSL certificates, which are each used to secure different applications. Even when it comes to SSL certificates designed specifically for websites, there are different sorts to choose between.

The more advanced type, Extended Validation (EV), is covered in Chapter 4, but this section talks about the two simplest types: Domain Validated and Organizational Validated SSL.

Why domain-validated certificates aren't good enough for businesses

Some Certificate Authorities will issue a domain-validated (DV) certificate to anyone who is listed as the domain admin contact in the WHOIS record. They just send an email to the contact email address, and that's it: not what you'd call very thorough.

So DV is the lowest level of authentication used to issue certificates.

As you can imagine, that's not much of a hurdle for a criminal to jump over: get an email address and buy a domain name. For example, if they were targeting BankOne.com they could register bank1.com and, using a free webmail account, get a domain-validated SSL certificate for that site.

Many website visitors therefore look for additional signs of authentication, such as Extended Validation, discussed in Chapter 4, which proves the site owners have been through more rigorous authentication.

Meeting the requirements of Organization Validation

Organization Validation, known as OV SSL, is the next step up from Domain Validation and it's a big step up. As well as checking on the ownership of the domain name in question, the Certificate Authority will also carry out some additional vetting to check the identity of the company and person applying for the SSL certificate.

This might include the address where the company is registered, and the name of a specific contact. The company name is taken from the certificate and then displayed in the browser's user interface. Figure 3-2 shows displayed OV SSL certificate information.

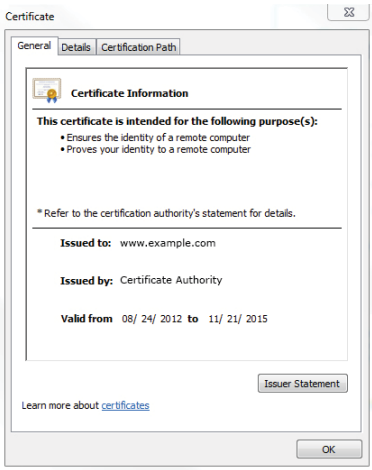

Figure 3-2. Example for displayed OV SSL certificate information in a web browser.

Choosing Between Different Certificate Authorities

There are a number of Certificate Authorities that you can buy SSL certificates from, and they are not all the same. Some have established a more trusted reputation, based on rigorous authentication, which in turn makes the certificates they issue more trusted by website visitors.

When deciding which Certificate Authority to go with, consider the following:

- **Have they ever been breached?** The security of your website is only as good as the security of the Certificate Authority protecting it. If they are breached, fraudulent certificates can be issued in their name, compromising the validity of your own certificate. Check their website and do a search to see if there have been any reported breaches, or serious security incidents.
- **Are they a member of the CA Browser Forum?** This is a voluntary group of Certificate Authorities and internet browser software vendors. It sets the minimum standards for different types of validation and encryption. You can find out more about the CA Browser Forum in Chapter 9. It's best to get your certificates from a member.
- **Who else uses them?** Look for case studies and statistics for how many companies, and what types of companies have chosen a particular Certificate Authority. If big names, or banks and other highly regulated industries are using them, they are more likely to be secure and reliable.
- **How much information do they require?** The more a Certificate Authority asks of you, the better. If they show a dedication to properly validating your identity, it shows that they are committed to online security, and it helps you establish better credibility with your customers. In addition, you can see if their procedures are audited to ensure they are following through on their checks. For example, Symantec's authentication practices are audited annually by KPMG.

- **How many browsers support their certificates?** Ideally you want your certificate to be recognized and trusted by as many browsers as possible, so that as many potential customers as possible will see your site is secure.

Understanding algorithms for encryption

When a website is authenticated by an SSL certificate, it allows data exchanged between website visitor and website server to be encrypted. This means criminals can't eavesdrop on confidential information.

How that data is encrypted is based on what algorithm is being used, and that is decided by the visitor's browser, the website server, and the SSL certificate itself. Different certificates enable different types of algorithms, and some are stronger and faster than others.

Elliptic Curve Cryptography (ECC) is one example of a more advanced algorithm that is available with certain premium SSL certificates from a few select CAs. It uses shorter encryption keys than the aging industry-standard RSA algorithm. This means your server is able to handle more encrypted connections at one time, without running out of processing power with lower cooling costs.

It is also stronger than the industry standard. For example, the ECC-256 keys are 10,000 times harder to crack than a 2048 RSA key. That might sound a bit abstract but a Dutch mathematician called Arjen Lenstra has come up with a way of explaining it that might make a bit more sense.

