1103 SECURITY POLICIES

SECURUS PRISON LEAK

Table of Contents

1 SECURUS TECHNOLOGIES (The Company Involved)

Securus Technologies is the company involved with the Prison Leak. A Telecommunications company based in Dallas; Texas owned by Platinum Equity. The company has regional offices in Carrollton, Allen, and Atlanta. With a workforce of 1000 employees, Securus Technologies have contracts with 2600 correctional facilities in the U.S.

- Securus was founded in 1986 as TZ Holding Inc. and changed the name to Securus Technologies in April 2009.
- Securus was one of the largest telephone service providers to inmates in US prisons during the 2010s. From the day Securus was found, the company has acquired 20 government services, software-based businesses, technologies, and patents.
- Providing mobile and video visitation services to the inmates is the primary business of Securus, through which the company offers a way for inmates to keep in touch with the outer world and their families and most importantly, communicating with attorneys.
- Dave Abel is the President of the company as well as the Chief Executive Officer.

The importance of the company is so much that, more than 1.2 million inmates across the United States, spread over 2200 facilities use the Securus communications Platform.

1. At the beginning of 2012, the company was processing more than 10 lakh calls every day, reaching a revenue of $404 million in the year 2014.
2. Till 2015, Securus was best known for high calling rates, charging more than $6.59 per minute for audio calls and $5.27 per minute for video calls at one facility.
3. The Federal Communications Commission (FCC) in October 2015 took action and capped the calling rates and fees making it affordable for inmates at just $0.14 a minute.

IMPORTANT: - Securus is a client with local and county governments and with several other states departments. The company attracts its clients by not only installing and maintaining phone systems but also agrees to pay back to its clients “site commissions” which comes from the revenue generated by inmate calls.

2 SECURUS PRISON PHONE CALL RECORDS LEAK

- On 11th November 2015, an anonymous hacker (also believed to be a rogue employee as the company changed claims multiple times during the lawsuit) released 70 million records of phone calls to the press.
- These calls were placed by the prisoners in the US jails to at least 37 different states and the hacker released the call cache with the links to the downloadable recordings of the calls.
- These calls were released via Secure Drop which was obtained by The Intercept (an investigative new organization). The cache of calls spans from December 2011 till the end of spring 2014.
- These call records included calls connected to 1.3 million unique phone numbers called by more than 63000 inmates.
- The data was contained in a 37 GB file which was scattered across hundreds of tables, like what a spreadsheet looks like, which the Intercept merged into a single table containing 144 million records.
- After removing the duplicates this figure reduced to 70 million individual phone calls.
- The database contained information like prisoner's first and last names; the phone numbers they called, the date, the time, and the duration of the calls as well as their Securus account numbers. In addition to all this data, each call recording included a "Recording URL" from where the audio recordings can be downloaded.
- The Majority of the calls appeared to be personal, in one leaked audio call relatives discuss someone whose diabetes is worsening.

But the most significant thing is at least 14,000 calls in the cache are calls made between prisoners and their lawyers.

- However, an actual number of calls with attorneys would have been higher because the 14000 number was crosschecked with the hacked data with the known telephone numbers and the mobile phone was not accounted for.
- Some of the recordings were confidential and privileged legal communications and these calls never should have been recorded.
- The recordings of legal attorney-client communications and the call storage offend constitutional protections including the right to be effective assistance of counsel and of access to the courts.

3 HOW THE ATTACK HAPPENED?

The biggest problem with Securus Technologies is that those who have privileged access to the database can easily get it. This means that someone with the right credentials can do whatever they want with the private information stored in the servers. While it is illegal to record all attorney-client privileged calls, Securus does so for the purposes of assisting counsel and gaining access to the courts which potentially offends the constitutional laws.

Furthermore, Securus claims that their phone systems have several protective mechanisms in place to avoid attorney-client recording and inform customers that their calls are being recorded and if they are an attorney, they need to enter their credentials. So, lawyers can register their phone numbers or a particular mobile number to avoid being recorded. And those who do not do so hear a warning every time attorneys and inmates make calls.

