simplisys

SERVICE DESK

Briefing Paper

Vulnerability Management in a GDPR World

Introduction

Maintaining security of your data, particularly personal data, is an issue that has been with us for many years. The Data Protection act formalised the requirements for businesses to take care when processing personal data imposing penalties for breaches of the act.

GDPR has increased both the expectations around protecting personal data and its processing and businesses have to up their game to ensure that they comply with the new, enhanced, requirements.

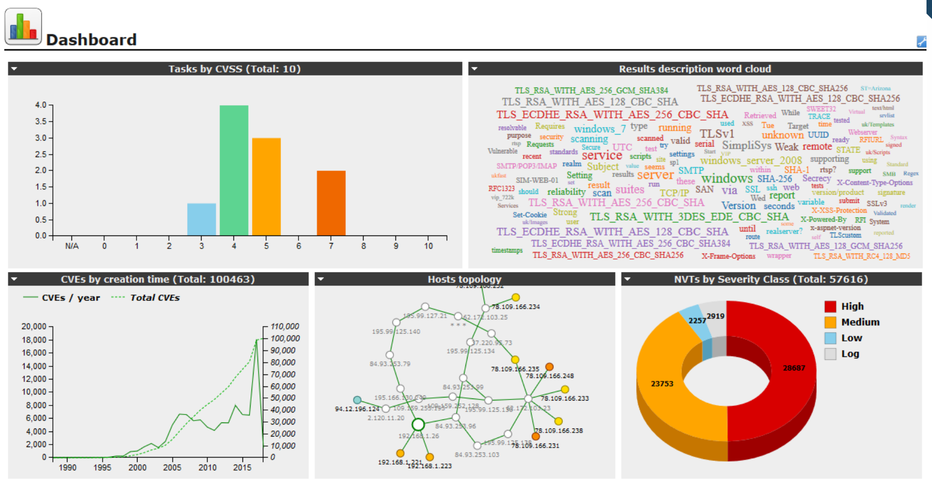
At the core of data protection is vulnerability management. This is the process of understanding the threat landscape, applying that knowledge to your infrastructure, in-house or SaaS / IaaS, and remediating any issues that are identified.

The core activity in this is the identification of Vulnerabilities that exist in your infrastructure and then risk assessing them to identify what threat they pose to your data processing security and what mitigation should be undertaken.

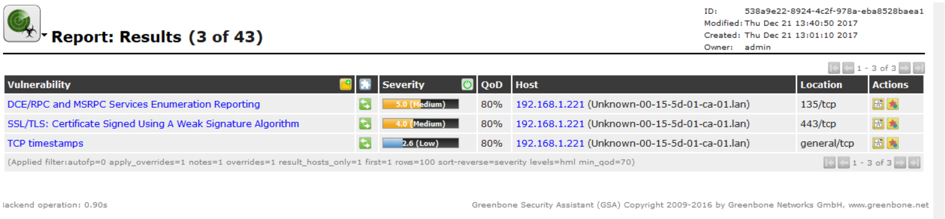
Identifying vulnerabilities in your infrastructure

Traditionally this task has required an in-depth knowledge of the threat landscape and your exposure to them, your ‘attack surface’. The big problem being that this landscape changes every day with new vulnerabilities being discovered and fixes and patches being developed in an arms race between software developers and the ‘bad guys’ who want to attack your systems.

Recently however tools have become available that automate the process. These Vulnerability scanners can scan your systems for known vulnerabilities giving you an over view of your infrastructure and even produce reports detailing the issues found, the risk that it poses and even the recommended action to take.



For example, a scan of a web server may show problems with the setup of your SSL certificates



Report: Results (3 of 43)

ID: 538a9e22-8924-4c2f-978a-eba8528baea1
Modified: Thu Dec 21 13:40:50 2017
Created: Thu Dec 21 13:01:10 2017
Owner: admin

1 - 3 of 3

Vulnerability		Severity	QoD	Host	Location	Actions
DCE/RPC and MSRPC Services Enumeration Reporting		5.0 (Medium)	80%	192.168.1.221 (Unknown-00-15-5d-01-ca-01.lan)	135/tcp	
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm		4.0 (Medium)	80%	192.168.1.221 (Unknown-00-15-5d-01-ca-01.lan)	443/tcp	
TCP timestamps		2.6 (Low)	80%	192.168.1.221 (Unknown-00-15-5d-01-ca-01.lan)	general/tcp	

(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 3 of 3

ackend operation: 0.90s

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

This information allows you not only to identify and treat security risks identified but also to demonstrate due diligence in managing your infrastructure. One of the key elements of GDPR is the need to be able to demonstrate that you have taken appropriate steps to secure the personal data you hold and process. Indeed Article 5.1 of the GDPR states

> “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).”