Lenstra compares the amount of computing power it would take to hack a cryptographic encryption with how much energy it takes to boil different quantities of water. So, it would take less energy to power the computers needed to break a 228-bit RSA key than it would to boil a teaspoon of water. To break a 228-bit ECC key, on the other hand, would require enough energy to boil all the water on earth. This is what Lenstra calls 'global security'. See `http://eprint.iacr.org/2013/635.pdf` for the original paper.

`http://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography` is a blog post with an explanation included.

Chapter 4

Achieving Extended Validation

In This Chapter

- Understanding what makes Extended Validation SSL different
- Giving visitors a visual clue to your credibility
- Gathering the right information to achieve Extended Validation

Website visitors look for familiar signs that indicate the site they are visiting is an official, authenticated site (as opposed to a fake clone site). A lot of *phishing* sites now exist that look very similar to legitimate ones. The intention of these phishing sites is to trick visitors into entering personal login details or bank details that criminals then steal.

Visitors therefore need proof that the site they're on is the right one, and that their data is only being shared with who they intend to share it with. While Organization Validation (OV) certificates (we cover OV SSL in Chapter 3) do confirm basic details about a website owner, Extended Validation (EV) requires a much more rigorous identity check.

This chapter looks at why it might be worth investing in EV SSL, and what you have to do to achieve Extended Validation.

What Makes EV SSL Worth It

When a site is authenticated with an EV SSL certificate, visitors will see a visual sign, most commonly a green address bar in their browser. This tells them that the owner of the website has had to provide detailed information about their company,

which has then been checked and audited by the Certificate Authority.

A little sign of reassurance can go a long way. For example, EV-secured sites often report increases in buyer click-through rates and conversions, and lower site abandonment.

In addition, many well-known brands and websites have adopted Extended Validation, including Twitter, HSBC, and the project management tool Basecamp.

The more popular your site, and the more sensitive the information you are asking for, the more likely it is that EV SSL will benefit your business.

What you need to prove to get EV SSL

The guidelines for what information you have to provide, and whether your organization is eligible for EV, are set by the CA Browser Forum (or CAB Forum for short). This is a group of Certificate Authorities and internet browser software companies that originally came together to reassure internet users by making better use of SSL certificates. See more about the CA Browser Forum in the sidebar at the end of this chapter.

The CA Browser Forum website goes into great detail about the types of bodies that are able to get EV SSL certificates, namely private organizations, government entities, and business entities. The common thread between them is that they all register themselves with a trusted third party, such as a local or national government organization.

If you are incorporated, or your organization falls into a more common business type, and you are based in a jurisdiction that provides good access to company registration information, it won't be too hard to get an EV SSL certificate.

When you apply you will have to provide quite a lot of information, some of which is mandated by the CA Browser Forum, and some, which the Certificate Authority has included for additional authentication. This includes a contact name and phone number for your business, which will be checked and verified.

If the Certificate Authority finds any discrepancies between your application and the public record, or independent register, they will contact you and ask you to rectify the error (if it is an error), or they will refuse to issue the certificate (if it's not an error).

Sometimes this can be a time-consuming process, but it is necessary for the Certificate Authorities to meet their own requirements for verification, to prove they are upholding the standards set out by the CA Browser Forum. For example, Symantec employs a team that is entirely separate from sales or support, whose sole purpose is EV authentication. They also keep a full audit trail, so they can reconstruct what they did for a particular investigation, even years later.

The CA Browser Forum

The CA Browser Forum was founded in 2005 by a combination of Certificate Authorities and browser software vendors. Its aim was to provide greater assurance to internet users about the web sites they visit by making more of the capabilities of SSL certificates.

In June 2007, the CA Browser Forum adopted version 1.0 of the Extended Validation (EV) Guidelines. EV certificates, discussed in Chapter 4, are issued after extended steps to verify the identity of the entity behind the domain getting the certificate. Internet browsers display additional information about the site owner's identity using different colors, icons, or website information.

The Forum has also adopted a set of 'Network and Certificate System Security Requirements', which all publicly trusted Certificate Authorities must comply with, and which all members are audited for.

Chapter 5

Switching to Always-On SSL

In This Chapter

- Differentiating Always-On SSL
- Understanding the motivations for implementing Always-On SSL
- Switching to Always-On SSL without damaging your search engine ranking

Most websites use SSL encryption on login pages or shopping carts, where confidential data is likely to be exchanged. This means some visitor interactions with a website are unencrypted, and as a visitor switches between the two it puts both their security and the safety of the website at risk.

