y

by Y T

Submission date: 06-Mar-2021 07:29AM (UTC-0800)

Submission ID: 1525856880

File name: Prompt.edited.docx (25.17K)

Word count: 1096

Character count: 6155

Article Prompt

Name

Institution

Course

Instructor

Date

Article Prompt

Prompt 1

The current world has utilized technology in almost every part of its life. Although technology has reduced the amount of work and make things easier for people, it has also caused significant challenges to organizations and governments. Attackers have developed new and advanced techniques for interfering with the systems and structures used. Ransomware is a form of malware attack that criminals use to lock and encrypt the victim's data and then ask for payment to decrypt and unlock their data (Siegel, 2019). As stated in the article, Riviera's city was faced with a ransomware attack, which resulted in interference with the system, network, and software services to the town, disrupting the city's services.

As an administrator, specific steps will be taken to help eliminate the occurrence of a ransomware attack. Because ransomware is vital in hindering proper service delivery to the public, it will require utmost concern. The first step is to provide appropriate education to employees. Employees play a vital role in the city administration, including reading mails. According to Sittig & Singh (2016), most ransomware attacks are delivered through the mail; therefore, since employees interact primarily by opening mails, they might easily click on a malicious link and affect the computers. Besides, proper employee education will help easily detect a phishing threat and respond appropriately to the mails.

The next step is to implement effective monitoring and detection strategies. Attackers use ransomware attacks, and they will ensure they remain undetected. Sittig & Singh (2016) stated that ransomware attacks are required to run an enormous number of file operations by utilizing a short period, such as opening files, generating encrypted copies, and deleting the original ones.

Although the action is not usual for other software, the user can quickly realize by monitoring the Application Programming Interface (API) call essential for accessing and encrypting files, hence shutting down the attack fast. This will help reduce the impact of the data retrieval by hackers hence enabling the daily operations if the organization to be accomplished with ease without any missing information.

Another step is focusing on implementing automated backups for the city's data. According to Sittig & Singh (2016), ransomware attacks depend on the victim to have one copy of their critical data; therefore, when they achieve encrypting and deleting the valuable data, the organization will have no other way than to pay the ransom. When the city has an automated backup system, it can keep its sensitive data safe and reduce the likelihood of data loss. Similarly, the loss of money through ransomware payments will be eliminated, and services continue in operation and force the criminals out of business. The final step is to maintain a security solution that is suitably preserved for its effectiveness. For instance, the installation of antivirus that is frequently updated to make scans regularly. For that reason, the data is always kept safe and prevention from landing in the wrong hands is highly improved. With this in place, the organization involved can concentrate on its daily mandate without fear of any external attack regarding data safety.

Prompt 2

Information plays a critical role in the operation of the organization or administration. Therefore, suppose the organization's data is attacked by ransomware. The criminals have asked for the payment to provide a key for the encrypted data; it will depend if the organization has backup data or finance to recover from their state or give in and pay the ransom where in most cases puts the organization in a tricky position. Nevertheless, developing the anti-ransom law seems to be a good idea because it will reduce the criminals' opportunity to prevail. According to the Editorial Board (2019), in 2018, Atlanta used 2.6 million dollars to recover from the ransomware attack than pay a ransom of 51000 dollars. This makes it challenging for law to act in such a situation because it will make the administration go through more cost than what is required on the ransom to fix the resources and recover on their operations. The above strategy seems to work in everyday effort to get back the organization's data without any extotion.

The current organizations depend on technology in almost every process. Consequently, when ransomware attacks occur, they have no protection on them and hence disrupt their operations. I would not advocate for the anti-ransom laws because the situation is immense to the local administration. It can lead to disruption of services that the federal government cannot get involved in helping them. For example, the attack on Riviera beach resulted in poor service delivery in three weeks. The city workers had not accessed their emails, other employees and suppliers had to be paid using paper checks, and emergency correspondents could not log calls using computers. This could result in severe catastrophes, including the loss of lives.

Moreover, I cannot entirely agree with implementing the anti-ransomware law because it has focused on the notion that the local administration is financially stable and can handle the expensive upgrades and software developments required when the attack occurs. This issue will need the local administration to ask for financial help, hence using the security department and other agencies to deal with the attackers and restore the administrative systems. Nevertheless, through upgrading the designs and creating more networks and comprehensive technologies, the city will be affected in operations and losing more money which is not acceptable under any circumstance.

The resident metropolises should choose whether they need to respond on giving out the ransom or work their way out because they know their financial abilities and the situation they are in. Moreover, the decision to pay the ransom is not made by one person, and before it reaches their proper, consultations will have been made. With consultations in place, it guarantees that the right decision is made concerning the issue at hand. Although I understand that ransom payment is discouraged by the federal bureau of investigation, it prevents people from paying the ransom because there is no guarantee of getting all the information. Nevertheless, it is still the easiest way to get back in operation and hence many organization should encourage practice of the same.

References

Editorial Board. (2019). Opinion: Hackers are taking cities hostage. Here's a way around it. *The Washington Post*. https://www.washingtonpost.com/opinions/hackers-are-taking-cities-hostage-heres-a-way-around-it/2019/06/23/f08b79ea-9459-11e9-aadb-74e6b2b46f6a_story.html

Siegel, R. (2019). Florida city will pay hackers $600,000 to get its computer systems back. *The Washington Post*. https://www.washingtonpost.com/business/2019/06/20/florida-city-will-pay-hackers-get-its-computer-systems-back/

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Applied clinical informatics*, *7*(2), 624.

y

ORIGINALITY REPORT

0%	0%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		