WHITEPAPER

How To Tell Your CISO: An Investment Case For Complete Website Security

How to tell your CISO: an investment case for Complete Website Security

Are you spending too much time managing SSL/TLS certificates? Can you scan and report on your entire certificate estate? Have you seen a service go offline because of an expired certificate? Do you have to update certificates manually?

If the answer to any of these questions is 'yes' then it's time to invest in an automated certificate management tool.

The business case is compelling. It shows that you can save time and money compared with imprecise manual processes and you'll have the right tools in place to enhance website security and gain the visibility to deal with security issues proactively. This article outlines the benefits of Complete Website Security and how to propose an investment case to your CISO so you can begin closing gaps in your security posture, enabling you to focus your time on more meaningful analysis, reporting and strategic security initiatives for the business.

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.

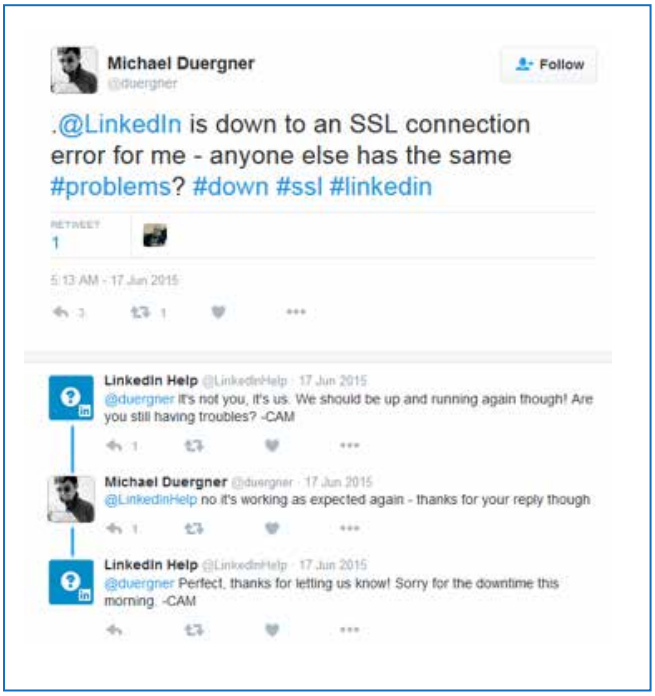
SSL/TLS certificates are an important weapon in your security arsenal. Besides their traditional role in web page encryption and authentication, increasingly they are becoming a critical component of a wider website security ecosystem that embraces malware scanning, vulnerability scanning and patching.

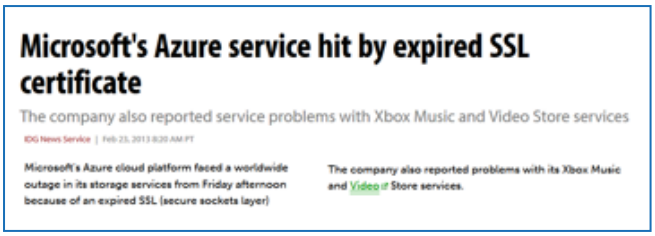
Their growing importance is highlighted by the number of high-profile certificate-related outages recorded in recent years that could have been blocked.

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.





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 its takes some fours 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 its takes some four hours of management time, at a cost of $288 per certificate to manually administer your SSL/TLS certificates.[1]

[1]Case Study: Scalable Key and Certificate Lifecycle Management with Cisco Systems," Session ID: SPO1-303, 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[2] an hour. 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 dip[3] 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

The key points to set out to your CISO to build a case for the necessary investment your company needs in website security are as follows:

Automation
A recent NopSec report[4] found that it took financial services firms an average of 176 days to remediate a security vulnerability because of laborious manual processes. The lack of automation can often cause unintentional security, compliance, and performance issues.

When you have to rely on your people to perform routine or complex website security tasks, it does more than just waste valuable resource time. It can lead to unintentional errors that create security and compliance risks, as well as negatively impact website performance. The subsequent results of these unintentional errors can dramatically harm the viability of your business, no matter how small or large its size. Manual processes also hurt your ability to protect at scale. Human intervention is too slow to stop fast-moving attacks. And when those attacks breach your systems, your remediation and recovery times go up, as does the extent of potential damage

Visibility
The complexity of managing security and compliance with few resources and little visibility creates a difficult game of balancing that you can't win on your own.

The breadth and depth of security makes protection a moving target. It becomes even more complex when combined with the needs of industry and government-driven regulatory compliance.

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 that ecosystem.

Without visibility 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.

Agility
Manual processes also 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.

Faced with the constant battle against new, sophisticated attacks, the case for investing in automating as much as possible in your website security ecosystem alongside multi-point and multi-layer protection, has never been more essential.

[4]http://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

digicert® | Symantec™ Website Security