Attorney-clients' calls are confidential and cannot be recorded let alone be stored. By doing this, Securus has been involved in many legal and ethical issues surrounding civil rights. This motivated the rogue employee turned whistleblower, to share these important materials to “THE INTERCEPT”, an online investigative news agency, who revealed this matter to the public and exposed the loopholes in the organization.

But in the latest press release, Securus Technologies claimed that this was a result of a software error rather than an intentional act, when asked why the recordings were there in the first place.

3.1 WHAT ORGANIZATIONAL ISSUES ALLOWED THE TECHNICAL FLAWS THAT ENABLED THE ATTACK/EVENT?

Initially, Securus claimed it was a glitch in their software that recorded calls even when the users opted out of the recording. On an organizational level, Securus lacked proper policies for frequent testing and updates for the software they were using. But the story does not end there. The recorded calls were downloaded and stored on a high-capacity hard drive and taken out of the premises. This would indicate the lack of equipment control and access control to the servers.

These call recordings were sent to The Intercept, an online investigative news agency. It was found that they had recorded even attorney-client conversations which were illegal. The links to this were shared via SecureDrop, a file-sharing service, with links to download these conversations. In response to this, Securus Technologies came out and announced it was an insider job and an employee had gone rogue and did all this. But from the perspective of an organization, their hiring policy is also lacking. They did not take the proper measures needed while hiring people, with virtually no background checks on the person, no non-disclosure agreements (NDA) considering the serious nature of their services and no imposition of penalty. All these are observations made from the fact that Securus has not taken any action against this employee, they have been very lax in their approach towards securing the data before they were required by the FCC to show compliance and the fact that the employee had the right methods of access to the right resources within the company to walk away with such a huge cache of data.

3.2 WHAT WERE THE TECHNICAL ASPECTS OF THE ATTACK?

Securus Technologies used their proprietary platform known as SecureCall to help prison inmates call their families and lawyers from within the prison facilities. These systems primarily use a 4G VOIP technology wherein the data is sent in form of packets. This makes it easy to potentially store data on a memory stick with the right tools and right credentials. This technology has been known to be potentially unsafe as anyone can tamper with the data packets if they have the right set of tools and access. Since the data was sent in terms of packets, it is easy to record and store them and that is exactly what Securus Technologies did.

Secondly, the SecureCall system has a provision for lawyers to register their number in their database and their calls will not be recorded and even during the call warning messages would be played out periodically to let the users know their calls are being recorded. All non-essential calls are to be recorded, according to the agreement between the FCC, Securus Technologies, and the prison networks for law enforcement purposes. According to Securus technologies, there was a flaw in their system. This flaw was that even though the lawyers had already registered their phone numbers with the system, it was still recording them. That was the reason why there were 70million phone conversations recorded by their systems and stored on their servers. Securus Technologies claims it was ignorant of such a thing happening.

Thirdly, we have an employee with access to these servers to be able to download this entire cache of recordings from the servers and take them out of the company premises. For this, the employee must have had the right credentials to access the servers. He must also have had the right permissions to be carrying around such high-capacity hard drives to store data or to be able to access the internet and use so much bandwidth to upload all this to the internet. The employee downloaded around 300-400 GB of data and posted it online. To do this, they must have had access to either a high-speed internet connection to do it from the company's own computer or a hard drive to store the data and patiently upload everything from the comfort of their homes. Considering everything, the employee must have been a part of the IT department to be able to do such things with no one asking him/her what they were doing or even why they were doing what they were doing.

4 POLICIES IMPLEMENTED TO SECURE THE COMPANY OR ORGANIZATION AND PREVENT/AVOID THE ATTACK FROM HAPPENING AGAIN?

According to Securus, the attack originated from an employee who wanted revenge, and Securus was just the victim of a traitor.

