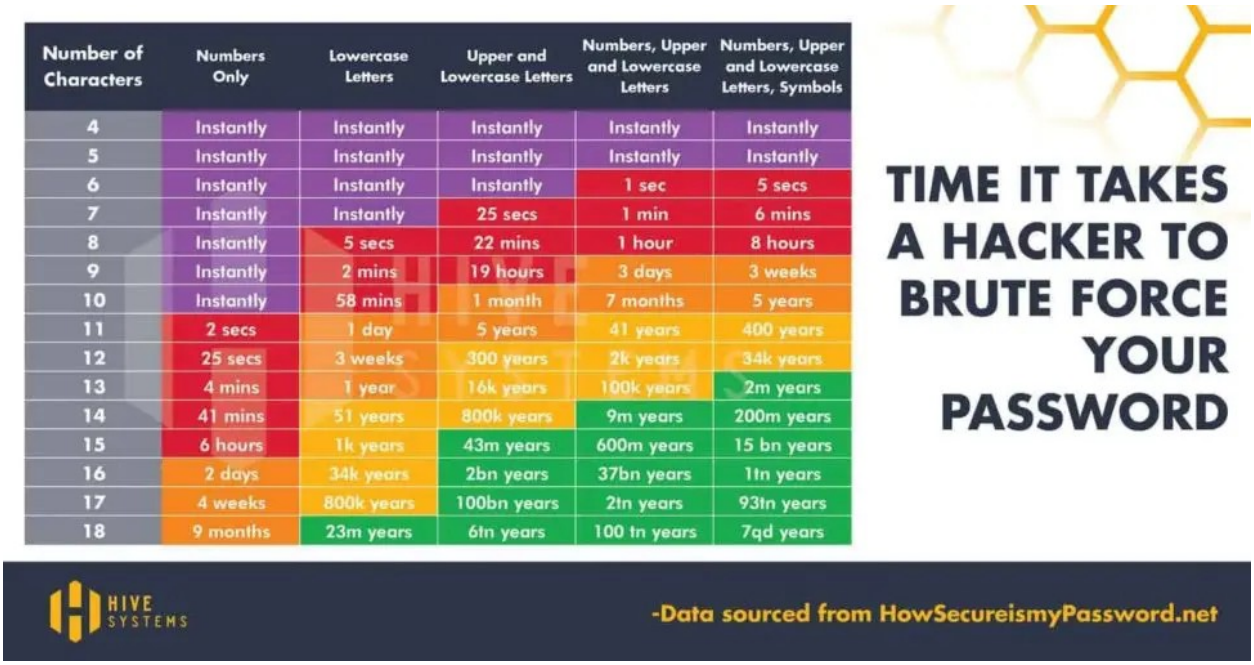
Introduction

In today's day and age, it is important that businesses, of all shapes and sizes, pay sufficient attention to the cybersecurity threats that are currently prevalent for their specific industry. When it comes to data breaches, everyone always thinks, "This won't happen to me.", but data is extremely lucrative whether you are a multi-billion dollar enterprise organization, or a family owned and operated business. For this reason, we at A3C Consulting pride ourselves on our extensive knowledge of the threat landscape and provide our clients with recommendations that will improve their security posture and help maximize their business returns. The following are recommendations we have for a small to medium-sized entity, focusing on software development and mobile app creation. These cost-effective yet efficient security considerations are recommendations for a business with a low to moderate budget for security enhancements.

Authentication

There are many different ways to ensure that the client's GitHub system is configured to enforce security best practices. Contrary to popular belief, the client can put relatively low cost measures in place while still achieving a well rounded security posture and also ensuring the integrity of their proprietary information in the GitHub repository. One of the organizations' first lines of defense against hackers is their password complexity requirements. It's imperative that the client enforce more than the minimum number or characters while also requiring the use of numbers, special characters, and both case sensitivities. "On average, it takes a hacker about two seconds to crack an 11-character password that uses only numbers. Throw in some upper- and lower-case letters, and it will take a hacker one minute to hack into a seven-character password." (Fripp, 2021). GitHub natively comes with the ability to enforce a password complexity requirement of a 15 character length with any combination of characters, numbers, and special characters.

According to the chart below, this estimates that the time needed to crack this password is 15 billion years. However, we all know this highly depends on the computational power being used to crack the password. Even though the probability of a password being cracked is low when enforcing strong password complexity requirements, there are other measures the client can take in conjunction with password complexity requirements to protect their environment.



