



WHITEPAPER

The High Cost of Poor Website Security



The high cost of poor website security

Your organization's websites are some of its most valuable assets. But they are vulnerable to security issues and criminal attacks. Fortunately, many of these problems are preventable with effective, integrated website security management.

For ecommerce sites, you can calculate the cost of downtime in terms of lost revenue. You can add to this the considerable cost of remediation, and beyond this, the damage to customer confidence and trust that may be intangible but will be significant. Even when there are no security issues, inefficient processes result in deployment of additional resource that drives up cost.

This article explains why in comparison to the above costs, investing in security management, particularly across SSL/TLS Certificate management, can be a highly efficient and cost effective measure to take.

The value of good website security

Website security involves protecting your websites against unauthorized access, data breaches and malware attacks while ensuring high levels of availability and reliability.

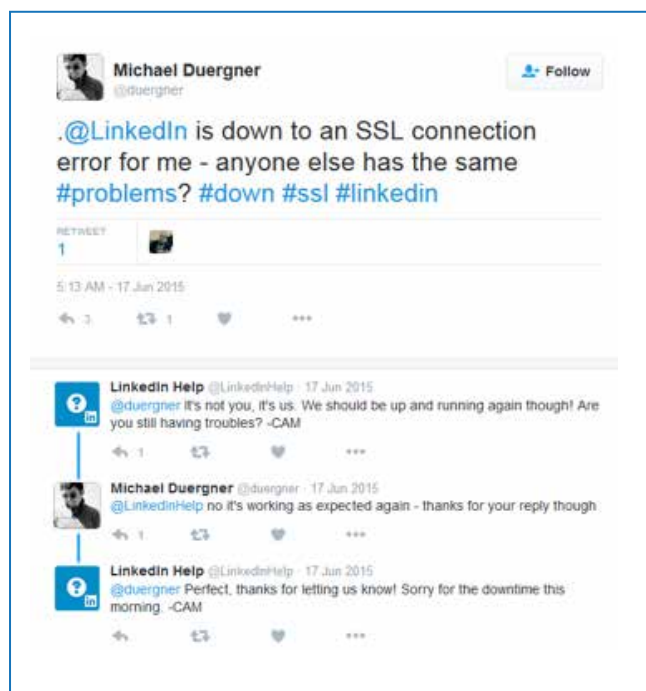
SSL/TLS certificates are an important weapon in your security arsenal. Besides their traditional role in web page encryption and authentication, increasingly they are becoming a critical component of a wider website security ecosystem that embraces malware scanning, vulnerability scanning and patching.

Their growing importance is highlighted by the number of high-profile certificate-related outages recorded in recent years that could have been blocked.

Website security is almost imperceptible when it's working well, but the impacts are clear to see when its performing inadequately or worse, is absent:

- Business critical sites down because of SSL/TLS certificate issues
- Distributed Denial of Service attacks locking out vast numbers of site visitors over prolonged periods of time
- Hackers stealing customer information on a wholesale basis and leaking online, or worse, selling on for criminals to exploit
- Trusted websites infecting visitor systems with malicious malware that can capture and erase all data
- Sites defaced or sabotaged for purposes of propaganda or reputation damage

In these circumstances the case for best-in-class solutions provided by a global security leader providing 24/7 support is strong.



Microsoft's Azure service hit by expired SSL certificate

The company also reported service problems with Xbox Music and Video Store services

IGG News Service | Feb 25, 2013 8:20 AM PT

Microsoft's Azure cloud platform faced a worldwide outage in its storage services from Friday afternoon because of an expired SSL (secure sockets layer)

The company also reported problems with its Xbox Music and Video Store services.

Instagram's SSL/TLS Certificate Just Expired, Security Warnings Pop Up

The problem seems limited to Instagram website

Advertisement

Apr 30, 2015 13:35 GMT · By Ionut Ilascu · Share: [t](#) [f](#) [g+](#)

The SSL/TLS certificate validating a trusted connection between Instagram clients and the service's server has just expired, causing browsers to issue a warning about a possible risk of losing sensitive information.

The operational cost of website insecurity

Of course, most companies pay attention to website security; for example, by trying to keep SSL/TLS certificates current and installing firewalls and anti-malware software on website servers. But there's a difference between best intentions and best practice.

Here are six questions you can ask yourself about your website security operations and certificate management landscape:

- Do you have SSL/TLS certificates from multiple vendors in your infrastructure and if so do you know how many, who issued them and exactly where they are?
- Do you know the expiry dates of every certificate under management?
- Do you know how much of your time you spend manually trying to process certificate renewals and installations?
- Do you know how much it costs your organization to administer your SSL/TLS certificates?
- Do you know how much to budget on an annual basis for your SSL/TLS certificate management?
- Do you know exactly who is procuring certificates within your organization and how they are managing the certificates?

It's rare for security professionals to answer yes to every question.

This is often due to a lack of automation in the existing website security system, the sheer volume of tasks you carry out daily, and the complexity of managing multiple, siloed vendor solutions and relationships.

Inefficient security management not only saps time, energy and budget, but also impacts on your threat detection and remediation, making identifying and fixing security issues more difficult and less effective.

In many organizations, time-consuming manual certificate management is compounded by lack of visibility across the entire certificate estate, limiting your ability to proactively reduce risk and ensure compliance.

Buying, renewing and installing certificates can be unnecessarily difficult; especially if you need to raise a separate PO for each one. And, of course, manual processes increase the risk for error.