Implementing Always-On SSL combats this risk by encrypting everything from the moment a visitor arrives on your site to the moment they leave. Always-On SSL is a cost-effective way of making it safer for website visitors to search, share, and shop online. Customers see an SSL encryption padlock in their browser during their entire visit, proving you are serious about both their safety, and protecting your business's reputation.

This chapter looks at the vulnerabilities that intermittent SSL encryption creates, and gives some pointers for ensuring you implement Always-On SSL properly.

What Makes Always-On SSL Different

Criminals can exploit any data exchanged between a web server and visitor, even if it's not a password or credit card number. For example, they can impersonate a legitimate visitor, or learn information that makes it easier to guess passwords. Always-On SSL stops criminals being able to eavesdrop on any communication between a website visitor and your server.

Say, for example, someone logs into a shopping site. The login page is secured with an SSL certificate so that the visitor's password is encrypted. Once the visitor leaves that page, however, they drop back onto an unsecured page of the site. At the same time, the website server sends over a *cookie* to the visitor's browser. This is a little bit of code that makes sure the server can recognize the customer as they move around the site. That cookie is sent unencrypted. A hacker can copy that cookie and use it to impersonate the real website visitor.

If a criminal is able to impersonate a customer that has already logged in, they can then access that customer's account details and, if a credit card is stored on the account, potentially spend money using it.

In addition, when a customer is hopping from secured to unsecured connections, it can trigger a security warning from their browser, just like the ones we talk about in Chapter 3, which encourage users to leave your site and abandon transactions.

Always-On SSL means a visitor will see the reassuring 'https' at the beginning of the address bar the whole time they are on your website.

Top Tips for Making the Switch

You may need to purchase additional certificates if different parts of your site run on different servers, and you also need to make sure you have implemented Always-On SSL properly so that there are no unencrypted gaps in your site, and so that you don't damage your search engine ranking and website performance.

Usually, the Certificate Authority that you purchase your certificates from can offer guidance on proper implementation, but these are some of the key steps to remember.

Redirection

When you switch to Always-On SSL, you are effectively moving your whole site to 'https', which is similar to moving to a new domain. This means you have to be sure to redirect all sites and pages to their new https counterparts. You also need to list the https site separately in Google Webmaster tools (we discuss Webmaster tools in Chapter 8).

Load speed

By enabling encryption across your site, there will inevitably be a small amount of extra processing power involved, so it may be worth assessing your web server infrastructure. The effect will most likely be minimal, and it's very rare that a slightly slower load speed will greatly affect your search engine ranking, but it's always best to check.

Unsecured connections

Be sure to disable all unsecured connections going to your web server, and carefully examine all the links and interconnections on your site to make sure they all have a secured connection to each other. No matter how a visitor navigates around your site, and no matter what link they click, their session must remain encrypted.

Staying ahead of the game

Certificate Authorities and mathematicians are always working to make SSL encryption better. That means making it harder to hack and less vulnerable if someone does manage to hack an encrypted session. We talk about how an SSL certificate establishes a secure, encrypted connection in Chapter 3.

The most exciting new development at the moment is Perfect Forward Secrecy (PFS) and big names like Twitter and Google are already using it. Instead of using the pair of cryptographic keys created when you install an SSL certificate to encrypt data, PFS uses those keys to securely establish a different set of keys. Those new, session-specific keys are never actually exchanged between the browser and the server, so there is no way for a criminal to get hold of them through a *man-in-the-middle* attack—in other words by eavesdropping on the conversation between the browser and the server.

This means that every new session that a visitor establishes with a website will be encrypted using different keys, so should a criminal hack one session, they won't be able to access any others. And should they steal the SSL certificate private keys, they still won't be able to hack any encrypted data exchanges that they may have been able to capture and store.

Chapter 6

Managing Your SSL Certificates

In This Chapter

- Assigning responsibility for website security and setting up procedures
- Using helpful software and automation tools
- Keeping private encryption keys safe

All types of SSL certificates have to be renewed on a regular basis. How often depends on what sort of package you buy from the Certificate Authority (CA) you choose, but certificates tend to remain valid for between one and three years.

The problem is, as you grow and get more certificates at different times, it becomes increasingly difficult to keep track of who bought what, from where, and when. This becomes an even bigger problem when someone misses an expiration date, and fails to renew a certificate.

When this happens, anyone visiting the part of your site secured by that certificate will see a browser warning (see figure 3-1). And this in turn has a big impact on customer trust and sales. In fact, in a Symantec online consumer study, 91 percent of respondents will not continue a transaction if they see a browser warning page indicating the absence of a secure connection.