First, we will propose a few policies to strengthen the business and avoid similar attacks in the future, regardless of whether the attacker is inside or outside the business.

The proposed policies are:

- **Classify the data, and folders:** these recordings should be labeled "top secret" or at the highest level - the level which is only accessible to senior staff and always absolutely confidential.

- **Authority and access control policy:** The purpose is to controls access to information systems, or data, databases of a company or organization. Applying a mechanism to save the log of the login account, access time, and actions of the account during the process and the access location of the accounts that have accessed the database, or the directory that has been labeled "top secret".

- **Network security policy** - a more specific policy of "Authority and access control policy", to enhance network security for businesses when an employee wants to access the network or server system of the company. This requires multiple layers of authentication and security to authenticate correctly, only authorized users can access the system, in addition, the system will warn every time there is access with the accounts, which have not been authorized or accessed in a new location. Intrusion alerts are not only for the account owners whose accounts are being accessed but also alert the system administrators to take prompt action such as temporarily stopping the compromised system or database.

  The purpose of this is to track down who has unauthorized access to these directories and generate evidence accusing the perpetrator.

- **Network Security Incident Response Policy,** in response to unauthorized access to the system, or suspicious behavior such as downloading or modifying data, to minimize the risk posed by disclosure of confidential data.

- **Bandwidth Limiting policies:** According to the report, at least 14,000 calls have been saved by hackers and posted online including links to download each call. That means that the attacker successfully downloaded those 14,000 calls, in addition to the 37 GB cache of report of more than 70 million calls. In order to do that, a high bandwidth will be required. Adopting a bandwidth-limiting policy will help slow down the attack and increase chances of detecting the attack.

- **Bring-your-own-device (BYOD) policies:** Applying the BYOD the policy will help businesses save the cost of buying equipment for employees, but it also has many potential risks such as employees can use phones as storage devices and store many important confidential data, in this case, it could be 14000 call records and

- **Password Protection Policy**: The aim is to set the standard for password difficulty and schedule password change after a period of time, to avoid brute force or dictionary attack on the highly privileged accounts in the system.

❖ **Hardware Policies:** Hardware: In this context, it is defined as all physical equipment and assets that belong to the enterprise. This policy identifies the hardware that must be used for the purposes set forth earlier, and that they must not be misused.

In addition, the policy should also state that hardware must be carefully managed, especially high-value devices.

4.1 WHAT COMPREHNESIVE SOLUTION (ADMINISTRATIVE, TECHNICAL, PHYSICAL, PREVENTIVE, DETECTIVE) SHOULD BE CARRIED OUT TO ENSURE COMPLIANCE WITH SECURITY POLICIES, TO SECURE THE COMPANY AND PREVENT ATTACK FROM HAPPENING AGAIN?

Setting out policies will be useless without all the compliance of all employees in the business. You need all employees to understand and adhere to the policies that have been and will apply to the business.

Technical solutions:

Implement a means of access control: In addition to the basic functions of access control: authentication and authorization with an account or a pin code issued to each individual to authenticate and authorize users, businesses should apply two-factor authentication (2FA), often referred to as two-step verification or dual-factor authentication to authenticate users, to increase the security of the account. Now it is more difficult for an attacker to gain access to accounts with only the user's username and password.

Activity logs and audit controls: Control log in and log user activities with data when logged in to an account and alert the system administrator or authorized people when someone tries attempts to interfere with data such as editing, deleting, or downloading data.

A few other technical solutions: These can include measures such as: disabling unwanted USB ports and network ports, implementing a filtering program on recording services for identifying and discarding confidential and private phone calls in case any are recorded, monitoring and testing the system for bugs and weak points and constantly testing and putting up software patches for the services provided and keeping a log of all the problems and how they were solved, running regular security checks and drills to see if any problems exist

Physical solutions:

Facility access controls: There is a need for control of individuals with physical access to data storage locations such as those where call recordings or backups are stored. Regardless of whether they are engineers, system administrators, or cleaners of the organization.