With the very next requirement, Article 5.2, being

> “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1”

Being able to demonstrate that you have taken all appropriate measures to ensure the security of the data you process is therefore clearly one of the key requirements in fulfilling your GDPR obligations.

SaaS and GDPR

Where processing has been outsourced to a third party, or you are using a SaaS product to process you data then the supplier of that service has become a 'Data Processor' within the meaning of the GDPR. This imposes a similar set of obligations on them to ensure the security of the data being processed but the data controller, that's you, has an obligation to ensure that the data process being used provides sufficient guarantees as to the security of their systems.

GDPR Article 28.1 states

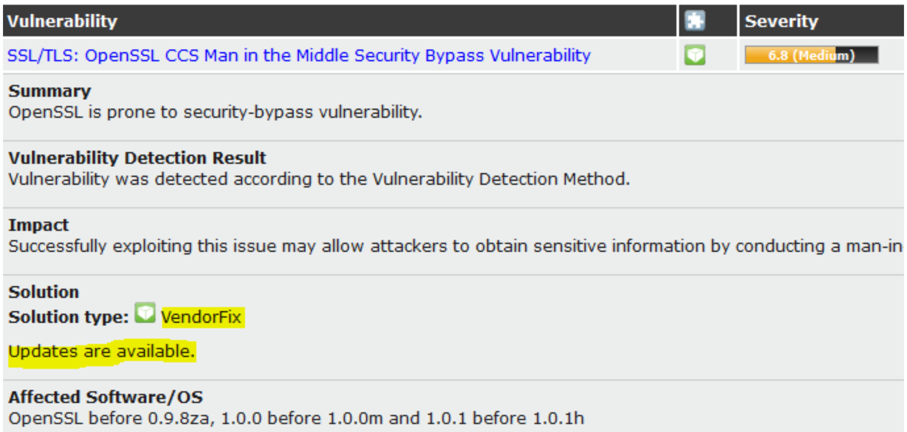
> "Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

So you should expect that the data processor is managing his attack surface and vulnerabilities in much the same way as you would yours. Does your Data Processor conduct regular, and here I mean monthly at least, vulnerability scans? Can they evidence this? Do they have remediation processes documents and can they evidence the mitigation steps they have implemented?

The Spectre of un-patchable vulnerabilities

The traditional remediation for vulnerabilities is to apply the software or firmware patch developed by the supplier. For example, a known vulnerability is one version of OpenSSL can be fixed by upgrading to a later version.

But what about vulnerabilities where no fix is available and the vulnerability is such that it simply isn't possible to mitigate by using firewalls, virtualisation of workloads or limiting external access?



Vulnerability		Severity
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	🟩	6.8 (Medium)

Summary
OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

Impact
Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in

Solution
Solution type: 🟩 VendorFix

Updates are available.

Affected Software/OS
OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h

One such issue is the recently discovered Spectre bug where the design of almost all modern processor chips would potentially allow access to any data being processed on the machine. This is particularly dangerous where the server is processing multiple workloads in a virtualised environment.

Virtualisation allows the servers resources to be shared by a number of workloads with each workload being given what looks like a dedicated machine. In fact, however this “virtual” machine shares the underlying server hardware with an unknown number of other virtual machines. This has thought to have been a secure method of allowing multiple workloads to share server resources because each virtual machine is separated from the others and the host servers. Software running on one virtual machine is isolated from that on other virtual machines in just the same way as if they were running on separate physical servers.

This is the assumption used by public cloud providers such as Microsoft and Amazon where they provide high powered physical servers which are used by an unknown number of workloads from many organisations each hosted in a virtual machine.

What the Spectre bug does however is to destroy the assumption that systems running in virtual machines are segregated from all other virtual machines. The Spectre bug would allow software running on one virtual machine to potentially access data running on any other virtual machine hosed on the same physical server and as this access is at a physical processor level no security measures that you can take can prevent such access.

In these cases the Data Controller needs to understand the underlying physical structure of the SaaS service he is planning to use. It may be that shared virtualised platforms such as Azure or AWS simply do not provide the level of assurance of data security he requires. In such cases he would be well advised to seek out a SaaS supplier that can provide a solution that is dedicated to the workload in question and not shared with other unknown and potentially hostile systems.

Conclusion

The Spectre bug has alerted all IT professionals to the prospect of the main stream Hardware, Chip and OS providers introducing vulnerabilities that are out of the control of the IT Manager i.e. a simple patch or firewall rule will not suffice.

The Spectre bug is a real concern when looking at mainstream cloud offerings. For the next 4 to 5 years at least the only option is to move to a Private Cloud Data Processor who can demonstrate an ongoing commitment to vulnerability management and data security such as Simplisys.

For more information on Data security and Secure Hosted services please do not hesitate to contact Simplisys.

References

The full text of the GDPR

Additional Resources