Lowering Ransomware

Kevin Picazo-Gonzalez

11/3/2021

South Piedmont Community College

Abstract

Ransomware is a sophisticated type of cyberattack and one of the most serious threats that security teams around the world face. Ransomware is used to attack all types of organizations, from small groups to large corporations, state systems, and government networks. When installed on a device, it scrambles or deletes all data until a ransom is paid to restore it. Microsoft is still attempting to deal with ransomware attacks that occur on a regular basis against their own and other companies. They are attempting to demolish criminal infrastructure through collaborative efforts. This helps to protect customers and improve the global internet community's security, so that all users can trust the technology and online services on which many rely for commerce and communication. One of the most effective solutions to this problem would be to implement a more secure and effective Multi-Factor Authentication (MFA) system. This solution has the potential to significantly reduce the number of cyberattacks that steal valuable data and information.

Introduction

To maintain global trust in technology and protect cyberspace from new and emerging threats, public policy must evolve. Microsoft supports these critical efforts by focusing on four broad policymakers' concerns: cybersecurity policy and resilience; cloud security and assurance; and cybercrime legislation and strategy, as well as collaborating with law enforcement and other public/private partnerships through the Digital Crimes Unit to disrupt nation-state activity. Cyberattacks pose a significant risk to the economy and national security. The world must be able to defend against known threats, respond quickly to new threats, and recover quickly from cyber incidents, whether the result of an accident, natural disaster, or malicious attack. Every day, many different types of cyberattacks occur, but ransomware is one of the most common and popular. Ransomware is a sophisticated type of cyberattack and one of the most serious threats that security teams around the world face. Ransomware is used to attack all types of organizations, from small groups to large corporations, state systems, and government networks. It is a type of malicious software (malware) that threatens to publish or restrict access to data or a computer system, usually by encrypting it, unless the victim pays a ransom fee to the attacker. In many cases, the ransom demand is accompanied by a deadline. If the victim does not pay the ransom in time, the data is lost forever or the ransom is raised. Ransomware attacks have become all too common in recent years. Ransomware has become a more serious threat in recent years. A number of high-profile attacks demonstrated to cybercriminals that ransomware was profitable, resulting in a rapid increase in the number of cybercrime groups using this malware. Ransomware claims a new victim every ten seconds on average around the world, and it will cost businesses around $20 billion in 2020, a 75 percent increase over the previous year. (Check Point, 2021) It has harmed major corporations. Microsoft must find ways to reduce the frequency of cyberattacks and prevent more from targeting critical files and data.

Cybersecurity is important because it safeguards all types of data against theft and damage. Sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and government and industry information systems are all included. Microsoft has dealt with a variety of attacks over the years, and they are doing everything they can to reduce the frequency and prevent more from harming critical information. Many files can be copied, altered, or destroyed if there is no security. Depending on the type of files a person has and how important they are to daily operations, not having cybersecurity can result in a variety of consequences ranging from inconvenience to complete shutdown.

Train a Team

Employees can act as a first line of defense against online threats and actively assist in preventing ransomware from infiltrating the organization's system. A strong security program combined with employee education about warning signs, safe practices, and responses can significantly help to prevent these threats. The best option is to look for a cybersecurity training company that can implement effective employee training. However, there are steps workers can take on a regular basis to ensure that employees are well-versed in the dangers of ransomware. First, make it a point to keep the staff up to date on the latest ransomware news. This can include companies that have been the target of a major attack, a new cybersecurity attack method, or other pertinent information. From there, train employees on the previously mentioned cybersecurity attacks on a regular basis. Inform them that they should never open email attachments unless they have permission from their supervisors. If they receive a suspicious message or email, teach them to check with the rest of their team to see if they received the same message. (CFISA, 2019) If not, notify the employees that these emails should be handled by executives. Cybercriminals are becoming more sophisticated, and they are devising new methods of attacking businesses. Ransomware prevention is critical, and the first step should be to train employees. The best approach is to hire a professional to train the staff. Because many people will notice the attack immediately and know how to deal with it, this method can make Microsoft more aware of each attack that occurs. While there are advantages, there are also disadvantages. One major flaw is the lack of time availability for those who detect a cybersecurity attack.