Without good SSL certificate management, employees will also often sign up for new certificates for their particular project without thinking about the credibility of the CA, or type of certificate that is most suitable for the business as a whole. This can result in people deploying *rogue certificates.*

Rogue certificates are SSL certificates that haven't been issued by a trusted CA, but instead have been self-signed or may have been issued by a CA that doesn't adhere to the CA Browser Forum standards, or standards for compliance with regulations such as Data Protection or PCI. We discuss these standards in Chapter 1, 'Making the Business Case for Website Security'.

In other words, rogue certificates do not offer the level of authentication and security that trusted CAs provide and, as with expired certificates, result in a browser warning when visitors attempt to visit a site secured by such a certificate.

This chapter looks at steps that you can take to make sure all your SSL certificates are kept up to date, issued by approved CAs, and are managed securely within your company.

Keeping Track of Who Knows What

Good processes are vital to good management of SSL certificates. The more people involved in website security, the greater the risk that something gets forgotten, lost, or compromised.

Responsibility

Centralize the management of your SSL certificates and put someone specific in charge. For bigger companies you might need more than one person, but you should keep the number of people involved to a minimum and have a single point of responsibility for overseeing the team.

Doing this means you know exactly who is authorized to buy and renew certificates, and you can ensure they know and follow company procedures for doing so. However, having only one person who keeps track of all SSL certificates is a risk; that person might go on vacation and fail to renew a certificate in time.

Handover procedures

One of the main reasons that SSL certificates expire is that the person who bought them has moved departments, or left the company. Centralizing management reduces the risk of this happening, but you still need a repeatable process for handovers for when the SSL management team changes.

Make sure all information about certificates—renewal dates, types, CAs they're issued from etc.—is stored in a secure company folder. You don't want the SSL manager keeping the data on their personal device, or in their private folder. Not only does this pose a security risk, it also means if they leave the company, you lose access to your management data.

When your SSL management changes you also need to change all passwords associated with your certificates. This includes access to the company folder, access to servers, and access to encryption keys (see 'Protecting your private keys' for more advice on this).

Tools to Help Things Run Smoothly

There are tools to help you manage your SSL certificates. They provide a secure place to store your SSL management information, and they can automate certain parts of the renewal process to help you save money and time. Symantec, for example, offers a few different tools, suited to businesses big and small.

Tools exist both for small businesses and larger enterprises. At a basic level they usually consist of a cloud-based repository for your SSL information, and a dashboard for monitoring expiration dates. This means you can simply log in to your account via a web browser, and all your SSL information is in one place, even if you have certificates from lots of different CAs.

These tools also help you with the hidden financial and time costs of SSL management:

- **Purchasing costs:** Buying SSL certificates in small quantities can be time-consuming. There are online forms to complete, purchase orders to raise, payment details to obtain, and so on. Central management helps you deal with your certificates in bulk.
- **Inventory tracking costs:** An accurate inventory is essential for preventing disasters, and is also an important part of good housekeeping. Which certificates are due to expire this month? If we virtualize these servers, what certificates will be affected? These, and many other common questions, are easy to answer with an automatically updated management tool.
- **Last-minute panics:** Even if you discover that a certificate is about to expire, getting it replaced at short notice can be hard work. It's much more efficient to renew large batches of certificates in one sitting than repeatedly rushing to do one or two renewals at the last minute. But to do this you need enough advance warning about expiry dates, which is exactly what these tools provide.
- **Missed opportunities for bulk purchasing**: Centralizing certificate management makes it easier to use a single, preferred CA for all your certificate purchases. This can unlock bulk discounts, and ensure that every certificate meets company standards.

More advanced tools also allow you to define management processes so that you can apply them consistently across the whole organization. You can then delegate certain tasks, or give access privileges to different business units without losing control or oversight.

Protecting Your Private Keys

Chapter 3, discusses how private keys are used to enable encryption of the data that visitors exchange with your website. No one should ever have access to your private keys.

Your private keys, quite literally, establish your online identity and enable encryption of data when in transit. Anyone who

has access to them can unencrypt that data. In fact, cyber criminals often find it is easier to hack into company networks and steal encryption keys, than it is to hack the encryption itself.

E-commerce sites in particular have to pay attention to private key security as those keys enable encryption of credit card information in transit. This process is regulated by the PCI, and poor private key management could mean you're falling short of compliance standards. We discuss PCI standards in more detail in Chapter 1.

If someone else gets their hands on your private keys, they also have the ability to set up SSL certified websites under your company name. These potentially malicious sites will appear to visitors as entirely legitimate—after all, the criminals have used a trusted CA's SSL certificate to authenticate it. Anyone infected by malware from that site will blame you.

