Ian Waweru

Cyber Fundamental

11/18/2022

Ransomware

Cyber-attacks are occurring all over the world and it’s our job to defend against them. There are different types of attack techniques that cyber criminals use. There are malware-based attacks, phishing attacks, Denial of service attacks (DoD), and more that create problems in different parts of the country. Some countries do a good job of defending against certain attacks. For example, The cybersecurity and infrastructure security agency (CISA) is an agency located in the US and they have done the best job of understanding and managing, and reducing the risk to cyber and physical infrastructures. The United Kingdom (UK) on the other hand has been struggling and dealing with cyber-attacks. Based on the reports made by the national cyber security center of the UK, the threat they face is a malware attack called ransomware. Ransomware is a software-based attack and it’s created to block access to systems until a debt is paid. In the UK this type of attack has only increased over the years. In 2019 these attacks were occurring and causing problems for organizations. In 2020 the issue has increased, and organizations have lost a lot of money over time. After only a few months into 2021 ransomware has caused major issues and has totaled to the same number of incidents in the previous year before. There are a couple of examples of how this ransomware affected the UK. For example, the vulnerabilities that are in Microsoft servers were exposed and it had about 30,000 organizations compromised in the US. That’s a lot and it’s even worse that it’s only with the United States which means the total amount is much higher. There have been two different reports on what’s going on in the UK. The first report is a confirmation of what is the cyber criminals’ objective. Cybercriminals are taking sensitive information and offering a price to keep that information from being leaked. The second report is about who is mainly being targeted in the UK. Retailers are targeted the most as they are seeing attacks occur at least once every 8 days. Retailers have been dealing with a lot of issues over the years and they believe that these attacks will only just increase over time. The cyber-attacks against retailers created problems within customer operations, the supply chain, and the ability to trade. IT leaders in retail have made it clear that IT should be their focus. An alarming report claims that 86 percent of an organization know where the vulnerabilities are but only 35 percent claim they address them. Let’s make a scenario where I lead the CISA in the US and the UK government officials contact me. The CISA in the US has done a better job of controlling these types of attacks. If I was given a contract by their officials to help fend off ransomware attacks, I would have a set plan for organizations to follow. My plan will consist of 12 important steps that will help reduce these attacks and even defend against them. The first 5 I will mention are the most notable ones in my opinion and can help a lot in the long term. The first step is to check for decryption tools, these tools can help if an organization has already been hit. The second step is not paying the ransom. A cybercriminal can bluff even if a payment was made after a system has been compromised just so they can get more money. The third step is a backup process step. Backing up data is one thing but testing them regularly is ideal and can help recover data in the event of an attack. The fourth and fifth steps would be patch management and multi-factor authentication. There are more steps I can refer to that can help aid the UK and decline the ransomware attacks by a better marine.

Sources

1. <https://blog.shi.com/cybersecurity/ways-to-protect-your-organization-from-ransomware/>
2. <https://eandt.theiet.org/content/articles/2021/11/ransomware-now-cyber-criminals-weapon-of-choice-as-uk-retailers-face-barrage-of-cyber-attacks/>