Cyber-attacks can occur at any time of day or night. People must be fully aware of this at all times. For full-time employment, most cyber security professionals work 40 hours per week in the office. They may also be required to work overtime on weekdays and weekends because cyber-attacks occur at any time. Another disadvantage is the time required for everyone to be fully trained to detect cyberattacks. It takes time for many people to be fully prepared and knowledgeable about detecting and stopping a cyberattack. Most people will need two years or more of regular study to fully understand and apply basic cyber security concepts. This amount of time is also dependent on the person's background and how in-depth they want to learn cyber security. When deciding on an endpoint security strategy, time and resources are critical. Having enough time to solve one attack while dealing with another is critical because delegating a task to another will not solve anything, and that person must complete one before moving on to the next attack. (Jon Hidalgo, Personal Communication, 10/28/21).

Multi-Factor Authentication (MFA)

To access a system or application, traditional single-factor authentication systems require users to provide only one verification factor, namely the password. Hackers can easily steal these passwords and use them to gain access to an enterprise system. To verify a user's identity and grant them access to an account, MFA systems require two or more factors. When a user needs to provide two or more pieces of evidence to verify their identity in order to gain access to an app or digital resource, this is known as multi-factor authentication. Multi-factor authentication protects against hackers by ensuring that digital users are who they claim to be. MFA ensures that an authorized user is who they say they are, reducing the possibility of unauthorized access. For these reasons, MFA is far more effective than passwords at protecting systems. All of these cyberattacks involve the theft of account credentials. To gain access to an account, MFA requires users to provide additional information or credentials. Even if an attacker is successful in stealing passwords, it is unlikely that they will also be successful in stealing or compromising the additional authentication factors required in MFA. As a result, MFA can deter cybercriminals and successfully combat a wide range of cyberattacks. Microsoft estimated that MFA can prevent over 99.9% of account compromise attacks (Microsoft Blog, 2021) Knowing or cracking the password will not be enough to gain access with MFA. MFA can also defend against more sophisticated attacks like MITM. Even if a hacker or malicious program infiltrates the interaction between users and applications and captures the information entered, MFA would require users to provide credentials from a different device. This keeps eavesdroppers from intercepting or manipulating communications between the user and the application. Push-based authenticators, such as mobile phone authenticators, are well-suited to providing a secure MFA mechanism while minimizing user inconvenience. MFA can also help prevent ransomware attacks. When an attacker gains access to account credentials, a ransomware attack begins. However, with MFA, the attackers lack the additional information needed to gain access to the target account. This keeps them from entering the system and thus prevents the attack. Furthermore, when IT administrators begin receiving unexpected MFA authorization requests, any unauthorized login attempts will trigger an alert. They can then take immediate action to keep these intruders at bay. The company can prevent ransomware attacks and protect themselves and other businesses from costly extortion demands by implementing MFA. Context-aware, adaptive MFA solutions, such as OneLogin's SmartFactor AuthenticationTM, are extremely effective in this regard. SmartFactor Authentication examines a variety of inputs, including user location, device, and behavior, to determine the number of authentication factors required to log in. It also evaluates the risk level for each login and dynamically adjusts the authentication requirements in real time. As a result, it reliably protects the organization from ransomware attacks. There may be some issues with this solution; for example, it may be difficult to implement multi-factor authentication across an entire organization, as it is frequently left up to the users to fully implement it. Cybersecurity administrators may not always be aware of an organization's use of multi-factor authentication. However, when properly implemented, multi-factor authentication can significantly improve cyber security without imposing a significant burden on the end user.

Implementation

To implement the solution of having multi-factor authentication to further improve Microsoft's cybersecurity, there must be issues to address before the entire solution is complete. Workers cannot be granted access to a specific application or system if they do not have access to the device or system to receive an multi factor and have not set up backup resources for authenticating user access. Another factor to consider is the cost and time required for the solution to be implemented. Multi-factor authentication has traditionally been quite expensive if an organization uses a solution that requires on-premises hardware and must integrate with existing identity solutions. The time required to log in to the system and verify using a mobile device or token, as well as setting it up for many others and their devices, can be inconvenient. There are some upfront costs, such as licenses (management, hardware, and for end users) and hardware requirements, such as high availability. Professional Services may also be required, depending on the change control requirements, to alleviate the burden on internal IT professionals. Help desk costs for end-users during deployment, as well as token shipping (if hardware tokens are required), must be considered. Other upfront costs may be less tangible, such as training and a price associated with increased productivity for enrolling users to authenticate using the platform. However, whether the costs are tangible or not, the total cost of ownership (TCO) is sometimes overlooked in the initial excitement to minimize network restructure disruption. When receiving an invoice for a maintenance renewal once the solution and training have begun to pay dividends, such as a decrease in calls for assistance. Maintenance renewals can be prohibitively expensive, and the costs are not always disclosed during the initial discussions. It's easy to see why ongoing total costs aren't always discussed or explored when the emphasis is on proof of concept and ease of deployment. Finally, even in the early stages of exploration, ignoring the costs of the solution in the medium term (years three and four) is a mistake. Ongoing maintenance costs may include help desk fees for end users and IT administration time for administrators. Patches and upgrades, new connectors/integrations, and even data center charges such as utility costs will be charged by suppliers. Implementing a solution like MFA is no easy task, and some suppliers will rely on others to bear the high ongoing maintenance costs because the thought of going through the entire process again is just too much to bear. Not wanting any unpleasant surprises after the first twelve months, make sure employees do their homework before signing on the dotted line. Everyone wants an easy life, especially when it comes to implementing something like MFA within their organization, but it's easy to get caught up in the 'plug and play' selling point, without realizing the hefty bills that can follow.

