**BSc in Creative Computing, Year 4**

**Module: Computer Security**

**Name: Mark Carley**

**Student Number: 20071864**

**Security Breaches Report**

**19/09/2019**

**Contents**

**1**………………………………………………………………………………………………………………………**Introduction**

**2**………………………………………………………………………**WhatsApp Security Breach (Ireland and EU)**

**3**……………………………………………………………………………………………**Mass Data Leakage (Ecuador)**

**4**………………………………………………………………………………..………**Ransomware Attack (Baltimore)**

**5**……………………………………………………………………………..……………**Categorised Table of Breaches**

**6**………………………………………………………………………………………………………………………**Bibliography**

**1.Introduction**

For this practical assignment I will be going through three distinct and quite different forms of security breaches that have occurred over the last six months, each breach I will be discussing will be a different form of hacking and will be explaining each situation in detail and the aftermath of each.

To explain what a data breach is, it’s a confirmed incident in which confidential, sensitive or otherwise protected data has been accessed, changed or removed by any unwanted third parties or organisations. There are many types of security breaches such as malware (ransomware, spyware), an impersonation of any organisation or a denial of service (DDOS) attack. From each situation to be discussed I will be labelling and identifying each category of virus that used through each attack into a table of information.

Following on from each breach that will be identified I will label the appropriate security services to would protect against these types of breaches and backed up by a real-world technological mechanism that would help support those given services.

I will be referencing the online web links for each breach incident that occurred under the references section.

**2.WhatsApp Security Breach (Ireland and EU)**

According to the independent online website, a journal was reported on the 15th May, 2019, indicating a mass security breach were a known issue of hackers have implemented a form of spyware on the current versions of WhatsApp onto peoples devices. The Irish data watchdog association were currently looking into the WhatsApp interception attack to try and figure out how many people were affected overall.

The company responsible for WhatsApp discovered a flaw which allowed any hacker to install malware (spyware) onto a person’s android or iPhone which then triggered the phone to ring up a specific device.

From any call sent out even if the person didn’t make it, the malicious code would be transmitted either way. It also deleted any call logs of that call made at that time so people wouldn’t know and allowed the attackers to activate the speakerphone or phone’s camera without that person’s knowledge. The company said the attack could have been an attempt at targeting higher up officials such human rights campaigners and that the breach that took place resembled similar spyware that could have been developed by intelligence agencies.

The initial security flaw for the app was reported weeks before becoming official but was patched later that month which said “it fixed the vulnerability earlier this month, making changes to it’s infrastructure to stop the attacks from taking place, but there are suspicions that there was an attempt to exploit it again over the weekend” (The Irish Times, 2019).

To classify any attack like this one would clearly be passive as it’s entirely sure that this attack was planned against specific people by extracting information through calls, texts or device recording.

**3.Mass Data Leakage (Ecuador)**

A reported data leak which was reported earlier this week on the 16th September 2019 where possibly the entire population of about 16.5 million people might have been affected. The leak itself was uncovered by a small internet security firm called vpnMentor where they discovered that the leak was coming from an unsecured server somewhere in Miami.

The breach itself exposed much information about the individuals affected such as full names, date of births, email addresses and home addresses, employment information, taxpayer numbers and much more.

Investigators later raided and seized the home of the perpetrator that was behind the leak but also found known financial information such as bank account numbers, credit types and so forth. The same security firm vpnMentor reported the initial breach days before becoming known and closed it but warned that the damage of this attack has already been done.

Once information like this goes live it also makes these victims even more at risk for identity theft, business espionage, financial fraud and other types. According to a report, “a local data analytics company names Novaestrat left an Elasticsearch server exposed online without a password, allowing everyone to access its data” (Cimpanu, 2019).

**4.Ramsonware Attack (Baltimore)**

On may 2019, a massive ransomware attack occurred on the city’s government computer system which was infected by a updated ransomware virus that they nick named “RobbinHood” which encrypted all their main hard drives data except their essential services (police, fire department, EMTs) to prevent access. Ransomware is basically a type of malware that’s design to block access to any device unless any ransom is paid. The total damage done to the city from the attack was estimated at around 18 million for the loss of services.

