CYBER SECURITY WELLNESS

CYBER SAVVY COMPANY

Hector Fernandez 26/03/2021

TRENDS OF THE CYBERCRIME: THEN AND NOW

Old Fashion Attack: The MAFIABOY “Rivolta”

- In 2000, Michael Calce (15) committed the first DDoS attack ever registered to a serial of high-profile commercial websites including Amazon, CNN, eBay and Yahoo.
- The attack caused losses of at least $1.7 billion.
- The young hacker didn’t make the script for the attack; He acquired online an automated “rootkit” written by somebody else.
- Calce, Hijacked computer at universities, and remote-controlled with his automated malware.
- Within hours, he had taken down six major websites, without possibility of defence or answer from any of them, showing the lack a resilience of the companies in that times.
- Because of his unexperienced, the attacker left a big trail or footprints after him, making possible to the FBI and the Canadian Police arrest him.

New Style Attack: “Wanna Cry”

- May 2017, a ransomware crypto-worm was used to target Microsoft Windows operating system computers. Encrypting their data and demanding ransom payments in Bitcoin for the decryption keys.
- It was propagated using the “EternalBlue”. An exploit discovered in older Windows systems.
- Patches were release prior attack, but most of infected devices did not applied the patches or were using older Windows systems like XP.
- 200,000 computers were infected across 150 countries.
- Many public organizations were affected like: NHS, State Government of India, Ministry of internal affairs of Russia or Chinese Public Security Bureau.
- Also private: Nissan, O2, Boeing, Honda, Telefónica.
- Losses from the cyber-attack could reach up to $4 billion.
- Evidences point to a state sponsored attack by North Korea.

EVOLUTION OF THE THREATS IN CYBERCRIME:

Early 2000's

- Attacks were committed to obtain notoriety or for curiosity.
- Firs DDOS attack registered.
- Beginning of Worm type attacks:
  - CodeRed (July 2001)
  - Code Red II (August 2001)
- **Buffer overflow:** Started to be committed.

2010's

- Cyber attacks started to be committed with monetary interests which made criminals get good organized.
- **Spams:** Began a medium to spread worms.
- **Botnets:** As part of its stealth tactic, It used fast-flux DNS and polymorphism to evade defenders and infect untold numbers of computers.
- **Trojans:** banking trojan targeted users primarily through spam, phishing, advertising or social engineering.
- The monetisation era led to an even greater level of email filtering due to the surge in email spam and phishing.

Nowadays

Nowadays

- **Ransomware and Crypto jacking**: Recent studies estimates the damages from ransomware attacks overlap trillions of dollars per year worldwide. Ransomware exposes vulnerabilities in IT defences, spawns new technologies, and can sink entire organisations.
- **Phishing Gets More Sophisticated:** Is trend nowadays use machine learning to craft and distribute convincing fake messages better and faster than ever.
- **State-Sponsored Attacks:** The next few years, state-sponsored attacks are expected to increase, with attacks on critical infrastructures a particular concern.
- **IoT Attacks:** **M**ore connected devices means greater risk, making IoT networks more vulnerable to cyber invasions and infections.

Evolution of the attack tools:

80’s & 90’s

- CIA blows a gas pipe in Siberia inserting a malicious code on a control software. (1982)
- First Warm is created.(1988)
- First use of a trojan malware inserted on a floppy disk.
- Sniffing password software was inserted on the US Air Force network, compromising more than 100 accounts.(1994)
- A backdoor was installed on US department of defence servers, allowing the interception thousands of internal emails from different government organizations.(1999)
- Virus infected Microsoft Word documents, automatically disseminating itself as an attachment via email.(1999)

2000’s:

- DDoS attack targets the thirteen Domain Name System (DNS) root server assaults the whole internet for 1 hour. (2002)
- Shadow Crew Group made a massive campaign of stool and sell credit card number online. (2003)
- Nigerian cyber criminal compromises customer data of Choice Point. (2004)
- Phone Busters reported 11K+ costumers identity theft in Canada, causing total losses of $8.5M, making this the fastest growing form of consumer fraud worldwide. (2005)
- 180,000 HSBC credit card customers information compromised during a security breach at Ralph Lauren. Also the data breach exposes transaction information from 1.4 million credit cards. (2005)

Evolution of the attack tools:

2010’s to nowadays:

- Eastern European cybercrime stole $70 million from U.S. banks using the Zeus Trojan virus. (2010)
- A hack of Sony’s data storage exposes the records of over 100 million customers using their PlayStation’s online services. The breach cost $171M.(2011)
- Anonymous, attacks Fox.com and then targets more than 250 public and private entities, including an attack on Sony’s PlayStation Network.(2011)
- Russian based hackers using malwares infiltrate in banks all around the globe stealing £650M from global banks.(2013).
- A cyberattack exposes names, addresses, dates of birth, and encrypted passwords of all of eBay’s 145 million users. (2014)
- WannaCry, the first known example of ransomware operating via a worm(2017)
- Ransomware attack towards Acer encrypt the company’s account. At the same time the documents are steal. (2021)

How to adapt to the new times?

Cyber Resilience:

A company which works on its cyber resilience, assumes that the organisation will suffer a security breach, gets prepare for that eventuality. A good Resilience could lead a company to recover in a shorter time.

CIA:

Confidentiality:

- A potential damage depends of the sensibility of the stolen data.
- Prisonization of the response of the sensible data over the over the one wo is not.
- Protect the “Crown Jewels” is a good metaphor.

Integrity:

- A copy of the data must be store to reduce the recovery time in case of data breach.
- Be able to point out the compromised data could help to trice the attackers

Availability:

- A company’s data has to be accessible, regardless if It was affected by a data breach or not.
- Regular Backups could lead to accomplished it.

Key fields to focus:

Staff Training:

- Tabletop exercises: As fire simulations, Cyber attack simulations are crucial to get the staff for a scenario of real attack.
- Staff awareness: Even having the best defences if the staff is regular trained how to interact online, the possibilities of suffer a cyber attack are important

Staff Identification and credentials:

- Passwords Policy: A secure and planned staff's passwords habits or even mechanism like two-factor authentication are crucial to protect the companies data.
- Biometrics: More secure than passwords. An implantation of any type of authentication could upgrade the security of a enterprise.
- Access Control: It is important to manage who has access to what data, and what type of access they should have.

Software and hardware detection:

- Firewalls: Firewalls give network administrators total control of how data comes into and goes out of their own network.
- Intrusion detection: Detection System (IDS) is a system set up with the purpose of identifying the presence of a cyber attack before it can do serious damage.

LEGISLATION RELATING TO CYBERCRIME

Existing legislation:

General Data Protection Regulation:

- European Union law; it is the is the toughest user's privacy and security law in the world.
- Implemented on 25th of May of 2018
- This law was the answer of the European Union to confront the lack of protection against attacks
- of the European citizen

- Based on the seventh principles of data protections:
  - Lawfulness, fairness, and transparency.
  - Purpose limitation.
  - Data minimisation.
  - Accuracy.
  - Storage limitation.
  - Integrity and confidentiality.

Existing legislation:

Regulation of Investigatory Powers Act:

- It is known as “RIPA”
- It was introduced in 2000
- Gives specially powers to the public bodies in matters of covert surveillance
- Including use of bugs, video, interception of private communication, and so on.