Follow these best practices to keep your private keys away from prying eyes:

- Keep servers with keys separate from the company network in case criminals hack their way into your network through a malicious email or social media phishing. Limit the number of people with access to keys, and the number of machines that they are duplicated on. Just like with real keys, the fewer copies you have, the easier they are to keep track of.
- Have separate administrators for managing the passwords for the server where the keys are stored, and for managing the systems the keys are actually stored in.
- Use an automated certificate and key management system to reduce human involvement in the private key generation and storage process.
- Regularly change your passwords, and be sure to have different passwords for each of the locations where your keys are stored.
- Anytime a member of the administration team changes, change the keystore passwords.

Symantec's helping hand

Symantec is one example of a Certificate Authority that has created tools to help companies of all sizes manage and maintain their SSL certificates.

For smaller businesses, there is the Symantec Trust Center, which lets you manage all your Symantec SSL certificates, and other SSL products in one place. It's an online portal where you can view and update your certificate and contact information, and purchase or renew certificates.

For mid to large-sized companies there is the Symantec Certificate Intelligence Center. This lets you automate some of the certificate lifecycle management. It also looks for and monitors any SSL certificates from other Certificate Authorities, including any internal CAs, to help you keep on top of things.

Finally, for larger enterprises that have lots of different SSL certificates, managed by different administrators across different business units, Symantec offers Managed PKI for SSL. This tool lets you customize the workflow for acquiring SSL certificates, delegate authority to different managers, and it enables instant issuing of certificates on pre-approved domains.

Chapter 7

Best Practice for Keeping Website Servers Safe

In This Chapter

- Installing updates and patches
- Remaining vigilant for vulnerabilities
- Minimizing the risk from employees

In order to keep your visitors and your business safe, you need to ensure there is no malware lurking on your website, or the server(s) that run it. Malware can do bad things including:

- Monitoring traffic to and from your website
- Capturing encrypted and unencrypted exchanges between your site and your visitor's computer
- Deploying malware on to visitor's devices
- Gaining access to your server, and worse, your company network, exposing data and devices to criminals

Cyber criminals can even buy *toolkits,* which are like off-the-shelf software packages that allow them to hack or exploit certain website vulnerabilities. This means that even criminals who aren't expert coders can attack your website.

This chapter therefore looks at the best ways to keep your web servers, safe and helps you figure out where your weak points might be.

Keeping Your Systems Up to Date

Your website servers are the same as any other device connected to the internet or a company network. And just as you have to update, manage and maintain PCs and laptops and the software on them, you have to do the same with servers.

The servers themselves have an operating system. Then there is the application software that serves up web pages to site visitors. Plus, many websites also use content management systems to allow non-technical users to create and edit web pages.

Any of these layers of software can contain vulnerabilities that leave them open to infection by malware. More often than not, criminals exploit a vulnerability that is known about, and which is easily fixed. The problem is so many people don't keep their hardware and software up to date that weaknesses remain unfixed.

Keep all your software and hardware up to date so that you are running the latest version, and have any patches or updates installed. Vendors issue patches in response to either criminals or their own teams finding weak spots. If you don't install the updates, you are potentially leaving yourself open to attack.

Conducting Vulnerability and Malware Scans

Despite your best efforts to stay up to date, you may miss certain vulnerabilities. This is where third-party scanning comes in. Many vendors and Certificate Authorities offer vulnerability and malware scanning for websites. For example, Symantec includes free scanning when you buy SSL certificates from them.

We discuss these scans in more detail in Chapter 8, but basically they look for weak spots you've missed, and hunt out any malware that has found a way in—and where it's hiding—so you can take action to remove it.

This type of scanning is an essential part of a multi-layered security strategy. Symantec's Website Vulnerability Assessment Services scanned thousands of websites in 2013. Over three quarters of the websites scanned were found to have unpatched, potentially exploitable vulnerabilities. Of the vulnerable sites, 16 percent had critical vulnerabilities that could 'allow attackers to access sensitive data, alter the website's content, or compromise a visitor's computer,' says the Symantec Website Security Threat Report, 2014.

Minimizing Access

Finally you need to consider the physical security of your servers. A disgruntled or careless employee can expose your website to malicious code, or help external criminals sneak their way in.

These are some of the best ways to minimize risk:

- **Two-factor authentication** for access into the servers. This means using two forms of identification rather than just one. For example, you might need to use a password and a card reader to log in. (This is a little bit like using bank ATMs where you need both card and PIN number to use the ATM.)
- **Dual key access** for servers, so two different people have to be present at the same time when logging into a server.
- **Limited network access** means that if criminals do manage to hack their way into your site, your entire company network won't be exposed. And vice versa, if criminals hack their way into your network, your website is potentially protected.
- **Restricted access** simply keeps the number of people who have access to your site servers to a minimum, making it easier to monitor or control any rogue access.

