Seminars, Challenges, Serious Games and Casus

Academic Year 2019-2020

Informative and analytic of the forth conference : (Windows) Patch management : should we care?

Conference presented by Mister Bob MULUMBA and Mister Stephane DAIDONE.

Under the supervision of Mister Bob MULUMBA and Mister Adrien VOISON, *Seminars, Challenges, Serious Games and Casus* teachers.

Third year of bachelor report, in cybersecurity option, Hénallux.

17 December 2019.

Thomas Matis

Contents

1 Introduction

This conference will be talking about the patch management and its implementation.
As my internship's subject will be *deployment of an automated vulnerability scanning platform*, I for sure am eager to learn about this.
Here are the topics that will be discussed :

1. Ransomware
2. Patching
3. New job ? Your turn?
4. Free talks

1.1 Presentation of the speaker(s)

This conference has been presented by two speakers :

The first one is Mister Bob MULMUBA, Senior Technical Consultant at GSK, and Assisant lecturer at Henallux.
He has graduated with a Computer and Information Systems Security master's degree from the University of Luxembourg.

The second one is Mister Stephane DAIDONE, System Engineer at GSK, currently consulting Adiutum.
He has graduated with a CES in Computer Sciences from LTC - Soignies. He is also Citrix XenApp6.5 certified.
He speaks English, French and Spanish.
His specialties are :

- Vulnerabilities & patch management,
- Citric Virtualization technologies,
- Industrial Control Systems,
- Business continuity and incident response.

1.2 Presentation of the GSK company

GSK is a science-led global healthcare company.
They have 3 global businesses that research, develop and manufacture innovative pharmaceutical medicines, vaccines and consumer healthcare products.
It was formed in 2000.

2 Conference

2.1 Ransomware

The speaker presented us multiple cases of ransomware attacks.

2.1.1 Johannesburg City

Hackers took control of the south African city's networks and asked 4 bitcoins as ransom.
The city's billing system was down.
Anyway, they refused to pay as they thought they would be able to restore the systems by themselves.

It has impacted 5 Million people, and critical services were shut down.
Critical services are, for example : electricity, medical stuff, transports, etc.
They used outdated software vulnerabilities as a vector attack. -> This attack was discovered the 24th of october and happened in July. Back then, the price of 4 bitcoins was about 36,000$.
The hacking group was called *Shadow Kill Hackers*.

2.1.2 Mexico Pemex Hack

During the Pemex hijax, the cyber crew has demanded 565 bitcoins, or roughly 5 million dollars, payable before the end of November to unlock the affected systems. Pemex didn't pay the ransom.
They used the DoppelPaymer tool as an attack vector, which is linked to high value target.
The attack damaged their infrastructure : they are currently wiping its installed servers and installing patches.

2.1.3 Spain Radio Stations

The ransomware hit radio broadcaster Sociedad Española de Radiodifusión (Cadena SER). A technician there said that the company was in "hysteria mode".
The hackers came with a €750,000 ransom demand.

I'm glad all these companies didn't pay the ransom : The more the ransom are getting paid, the more the attack might happen.
-> As a way to protect from these attacks, the companies could or should have done :

- Phishing education.
- Application control.
- Incident response plan.
- Continuous Vulnerability Management.
- Backup and restore (recovery).
- Critical incident response program.
- Third party risk management.

- Securing RDP.

Here are some incredible statistics :

- 97% increade in cyberattacks in two years.
- 97% of US companies refused to pay for these attacks.
- 75% of canadian companies paid.
- 58% of UK businesses accepted to pay.
- 34% of organizations spent a week or more to regain access.
- 27% increase in the frequency of attacks.
- every 14 seconds, a new company falls victim to ransomware.

2.2 Patching

Here are some issues with patching :

- The down time : you have to shutdown your systems for a certain amount of time.
- You have to test your patches before applying them.
- You have to keep some features running and sometimes cannot afford to take them down for a certain amount of time.

Furthermore, 44% of companies say that they have a high ability to patch in a timely manner, while 50% of organizations say that they are not protected for a cyberattack.
For critically-dangerous vulnerabilities, it takes 43 days on average to get attacked after a patch is released. That is a huge time gap, when we know that the average timeline for a patch is 16 days.

2.3 New job ? Your turn?

If you are new to the job, your responsibilities can cover up to timelines, approving the patches, verification of the patches impact, communication of a breached caused by a patch and reporting.
Your job is to fulfill the security compliance, as much as the others.
There is one week of patch, you **have** that to be done.
While patching, you have to check synchronisation before the patch day.
Here are some rules :

- You only have to apply the *approuved* patches.
- 6 days after you should report the patches.
- Here is the list of the priority of the appliance of the patches :
    1. Your infrastructure (Dns, etc).

2. The test machines.
3. The SQL patches, cluster ones, ...
4. All the remaining machines.

You should check the logs to see if there are any failure. The most common one is the disk space. If you don't have enough disk space, it is going to stop and no patch will be applied.
Before applying the patches, show you boss the patch you are going to do, it is going to cover you in case of failure.

Once you have done the patches, you have two full days to test them.
You should at least have 96% of compliance in all your patches to be good.
Powershell scripts help them automate this.

The bad part of the job is that for instance, you sometimes have an old machine using Windows XP that costs a lot but you can't take it down.
So you are using a fully vulnerable machine that you can't update, so you have to make patches as and when.

2.4 Free talks

The speaker asked us if it was easier to apply patches on Linux or on Windows.
Someone said : -> Windows because they thought well the applying patches system.
Someone else said : -> Linux Redhat is also great at it, but it is different and harder to manage logs.
The speaker answered : -> It is the same.
There are commercial distributions, such as Redhat, Ubuntu or SUSE.

Someone asked : Is there any bad month?
-> Yes, when you have to apply every single category of patch.

3 Conclusion

To conclude, I have learnt a huge amount of things about patching vulnerabilities. I am eager to apply the knowledge I gathered during my internship, where I will deploy an automated vulnerability scanning.

4 Sources

1. Linkedin :
    - Bob MULUMBA
    - Stephane DAIDONE
2. websites :
    - GSK
    - Johannesburg city ransomware attack

- Pemex ransomware attack
- Spain Radio Stations ransomware attack