Each computer that was effected by the virus had a note implemented on each terminal demanding a payment of 13 bitcoin which was estimated at around 75 thousand dollars worth of online currency but were advised against paying the ransom by the FBI ( Federal Bureau of Investigation) as it would not reduce the cyber security cost of the aftermath.

After the aftermath of the attack, a spokesperson “Young estimated that the aftermath of the attack would cost the city $10 million, in addition to the $8 million lost while the city could not process payments. This figure could rise as the city pays for cybersecurity experts to bolster their systems in the future” (Engadget.com, 2019).

In reality to this interruption, Baltimore at that time was more susceptible to any outside attack due to poor IT practices and a lack of cyber security to fend off such an attack along with tight budgets.

**5.Categorised Table of Breaches**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Treat Type** | **Security Service** | **Technological Mechanism** |
| WhatsApp security breach effecting both Ireland and the EU, occurred between May 1st to May 16th. | The type of treat this would fall under is illegitimate use of WhatsApp as the service by an unauthorised third party by allowing these individuals to make use of features on people’s devices, record information and the use of spyware on their devices. It would also be considered an integrity violation considering these third parties could make unregistered calls from people’s devices and delete the logs afterwards. | The integrity of data is definitely a main one here considering the malware installed at the time was able to manipulate peoples call records so a system in place that could block that action to delete or recover via cloud storage that lost call record would be beneficial. A better service that’s non-disclosure to external parties (data confidentiality). Finally liked mentioned earlier proof that all communication with WhatsApp took place, non-repudiation. | A mechanism to put in place firstly would be better encryption for the use of phone features + calls, texts on the app itself. The use of traffic padding would also be of good use here by inserting dummy traffic into a network used by the app and present to the intruder a completely different traffic pattern. A checksum would also be of use by using a block of digital data to detect errors that may appear during transmission of data or storage. |
| Mass data leakage located on Ecuador which resulted in a mass data leak resulting in about 16.5 million people exposed. | The main threat this would 100% come under is information leakage due to an unchecked server which revolved in getting every local person in Ecuador getting their information put online for misuse. This treat would also be considered illegitimate use is any persons exposed data could be used for other crimes such as identity theft, emails been locked out, financial fraud etc. | A more secure way of access to these servers would be a plus such as proper access control and an organised division of trusted staff that can manage all user data. Proper Data confidentiality that cant be leaked as freely as misused later for other crimes. Lastly correct source of authentication when accessing data without the risk of 3rd parties using it. | Absolute first mechanism to implement is proper access control to each server so there not as easily looked into such as file permissions. Again the use of encryption for each persons personal information and traffic padding would be of great use here and finally proper authentication when accessing terminals or servers such as digital signatures, face scan or other biometrics. |
| Ransomware attack located in Baltimore, USA. A total block of third-party services in the city resulting in massive costs of 12 to 18 million dollars of service disruption. | The security treat type an attack like this would be considered a denial of service resulting in total unavailability of systems/ services/ networks. Would also fall under illegitimate use of these systems for unauthorised use by a unknown third party. | A main benefactor here is a better security services that bands together proper access control to who’s system, servers or computers. Another service to keep in check would be better data confidentiality to prevent access to any 3rd parties. A better service to put in place would be proper authentication to make sure who’s the right entity to access data. One final thing to mention is better availability of data ensuring all systems run fine with backups after an attack occurs. | When discussing this treat I think the top mechanism to put into place was a backup of their systems by use of the cloud or externals. Better access control could have been put into place and the use of encryption for files used in each system or server. |

**6.Bibliography**

1.The Irish Times. (2019). *WhatsApp attack: what you need to know*. [online] Available at: https://www.irishtimes.com/business/technology/whatsapp-attack-what-you-need-to-know-1.3891925 [Accessed 20 Sep. 2019].

2.Cimpanu, C. (2019). *Arrest made in Ecuador's massive data breach | ZDNet*. [online] ZDNet. Available at: https://www.zdnet.com/article/arrest-made-in-ecuadors-massive-data-breach/ [Accessed 20 Sep. 2019].

3.Engadget.com. (2019). *Engadget is now a part of Oath*. [online] Available at: https://www.engadget.com/2019/06/06/baltimore-ransomware-18-million-damages/ [Accessed 20 Sep. 2019].