Avoid using a browser on any system that's running a web server. Many systems are put at risk by malware that's downloaded through a browser visiting a malicious web page. To keep your web servers safe, make sure no one ever runs a web browser on those systems.

Chapter 8

Maintaining Good Website Security

In This Chapter

- Teaching staff the basics
- Staying vigilant and up to date
- Using Webmaster tools to watch out for blacklisting

Criminals are always looking for new ways to hack, exploit, and make money. Their ingenuity and constant advances in computer technology mean that the field of website security is constantly evolving.

This is why having SSL certificates and a secure server is essential, but not sufficient. For really effective website security you also need vigilance, education, and good maintenance practices. The human element is considered the weakest link in the security chain.

This chapter looks at what your employees need to know about online threats in order to keep your site safe. We also cover how website scans, Webmaster monitoring tools, and a little planning can keep threats (and their impact) to a minimum.

Making Sure Everyone Knows What to Watch For

While the focus of this book has been website security, there are of course lots of other online threats that individuals and businesses face. Some of those threats can also put your website at risk.

For example, if an employee opens an attachment in an email from an unknown sender, they could end up releasing malware onto the company network. If your web servers are connected to your company network, or any server passwords or cryptographic keys are stored anywhere on the network, criminals might be able to gain access to them, and use them to compromise your website.

Teach your employees what to watch for when using their work devices, including:

- **Social media phishing.** People publish so much personal information on social media sites that criminals are starting to use it to trick people into clicking on malicious links or providing sensitive information. It might be a fake voucher or a link to a site that seems to be posted by a friend.
- **USB lures.** Criminals have been known to load malware onto a USB stick (or several) and then leave them on the ground in the car park outside the company they are targeting. Human curiosity means that employees pick them up and plug them into their computers, and consequently unknowingly infect the company network. Train employees to take any unidentified USB sticks or discs straight to IT.
- **Email phishing.** Targeted attacks have become increasingly sophisticated and convincing in recent years. Criminals sometimes call ahead to prep the recipient for an email. A recent example in France saw employees in the finance department targeted. The criminals would call ahead claiming to be from a company waiting to be paid by the target company. They would warn that they were resending their invoice, and that they wanted it paid immediately. The email would then arrive, the

employee would open the attachment, and the malware would be unleashed.

- **Unsecured websites.** Throughout the first five chapters of this book we discuss the various benefits of SSL certificates, including the fact they authenticate the owner of the website, and they encrypt data sent between visitor and site. It's important to teach your employees about this in relation to the sites they visit at work. They need to know to look for a green address bar, or 'https', to be sure they are not being tricked by a cloned website.

Implementing Effective Damage Limitation

Sometimes, despite your best efforts, you may suffer a security breach on your website. The most important thing to do is find out as fast as possible, and react the right way to minimize impact.

Regular website scans

While some malware causes lots of disruption, and takes down servers, often criminals want to keep their malware running on your website server undetected, so they can continue to steal information and look for other weaknesses to exploit.

In addition, criminals are always finding new vulnerabilities in software that they can exploit, meaning new forms of malware emerge. Daily or weekly malware scans are therefore vital in spotting any breaches as soon as possible. A malware scan will usually not only spot the malware, but will also extract the code that needs to be removed to solve the problem.

For the same reasons, you also need to regularly scan your site for vulnerabilities. Again, usually, a vulnerability scan will provide an actionable report that identifies both critical vulnerabilities that should be investigated immediately, and items that pose a lower risk. This helps you prioritize budget and effort in maintaining a secure website.

Webmaster tools

When you sign up for Google and Bing Webmaster tools, you will get instant notification in the event your site is ever blacklisted. This is definitely preferable to suddenly noticing that your website traffic is dropping off.

Notification from these tools means you can act faster to find the problem, fix it, and get taken off the blacklist.

Disaster recovery plans

Hope for the best, plan for the worst. If you suffer a data breach or malware infection, it's best to have a set of procedures in place that will help you get back on your feet as quickly as possible.

What goes into your plan will depend on what industry you are in, what sort of data your website collects, and the jurisdictions you work in, but the following points are worth considering:

- **Who** do you need to inform of the problem? Do you have to tell customers or an external regulatory body? Who is responsible for informing them?
- **What** data is actually at risk? Do you know what networks are affected, and which files need to be checked to see if they've been compromised?
- **Why** has the breach occurred? Who is responsible for tracking down and fixing the vulnerability that caused the problem?
- **When** did the breach occur? How much data is compromised?
- **How** much is the breach costing in terms of lost revenue, person-hours, compensation, or fines?

