Cybersecurity Services and Network Management

Ransomware As A Service

Detailed research and report regarding the latest cyber threat circulating the network

Dexcom Inc.

April 21, 2021

Jose Enquito

6340 Sequence Dr

San Diego, CA, 92126

Table of Contents

Introduction

Ransomware attacks have been receiving major news coverage recently due to the rise of these lucrative attacks. Many of these attacks are now targeting major high-profile corporations leaving every type of industry vulnerable, including government, healthcare, education, and financial industries. We know ransomware attacks are a damaging form of malware which aims to restrict users from accessing their devices unless a ransom is paid. This specific malware works by employing encryption to the targeted system and restricting user access to their systems. The complexity of these attacks allows the malware to spread through networks infecting specific targets, including major databases and servers. Many times, this can leave an organization entirely immobilized and drive them to pay the ransom to keep their business afloat. We know the first form of ransomware attack took place in 1989, it was known as the AIDS trojan attack which was released via a floppy disk. Attackers demanded the victims send $189 to a P.O Box located in Panama if they wanted access to their systems restored. Although the first attack took place in 1989, ransomware attacks didn't take off until the mid-2000s. Now we are seeing over 4,000 ransomware attacks daily in the United States. Not only have ransomware attacks increased in numbers, but the attacks have become increasingly more complex and automated. It has become incredibly easy to build and launch a ransomware attack through something called Ransomware as a Service (RaaS).

Ransomware as a Service (Raas) is known as a subscription-based model that enables attackers to deploy ransomware that has already been developed. RaaS closely follows the SaaS (Software as a Service) business model except it is an illegal form of service. The developer of the ransomware will sell their product as a kit and earn a percentage of each successful ransom

payment. These RaaS kits make it exceptionally easy for attackers to purchase profitable software for a very cheap price and launch major attacks anywhere they desire. Many of these RaaS kits also include 24/7 support and come in bundled packages which include user reviews and forums. Prices for these kits can range from $40 a month to several thousand a month depending on the complexity of the ransomware. Some of these kits include WanaCry, DarkSide, REvil, Dharma, and LockBit. Because these attacks continue to rise and become more complex, companies are investing heavily to prevent them and making plans to quickly recover from these attacks.

Related Course Concepts

It is very important for businesses to have IT Security Policies in place at their organization. Businesses need security controls and procedures that give their employees instructions on how to implement, enable, or enforce their security policies. There are various malware infections that ransomware users try to use to gain entrance into a company's internal networking system. The most common types of malwares used are viruses, worms, trojan horses, spyware, adware and of course, ransomware. Hackers will send out phishing emails to a list of people in a business in hopes that just one person will click on the malignant link which will allow the hacker access into the company's networking system. This is how it begins, and before you know it, the hacker has created a lock into the business files and has requested a hefty ransom to release the lock on their own files. It has been shown that 94% of all malwares are delivered by email, so it is imperative to train your employees on what to look out for.

There are three principles of information security that all businesses must follow to protect their business assets: confidentiality, integrity, and availability. Confidentiality is

protecting the company's information against unauthorized disclosure. Integrity is protecting the company's information against unauthorized modification and ensuring the authenticity, accuracy, and completeness of the information. Availability is protecting the company's information against unauthorized destruction and ensuring data is accessible when needed. Following these principles are important because without them it can leave a company susceptible to compromise or theft of their data.

Businesses will also implement multiple layers of security such as using a firewall, anti-malware or antivirus software, email filtering, web filtering, patch/update management, network monitoring, and managed detection and response services, just to name a few. Businesses will also need to implement a solid "Disaster Recovery Plan " to be able to recover business systems, files and data in case there is a breach and information is lost, locked or stolen. Companies should have a way to back up their information either off-site, on cloud storage, HDD or SSD drives or on 5D data storage. In these ways, data can be restored, and processing can continue, in the event of lost or stolen data. If data is stolen, you wouldn't have to pay any ransoms to hackers, if you could just retrieve a copy of your data and re-implement it on new servers. To meet today's expectation of continuous business operations, organizations must be able to restore critical systems within minutes, if not seconds of a disruption.

One of the biggest deterrents used to safeguard business information is data encryption. It is a mathematical process that converts readable plaintext data into what is called ciphertext data that is non-readable without a decryption key. The key is then used on the encrypted information and becomes readable to the intended party. Data encryption is important in today's digital age to safely use the internet to conduct business and communicate private information and keep it safe from any exploiting sources. Most businesses will have data encryption built

into their systems to automatically encrypt data as it is being sent. In this way, the company doesn't have to rely on manual encryption by the employees to safeguard their data.

Management – Act, react, mitigate, and remediate risk.