Investigatory Power Acts:

- Made to replace RIPA in matters of communication and data communication.
- On force on 2016
- Extends RIPA in record collection and communication intercept

Existing legislation:

Computer misuse Act:

- Implemented on 1990
- This law is made to give protection to both users and organizations against cyber-attacks:
- The offences are:
  - Unauthorised access to computer material.
  - Unauthorised access with intent to commit or facilitate commission of further offences.
  - Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etcetera

Copyright, Design and Patents Act:

- In force since 1988
- This law is created for protect the intellectual property of authors against of illegal copy, distribution or reproduction.
- It just applies for certain fields:
  - Literary work.
  - Dramatic work.
  - Musical work.
  - Artistic work.
  - Films.
  - Sound recordings.
  - Broadcasts, and typographical arrangement of published editions

Existing legislation:

Data Protection Act:

Controls how personal information can be used and the rights to ask for information about an user.

Is based on the 7 principles of data protection (GDPR)

In forcer on May2018

Intellectual Property Act:

Update of the old 1988 intellectual property law

It simplifies the complex areas of Copyright, Design and Patents Act.

In force since 2014

Police and Justice Act:

Intender to create a police reform programme.

Redraw lines about power and duties of Police Officers.

Stablish on 2006

Are the laws enough?

Cyber attacks:

- The laws give useful tools to law enforcement to prosecute cyber criminal which committee classic cybercrimes, but they are showing weakness to modern ways of cyber crime.
- They have an appropriate economic penalties and Jail convictions for the criminals.
- On a field which evolves has fast as the Cybercrime it is impossible for the governments to update the law as the cybercrime trends do
- A new and update computing law is mandatory

Data Security

- Huge improvement has been made on recent times with GDPR and DPA.
- European courts have fail in cases of “right to be forgotten” in favour of citizens against big companies, making this sentences “de facto” in future cases.
- ICO is applying important penalties to big companies which suffer data breach on the last couple of years.

Copyrights

- The protection to the intellectual property has been a priority for the governments since the 2000’s
- Recently updates on laws like Intellectual Property Act made easier the legal procedures.

Where the law are not enough?

Cyber attacks:

- CMA came into force in 1990, when only 0.5 per cent of the UK population used the internet, and the concept of cybersecurity and threat intelligence research did not yet exist.
- A coalition of leading cybersecurity experts, organisations, lawyers and academics have sent an open letter to Prime minister claiming that a brand new law is absolutely necessary to be able to confront future cybercrime challenges.
- The experts claim that do not do this reform could cause by 2023 the lost of 4000 high-skill jobs related with the Cybersecurity.

Data Security

- In many cases the fact that companies doesn't suffer a data bridge doesn't mean that the data is protected, public auditory have to be done to randomly control the companies which important penalties in case of non minimums achievement.

Copyrights

- Last implementation of these laws were in 2014 but they are bellow the future challenges already
- In 2018, Stephen Thaler try to patent 2 inventions created by a IA made by him. The court had several problems do dictate sentence.

Controversy of RIPA and IPA:

- RIPA and IPA were made to give special power to law enforcement organizations in cases of high risk cases like terrorist attack, organised crime and national security
- They are laws which play closed to the edge between the citizen's freedom and the security.
- Many reports from human rights associations claims that they have been use in common cases like minor frauds and legal faults.
- Numerous examples prove that the misuse is constant and systematic by public organizations.
- A misuse of these law is an attack to the citizen right of privacy and freedom.
- A special power must be used just in special situation.
- The National union of Journalist and other press freedom campaigners believe the powers within RIPA are in contravention of article 10 of the European convention on human rights.

Examples of a misuse:

Police using RIPA to spy journalist:

- NUJ claims that police use RIPA to snoop on journalists and their sources is “systemic and institutionalised” and is doing “irreparable damage” to the industry.
- Former MP Chris Huhne investigated after obtained a Mail on Sunday reporter’s phone records without his consent using RIPA.

British councils used RIPA to secretly spy on public:

- Councils could do more than 55,000 days of covert surveillance over five years.
- Including spying on people walking dogs, feeding pigeons and fly-tipping.
- Information has been found of 186 local authorities used the RIPA to gather information using secret listening devices, cameras, and private detectives.

T I M E

F O R

Q U E S T I O N S !