By configuring the GitHub server to enforce two-factor authentication the client can significantly increase their security posture and reduce the risk associated with a breach associated with a username and password hack. “Two-factor authentication (2FA), sometimes referred to as two-step verification or dual-factor authentication, is a security process in which users provide two different authentication factors to verify themselves.” (Rosencrance, 2021). Two-factor authentication leverages two of the following criterias: something the user knows- the password, something a user has- a security token, and something the user is- a form of biometrics, to grant access to networks, applications, and databases. GitHub natively comes with the ability to configure several forms of two-factor authentication- some of which include: using time-based one-time passwords, using text messages, and using security keys.

We feel that the client's security posture will be maximized by configuring two-factor authentication using a complex password along with an authenticator to implement a time-based

one-time password. “A time-based one-time password (TOTP) is a temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors.” (Steele, 2022). This option gives the individual users accessing the GitHub repository the ability to select their own authenticator while still ensuring that the same security is being met. When a user wants to access the repository, they navigate the web interface and input their username and complexity compliant password. The authenticator then uses the current time of day and a shared secret key to generate a temporary password that expires within a certain amount of time- generally within 30, 60, or 90 seconds. The user will enter the temporary password and be granted access to the repository. By implementing a time based one-time password, the GitHub server repository will have an added layer of security and help prevent compromise- even if a threat actor were to come into possession of a username and password.

Virtual Private Networks (VPNs)

With threats like data breaches and cyber attacks becoming more commonplace against small businesses and an increase in remote work, safeguarding data as it's being remotely accessed is critical (Goldberg, 2023 & Segal, 2022). One technology that will accomplish this is a Virtual Private Network (VPN). A VPN is a secure method of establishing remote access to your GitHub server via the internet that protects your data and your worker’s privacy. VPNs use tunneling or encapsulation protocols, which wraps data being sent from remote workers in a secure protocol which can then be securely sent over the internet. VPNs can be thought of as private tunnels through the internet that shield and secure all data being sent through them. Some encapsulation protocols also encrypt the data to provide another layer of protection. A hybrid VPN provides both confidentiality and integrity of data over trusted VPN connections. A VPN

will provide a simple, easy and efficient way for remote workers to securely connect to the GitHub server (Stewart & Kinsey 2020).

VPNs provide many benefits for business, including secure remote access, data encryption, and masking of IP address, network segmentation, and two-factor authentication. Secure remote access is essential for the success of business. A VPN ensures that workers can safely access the resources they need, such as the server and all files, without exposing the business's network to outside threats. Additionally, remote workers can log onto public IP addresses, such as coffee shops, hotels, or libraries, and will still have a secure connection to the server. This also allows workers to use their own devices to securely connect to the GitHub server (Stewart & Kinsey 2020).

A VPN will encrypt all data transmitted to and from the server. This means that even if the data is intercepted by a hacker, they will not be able to decipher any content, thus all proprietary and sensitive information is protected. A core service of VPNs is the protection of the user's actual IP address. This prevents hackers from tracking the user's online activity and prevents the user's location from being revealed as well. Public Wi-Fi networks are often unsecured and can be a hotbed for cybercrime; a VPN will protect your user's location and activity (Stewart & Kinsey 2020).

A VPN will also allow for network segmentation, which can enhance server security. Remote workers can be assigned to specific network segments based on necessary resources for their roles. This will further safeguard data and protect proprietary information on the Github server. The VPN will also allow for integration with two-factor authentication, requiring remote workers to provide two types of identification before accessing the network. Users will have a password and can also be required to have a Yubikey before logging on. This adds another layer

of security so that even if a password is compromised, a hacker could not gain access to the Github server without the second form of identification (Stewart & Kinsey 2020).

This technology typically costs on average $72/year (Haan, 2023) and will greatly enhance the security of your network. VPNs provide an extra layer of security and privacy, protecting your Github server and your remote workers.

Physical Security

By implementing surveillance cameras around the server room allows for real-time monitoring and allows businesses to track unauthorized physical access attempts. These devices are even more helpful when combined with advanced features like motion detection. Camera surveillance acts as a deterrent and, at the same time, gathers valuable evidence in case of a security breach (Han, 2022).

Cameras would be strategically positioned to cover all potential access points and sensitive areas inside the server room. This can include doorways, and the server racks themselves. High-resolution cameras should be used to ensure that the captured footage is of high quality to be able to identify intruders or malicious actions (Bhattacharya, & Sengupta, 2023). Also, by using clear and visible signage at access points has many purposes. Firstly, it acts as a deterrent, warning potential intruders of the surveillance measures in place. Secondly, it can provide legal protection for the business by demonstrating that any potential intruders were clearly warned (Blythe, 2021). Signs can also serve as a guideline for authorized personnel, reminding them of their responsibilities and the necessary precautions when entering and operating within the server room. These guidelines may include instructions on securing the door behind them.