Someone needs to be in charge of both developing this plan, overseeing it should it ever have to be put into action, and reviewing it regularly to make sure it's still relevant and useful.

The Heartbleed Bug

In both this Chapter and Chapter 7, we talk about the importance of maintenance and keeping servers up to date. The newsworthy security incident surrounding SSL, called the Heartbleed Bug, demonstrated exactly why this is so important.

What the Heartbleed Bug actually did is a bit complicated, but it's enlightening to understand the problem, and it'll be a good test to see if you've been paying attention along the way!

When a browser and a web server establish a secure connection using SSL certificates, it's useful to be able to maintain that connection, even if no data is actually exchanged for a while. You wouldn't want to have to keep logging into the same site over and over again, would you?

On many web servers, an open-source cryptographic library, called OpenSSL, implements the SSL functionality. OpenSSL uses a 'heart beat' to keep secure connections open. It regularly sends a message to the server, which in turn relays that message back to the sender, verifying the connection.

The message it sends contains two components: a packet of data known as the payload which can be up to 64KB, and information on the size of that payload.

The Heartbleed vulnerability in OpenSSL allows an attacker to pretend they're sending a bigger data packet than they actually are.

How OpenSSL deals with this message is what makes it dangerous. It doesn't try to check if that payload is actually the same size as it's told it is. Instead, it assumes that the payload is the correct size, and attempts to send it back to the computer it came from. However, since it doesn't have the full 64KB of data, it will instead automatically 'pad out' the payload with data stored next to it in the application's memory. This could include the login credentials of a user, personal data, or even, in some cases, session and private encryption keys.

The only way to fix this vulnerability was to update your servers to the new version of OpenSSL. Updates are always important, but, as in this case, sometimes they are absolutely essential. It's important to note that this was not a weakness in SSL, but in this commonly used open-source program.

Chapter 9

Ten Useful Sources for Information on Website Security

In This Chapter

- Where to go for information
- Who they are
- What they can tell you

This book gives you the basics on website security, but you might want a little more. Perhaps you work in a highly regulated industry, and need more details about compliance, for example.

Or maybe you'd like more information for educating your employees about online threats?

The following bodies, organizations and resources aim to educate, inform, and aid when it comes to website security.

CA Security Council

`casecurity.org`

The CA Security Council (CASC) is 'comprised of leading global Certificate Authorities that are committed to the exploration and promotion of best practices that advance trusted SSL deployment and CA operations as well as the security of the internet in general. While not a standards-setting organization, the CASC works collaboratively to improve understanding of critical policies and their potential impact on the internet infrastructure.'

Their website offers a lot of informative blogs and whitepapers that help educate the public on security threats, attacks, and other news related to Certificate Authorities.

Certification Authority Browser Forum

cabforum.org

The Certification Authority Browser Forum, or CA Browser Forum, is a group of Certificate Authorities and internet browser software vendors that came together in 2005 in the hope of better reassuring website visitors about the security and authenticity of the sites they were visiting.

The group aims to work together to make more of SSL certificates, in particular in relation to verifying site ownership and business credibility.

The website offers information for individuals, businesses, coders, and auditors. They give a nice introduction to SSL certificates, and how to install them. As the creators of the guidelines for Extended Validation SSL, which we talk about in Chapter 4, they also provide lots of info on that.

Symantec Website Security Solutions

http://www.symantec.com/ssl-certificates

Symantec, one of the leading Certificate Authorities and a founding member of the CA Browser Forum, has lots of resources dedicated to helping you understand website security.

You can learn about the different types of SSL certificates and website security tools that Symantec offer, and you can also download the Symantec Website Security Threat Report, which looks at current trends and statistics in the website security world.

Online Trust Alliance

otalliance.org

The Online Trust Alliance (OTA) was formed in 2005, and is a global, non-profit organization, headquartered in Bellevue, Washington. They describe themselves as 'an informal industry working group… with the mission to enhance online trust and empower users, while promoting innovation and the vitality of the internet.'

The site offers lots of information on best practices on topics like Always-On SSL, data protection guidelines, mobile app security, and Certificate Authorities. They also run specific initiatives around issues such as brand reputation.

Electronic Frontier Foundation

https://www.eff.org

These guys are a bit more focused on the effects of technology and online security on individuals and consumers than businesses. They were founded in 1990 and they champion 'user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development'.

What they say could affect how you approach website security, especially if your aim is reassuring visitors. They produce several whitepapers about where the law and technology meet, which are worth a read, especially if you're in a more regulated industry.