To give a clear perspective, Cisco estimated that it takes some four hours of management time, at a cost of \$288 per certificate to manually administer your SSL/TLS certificates.¹

For companies with thousands of certificates, the cost of manual management can be very high indeed. And so if you're using Excel spreadsheets or other manual processes to track certificates and you have a few hundred plus, then you should strongly consider an automated solution. Its likely to pay for itself quickly in saved time alone.

Cisco estimated that it takes some four hours of management time, at a cost of \$288 per certificate to manually administer your SSL/TLS certificates.¹

¹Case Study: Scalable Key and Certificate Lifecycle Management with Cisco Systems, Session ID: SP01-303, RSA Conference 2011, Cisco Systems Inc.

Pricing website risk

The cost of poor website security and inefficient SSL/TLS certificate management goes beyond the cost of day to day admin. When a problem occurs, the cost can be significant.

- Service outage. The cost of individual outages can be very high. Reports put the cost of a Denial of Service attack at up to \$20,000 an hour². The cost is likely to be the same be it if the outage is caused by a certificate issue or other vulnerability
- Fixing problems. The average Global 5,000 company spends \$15 million to recover from a certificate outage and a further \$25 million in potential compliance costs . Similarly, fines for data breaches are escalating.

- Reputation damage. Apart from the risk of being blacklisted by Google and increased insurance premiums, the damage to your brand from security breaches can be significant. While stock prices usually suffer only a temporary dip³ after a major security breach, it takes far longer for companies' reputations to recover.

Without visibility, automation and an understanding of your true risk and compliance posture it becomes near impossible to make smart decisions about how and where your IT and security resources should be allocated.

The cost of poor website security and **inefficient SSL/TLS certificate management** goes beyond the cost of day to day admin.

²<https://www.theatlantic.com/technology/archive/2016/10/a-lot/505025/>

³<https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices>

Conclusion

Nine out of ten large organizations reported a security breach according to a UK government information security breaches survey⁴. Unlike car or house insurance, where the chance of disaster is relatively small even if the cost is high, good security is insurance against a risk with a very high probability.

The cost element involved in deciding on which solution to go with should never just be based on the price point. Having the holistic view of the full management cost of your website ecosystem is essential.

A recent NopSec report⁵ found that it took financial services firms an average of 176 days to remediate a security vulnerability because of laborious manual processes. All of those man hours need to be factored into your buying decision.

These manual, cumbersome, time-consuming tasks also take your team away for the strategic needs of the business. Manual processes hurt your ability to protect at scale. Human intervention is too slow to stop fast-moving attacks. And when those attacks get through, your remediation and recovery times go up, as does the extent of potential damage

For large companies it can become a continuous trade off in investing time and resources between business progress and business security. Those resources get further strained when you lack visibility across your website ecosystem due to silos in your efforts to secure the servers, apps, and data that make up your ecosystem. Your cost analysis should include:

- The headcount resources you need to manage all of those manual processes.
- The visibility you need across your website security ecosystem to establish your level of exposure.

Point solutions and manual processes are going to leave gaps in your security and this is likely to be where the attacker gains entry.

Focus on automation – it will save not only your budget and reduce your resource needs, but more importantly your brand.

Investing in automated, multi-point and multi-layer protection that keeps your website ecosystem safe from the most sophisticated new and emerging threats has never been more necessary.

⁴<http://www.computerweekly.com/news/4500247376/Cost-of-UK-cyber-breaches-up-to-314m>

⁵http://info.nopsec.com/rs/736-UGK-525/images/NopSec_StateofVulnRisk_WhitePaper_2015.pdf

About us

DigiCert is the world's premier provider of high-assurance digital certificates. Since our founding almost fifteen years ago, we've been driven by the idea of finding a better way. A better way to provide authentication on the internet.

A better way to tailor solutions to our customer's needs in SSL, PKI and IoT security. Now, we've added Symantec's experience and talent to our legacy of innovation to find a better way to lead the industry forward and build even greater trust in the world's digital interactions.

For more information call + 44 (0) 208 528 1415,
email enterprise@digicert.com or visit digicert.com/contact-us

Lehi

2801 North Thanksgiving Way Suite 500
Lehi, UT 84043
USA

Mountain View

487 E. Middlefield
Buildings K & J
Mountain View, CA 94043
USA

UK

88 Wood Street, Suite 1001 & 1002
London EC2V 7RS England

Switzerland

Balexert Tower, 18 Avenue Louis-Casai
Unites 01 and 30CH-1209
Geneva, Switzerland

Cape Town

Gateway Bldg. (3rd, 4th, & 5th floors)
Century Blvd & Century Way 1
Century City, Cape Town 7441
South Africa

Australia

437 St. Kilda Road
Level 3, Unit 4.01
Melbourne VIC 3004
Australia

China

23F/Taikang Financial Tower
38 East Third Ring Road
Chaoyang District, Beijing, 100026
China

Japan

Ginza 3-Chome
5F Okura Bekkan
3-4-1 Ginza Chuo-ku
Tokyo 104-0061
Japan

India

10th Floor-RMZ Eco World, Sarjapur,
Marathalli Outer Ring Road
Devarabeesanahalli Village
Bangalore, India 560103

© 2018 DigiCert, Inc. All rights reserved. DigiCert and its logo are registered trademarks of DigiCert, Inc. Symantec and Norton and their logos are trademarks used under license from Symantec Corporation. Other names may be trademarks of their respective owners.