An organization's response to a security incident is critical. Every company which utilizes technology to conduct business, should have an incident response team, business continuity plan (BCP), and a disaster recovery plan (DRP). An organization that does not have any of these best practices, often mandatory practices, in place are subject to experience a full-scale disaster. According to the NIST Cyber Security Framework, risk management is composed of five functions: *Identify, Protect, Detect, Respond, Recover*. Identify is to define what assets, functions, data, and systems are important to the company in order to conduct business. Protect is to provide guidelines on how the organization can secure these devices which are critical to conduct business. Detect is to identify the occurrence of a security breach/incident. Detecting can include event logging, physical breaches, understanding potential impact of a threat, and perhaps the use of a NIDS (Network Intrusion Detection System). The Response is how the organization and IT department/Security team will respond to the incident. The response requires an action to be taken. The response can be notifying others, managing a direct line of communication to all affected parties, and analyzing the incident. Recover is how the company identifies the most appropriate path to restore services/systems to normal operations. An example of recovery would be to restore all systems affected by a Ransomware attack.

Risk Management is a critical framework to follow to prevent or recover from any incident, such as a ransomware attack. Without having an idea of what the general plan is, some organizations might find themselves running around without an idea of where to start or how to

mitigate the risk. This may cause an organization to over-react, or not react in a timely or appropriate manner. According to an article published by riskandinsurance.com, only 20% of companies feel confident in their ability to respond to a ransomware attack. Ransomware attacks may cost companies from thousands to millions of dollars. While the ransom itself may not cost that much, the labor involved to mitigate the threat and the damage to the company's image may approach in the millions.

Conclusion

Ransomware attacks have been receiving major news coverage recently due to the rise of these lucrative attacks. The complexity of these attacks allows the malware to spread through networks infecting specific targets, including major databases and servers. Ransomware as a Service (Raas), known as a subscription-based model that enables attackers to deploy ransomware, has already been developed and out there being used and spread throughout the network. It is, therefore, very important for businesses to have IT Security Policies in place at their organization. Businesses need security controls and procedures that give their employees instructions on how to implement, enable, or enforce their security policies.

To summarize, we have mentioned that there are three principles of information security that all businesses must follow to protect their business assets which are Confidentiality, protecting the company’s information against unauthorized access from unauthorized personnel, Integrity, protecting the company’s information from being modified by any unauthorized employee, and Availability which is enabling data to be accessible when it is needed and would not allow the data to be deleted or removed without proper authorization. In these ways, data can be restored, and processing can continue, in the event of lost or stolen data. If data is stolen, you

wouldn't have to pay any ransoms to hackers, if you could just retrieve a copy of your data and re-implement it on new servers. One of the biggest deterrents used to safeguard business information is data encryption. It is a mathematical process that converts readable plaintext data into ciphertext, which is data that is non-readable without a decryption key. Another thing that we have discussed is that there are five functions that the NIST Cybersecurity Framework laid out for Risk Management. Identify, defining the assets, functions, data, and systems based on the importance to the company in order to conduct its business. Protect is to provide the guidelines about how an organization can secure devices critical to conducting businesses. Detect is to identify the occurrence of a security breach/incident. Response is how the IT Department, and the Security Team would handle the situation and how fast they would react and act upon a possible breach and recover, which is how the company identifies the most appropriate path to restore services/systems to normal operations. Risk Management is a critical framework to follow to prevent or recover from any incident, such as a ransomware attack. While ransomware itself would be devastating on any unsuspecting network, especially on an organization the deals with sensitive information, having guidelines such the Risk Managements that had been laid out will mitigate and/or prevent attacks from being initiated from the start and will absolutely help business deter ransomware attacks in the future.

Lastly, with the complexity of ransomwares, malwares such as we have discussed will spread throughout the network if it was prevented and stopped from the start. The attacks targeting major high-profile corporations are the absolute reason why other corporations should not become complacent in their security due to the fact that malwares like ransomwares can adapt and change based on the event that it will be used on and how determined a person who

programmed the malware is from damaging and possibly bringing down corporations for the betterment of his/herself.

References

Editorial Staff. *"The three-pillar approach to cyber security: Data and information protection."* DNV.com, https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683 . Accessed 27 Sept 2021.

Fruhlinger, J. (2020, June 19). *Ransomware explained: How it works and how to remove it*. CSO Online. Retrieved September 20, 2021, from https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html.

Milosh, Alex. *"Disaster Recovery Plan for IT Professionals: MSPs and Internal IT."* Atera, 30 Sept 2020, https://www.atera.com/blog/disaster-recovery-plan-for-it-professionals-msps-and-internal-it/ . Accessed 27 Sept 2021.

Strike, C. (2021, June 5). *Ransomware as a service (raas) explained: Crowdstrike*. CS. Retrieved September 20, 2021, from https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

Witts, Joel. *"Why It Matters Where Company Data Is Stored."* Expert Insights, 31 Aug 2021, https://expertinsights.com/insights/why-it-matters-where-your-company-data-is-stored/ . Accessed 27 Sept 2021.

Nicole.keller@nist.gov. (2021, May 12). *The five functions*. NIST. Retrieved September 25, 2021, from https://www.nist.gov/cyberframework/online-learning/five-functions.

Katie Dwyer (2020, March 13). *It's 2020 and only 20% of companies are ready for a ransomware attack.* Risk & Insurance. Retrieved September 28, 2021, from https://riskandinsurance.com/its-2020-and-only-20-of-companies-are-ready-for-a-ransomware-attack/.