PCI Security Standards Council

https://www.pcisecuritystandards.org

As we talk about in Chapter 1, these guys are the regulatory body you need to be aware of if you take financial transactions on your website. Again, it's an open global forum that was founded in 2006.

As well as all the information you could want on online credit card transactions, they also give help and guidelines about other forms of credit card payment, like mobile payment and card swipe payments.

U.S. Small Business Administration

`http://www.sba.gov/content/online-business-law`

According to its website, 'The U.S. Small Business Administration (SBA) was created in 1953 as an independent agency of the federal government to aid, counsel, assist and protect the interests of small business concerns, to preserve free competitive enterprise and to maintain and strengthen the overall economy of our nation.'

This particular page relates specifically to laws affecting online businesses, and provides links and resources that can help you understand your regulatory obligations, as we talked about in Chapter 1.

The Federal Trade Commission

`https://www.ftc.gov/tips-advice/business-center`

We also mentioned this government agency in Chapter 1. They are the main body that regulates data protection in the US. As the website states, 'The FTC is the only federal agency with both consumer protection and competition jurisdiction in broad sectors of the economy'.

This particular page of the FTC website offers tips and advice for businesses and covers topics including, advertising and marketing, and privacy and security.

Google Webmaster

http://www.google.com/webmasters/

Signing up for Google's Webmaster tools does a lot more than let you know when you're blacklisted. The tool also gives you tips and analyses of your site to help you make it more search-friendly and get found on Google.

Symantec Connect

http://www.symantec.com/connect/security

As we mention earlier in this chapter, Symantec is a leading Certificate Authority. Symantec's robust PKI infrastructure includes military-grade data centers and disaster recovery sites for customer data protection, availability, and peace of mind. That's probably one of the reasons that as of September 2013, according to a Netcraft SSL survey, half of websites using Extended Validation SSL choose the Symantec brands, including some of the biggest names in ecommerce and banking.

This site is where 'Symantec business customers, partners, and employees find solutions, share technical knowledge, and submit product ideas.' It's a collection of blogs and discussions focused around different online security topics, including website security of course.

Symantec | Website Security Solutions

Secure your website and grow your business

Symantec Website Security Solutions include industry-leading SSL, certificate management, vulnerability assessment and malware scanning. The Norton™ Secured Seal and Symantec Seal-in-Search assure your customers that they are safe from search, to browse, to buy.

Norton SECURED
powered by Symantec

Norton Secured Seal

Viewed over a billion times a day in 170 countries[1].
90% of respondents more likely to continue online transactions if they see the Norton Secured Seal[2].

Vulnerability Assessment

6,787 vulnerabilities reported in 2013[3].
A weekly scan helps identify and act against exploitable website vulnerabilities.

Malware Scanning

67% of identified malicious sites are regular websites[3].
A daily scan detects and reports malware to site owner.

24-hour support

24/7, 365 days a year.
A dedicated technical account manager.

01001
00101
00111

Even stronger encryption

Elliptic Curve Cryptography (ECC) Algorithm[4].

To learn more about Symantec, contact your Security Advisor today

Call 1-866-893-6565 or 1-520-477-3111 or visit www.symantec.com/ssl

[1] Symantec internal customer data. [2] International Online Consumer Study: US, Germany, UK, July 2013.
[3] Symantec Website Security Threat Report 2013.
[4] An ECC certificate is included at no additional cost with all Symantec Premium SSL certificates.

Understand why a secure website means a successful business

Potential customers know the internet is a dangerous place, which is why they won't give away their data without proof that you'll keep it safe. This guide explains how SSL certificates, best practice maintenance and a bit of A/B testing can vastly improve your credibility and help you win over wary website visitors.

- ***Establish credibility* – demonstrate you've been through a business identity check by obtaining SSL certificates from a trusted certificate authority.**
- ***Keep customer data safe* – ensure hackers can't eavesdrop on the data visitors enter on your website by implementing SSL encryption.**
- ***Increase confidence and conversions* – use trust logos and other symbols of security to encourage visitors to give you their data and their custom.**

Open the book and find:

- **The risks to your business of bad website security**
- **What SSL certificates do and how you get them**
- **The importance of partnering with a trusted certificate authority**
- **How to maintain a secure website**

Symantec: Symantec Website Security Solutions include industry leading SSL, certificate management, vulnerability assessment and malware scanning. The Norton™ Secured Seal and Symantec Seal-in-Search assure your customers that they are safe from search, to browse, to buy.

WILEY

ISBN: 978-1-119-14165-5
Not for resale