Conclusion

Microsoft's cybersecurity necessitates a more secure and safe system to prevent and protect users and businesses from cyberattacks, particularly ransomware attacks, which are one of the most common types of attacks that can target networks, data, files, and systems. There are numerous ways to reduce the frequency of ransomware attacks, but the best solution must be to implement a multi-factor authentication system for the company. Multi-factor authentication is an important and necessary tool in the fight against identity theft and unauthorized access to company resources. MFA, or multi-factor authentication, adds a second or third (or more) factor to the login process for company resources (apps, services, servers, etc.). It significantly improves the security of personal and professional information. Multi-factor authentication does not completely solve cybersecurity problems, but it does add another layer to security posture.

Works Cited

Jon Hidalgo, Personal Communication, October 28, 2021.

Biggest cyber security challenges in 2021. Check Point Software. (2021, November 2). Retrieved November 3, 2021, from https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cyber-security-challenges-in-2021/#.

Educate your employees: What Ransomware is and why you should care about the risks. cfisa.com. (2019, October 7). Retrieved November 3, 2021, from https://www.cfisa.com/educate-your-employees-what-ransomware-is-and-why-you-should-care-about-the-risks/.

The growing threat of Ransomware. Microsoft On the Issues. (2021, July 21). Retrieved November 3, 2021, from https://blogs.microsoft.com/on-the-issues/2021/07/20/the-growing-threat-of-ransomware/.

How to prevent ransomware. Trend Micro. (n.d.). Retrieved November 3, 2021, from https://www.trendmicro.com/en_us/what-is/ransomware/how-to-prevent.html.

How to stop ransomware attacks: The best ways to stop ransomware. Expert Insights. (2021, October 15). Retrieved November 3, 2021, from https://expertinsights.com/insights/how-to-stop-ransomware-attacks/.

Microsoft report shows increasing sophistication of cyber threats. Microsoft On the Issues. (2021, May 4). Retrieved November 3, 2021, from https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/.

A moment of reckoning: The need for a strong and global cybersecurity response. Microsoft On the Issues. (2021, June 15). Retrieved November 3, 2021, from https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/.

Multi-factor authentication: What is it and why should you use it? JumpCloud. (2021, October 19). Retrieved November 3, 2021, from https://jumpcloud.com/blog/what-is-multi-factor-authentication-and-why-should-you-use-it.

The potential hidden costs of deploying multi-factor authentication in your business. Swivel Secure. (2021, June 7). Retrieved November 3, 2021, from https://swivelsecure.com/blog/2019/07/10/the-potential-hidden-costs-of-deploying-multi-factor-authentication-in-your-business/.

Prevent, detect and recover from a ransomware attack. Lepide Blog: A Guide to IT Security, Compliance and IT Operations. (2020, June 15). Retrieved November 3, 2021, from https://www.lepide.com/blog/prevent-detect-and-recover-from-a-ransomware-attack/?utm_source=LepideBlog&amp;utm_medium=Internal&amp;utm_campaign=15Cyber.

What is ransomware? - definition, prevention &amp; more: Proofpoint us. Proofpoint. (2021, October 28). Retrieved November 3, 2021, from https://www.proofpoint.com/us/threat-reference/ransomware.

What types of attacks does MFA prevent? OneLogin. (n.d.). Retrieved November 3, 2021, from https://www.onelogin.com/learn/mfa-types-of-cyber-attacks.