In addition, measures must also be taken to prevent unauthorized physical access or impersonation of privileged individuals, or theft of data. One way of doing this is to install biometric locks in key areas. This will help the administration to control who gets access to the server and have a time stamp on who accessed the service or the system at what time. Another thing would be adding video cameras for recording at these places along with biometric locks to have a clear idea of who accessed it and when they left the area.

Policies for the use/positioning of workstations: Policies and compliance must be in place to restrict the use of workstations that have access to important data or databases, in particular the database of call recordings. One way of doing this could be by restricting internet access of these workstations to anything other than the internal, necessary work-related services. The enterprise must also take measures to protect important data such as defense in depth or the management of functions performed on workstations.

Policies and procedures for mobile devices: Policies for personal devices must also be in place and implemented for those whose personal devices have access to confidential data. Make sure that when these people quit their jobs, these confidential data will no longer exist on their personal devices and their access to the confidential system are disabled.

Hardware inventory: An inventory of all the hardware and who is responsible for each device must be maintained and monitored, along with the movement of that hardware.

Administrative solution:

People are the weakest link in information security, so problems can be solved or mitigated from this weak link, in particular by increasing users' awareness of this area. Enterprises should have advanced information security training sessions so that employees know how to protect their own information.

This training includes:

Social engineering attacks, such as Phishing, Watering Hole and other common network attacks

Clean desk policy: This the policy will require that personal item such as personal laptops, notes, notebooks ... should not be left on the desk.

Acceptable usage: Require employees to understand restrictions on using work equipment and the Internet.

And to make sure that all employees are fully aware of these policies, companies should hold understanding tests for employees, and regularly check their compliance with the policies and create penalties for not complying with or against these policies.

Preventive control:

Preventative control functions are important too, as prevention can be more time and cost-efficient as compared to finding a solution after the incident. This will include multiple ways such as:

Security Awareness Training Employees should be given training to ensure that they are careful with the company's assets/data and are aware of what actions might be considered negative for the company.

Better Hiring Practices Employees should be screened thoroughly to ensure they won't do anything harmful, & become a liability to the organization later on.

Secure Hardware Organizations should try to keep the hardware/asset as secured as possible, and direct access should also be limited.

Detective control:

The detective control function can help detect the data leak/breach in an earlier stage so that required actions can be taken in order to reduce the damage to the organization. Some of these functions are:

Audit Logs Organization should keep track of employees' access and activity with their assets/data. Keeping proper logs can help detect the cause of an anomaly.

Investigate Unusual Activity If anything is detected then the organization should try to locate its source and then investigate it properly. Any unusual or suspicious activity should be considered a threat to the organization and should be treated accordingly.

Audit Logs Organization should keep track of employees' access and activity with their assets/data. Keeping proper logs can help detect the cause of an anomaly.

Investigate Unusual Activity If anything is detected then the organization should try to locate its source and then investigate it properly. Any unusual or suspicious activity should be considered a threat to the organization and should be treated accordingly.

5 REFERENCES

- https://www.publicknowledge.org/blog/securus-leak-of-prison-call-records-underscores-importance-of-fcc-oversight/
- https://www.theregister.com/2020/08/19/securus_lawsuit_attorney_client_calls
- https://www.theregister.com/2020/05/21/securus_prison_wiretapping_lawsuit/
- http://blog.prisonconnect.us/the-breach-of-the-securus/
- https://www.inverse.com/article/8258-prison-phone-company-securus-denies-violating-inmate-rights-with-call-recording
- https://www.ibtimes.com/securus-technologies-rogue-employee-not-hacker-exposed-70-million-inmate-calls-2181819
- https://innovationatwork.ieee.org/five-lessons-learned-from-recent-cyber-attacks/
- https://www.blumshapiro.com/insights/cyber-attacks-outsourced-cybersecurity-cybersecurity-solutions-ct-ma-ri