Physical security measures can be supplemented with policies that control access to server rooms. These policies include guidelines on who has access to the server rooms, when access is permitted, and the procedures for granting temporary access to visitors or maintenance personnel (Palmer, 2021).

While firewalls and other digital security measures are essential, it is also important to address physical security. Surveillance cameras and clear signage, in combination with stringent access control policies, can significantly enhance the overall security of an organization's information infrastructure.

Honeypots

A honeypot within a network is the name given to a service or workstation that is utilized as a decoy. It is a fake system that doesn’t have any real data worth anything that the hacker can steal. If a honeypot is hacked, no real damage is done. In fact, the goal of a honeypot is to attract hackers to attack it. (DevSafeHouse) Its role in network security is to attract malicious parties to it by being intentionally vulnerable. Because a honeypot should have no network traffic going to it, it will be easy to detect malicious intent when someone interacts with the honeypot. This detection and interaction by a threat actor can serve several security purposes with the goal of protecting the network from malicious attacks while securing and preserving data.

Network traffic to the honeypot can serve as an early warning or as an indicator that someone is attempting malicious actions against a network whether from the outside or from the inside of the network. These actions can trigger alerts which allows for a swift response to securing the network. These responses could be automatic where the IP is automatically put on the deny list or they could be a manual response A honeypot should be configured to record all

activity against it. In this manner the actions recorded by the honeypot are used to study attacker behaviors and this data can be used to further secure the network. A honeypot serves as an excellent means to stop or delay threat actors, record threat actor techniques, learn from attacks, fine tune network security appliances (NSA) or gather analytics to drive network security business decisions. What is learned by using a honeypot can be used in many different ways with the goal being to protect, secure, and preserve data.

Firewalls are an excellent NSA and when configured properly provide a good level of security. However, attackers can find ways around a firewall thus this should be taken into consideration when designing a secure network. We recommend the use of a honeypot within any small to medium sized business's (SMB) network as it can serve as a means to identify a possible intrusion where other measures fail. We assume that the honeypot will be placed beyond the firewall and have no network traffic going to it thus allowing malicious traffic to be easily recognizable. The honeypot solution should be low cost and easy to use and set up. Alerts should be configured requiring a manual response and all activity should be automatically recorded. This configuration maximizes security while taking into consideration lack of personnel and budget considerations for the SMB where we assume there is a small budget. The honeypot should mirror a service that exists on the network such as the GitHub repository. We make this suggestion because this will further enhance any analytics and lessons learned from any honeypot interaction as any hardening actions to be taken will be directly correlated with further protecting the actual GitHub repository.

Conclusion

We have outlined four different solutions for security that extend beyond the firewall. Firewalls serve an excellent purpose in filtering traffic with many firewalls including several feature sets such as anomaly detection or packet inspection; however, it is not prudent to trust the entirety of security on one layer of defense. Threat actors are savvy and are very good at finding ways to circumvent security measures. Businesses of all sizes must take their network security seriously as it is the avenue for the life of their business and valuable data. It is not enough to rely on only one solution, such as a firewall, but rather to incorporate a layered, defense in depth strategy. (Stewart & Kinsey, 2020)

As our solutions have demonstrated, network security for businesses of any size is possible. A firewall in conjunction with the solutions we have presented make for a well rounded application of security. Harnessing the plethora of free or low cost security applications available coupled with the ingenuity in bringing those pieces together in a secure network design is the product of a robust network security engineering methodology that is a key component in the solutions we deliver.

References

Bhattacharya, S., & Sengupta, A. (2023). Surveillance Technologies and Infrastructure Security. Security and Communication Networks, 17(8), 123-134. Retrieved July 26, 2023.

Blythe, J. M. (2021). The Legal and Ethical Implications of Surveillance in the Workplace. Legal Studies Review, 41(4), 65-80. Retrieved July 26, 2023.

DevSafeHouse. (2021, June 9). What Is a Honeypot and How Does It Help My Business? Medium.https://devsafehouse.medium.com/what-is-a-honeypot-and-how-does-it-help-my-business-7f0acb31d44d

Fripp, C. (2021, March 22). Use this chart to see how long it'll take hackers to crack your passwords. Retrieved from https://www.komando.com/security-privacy/check-your-password-strength/783192/

GitHub Docs (n.d.). Creating a strong password. Retrieved July 27, 2023, from https://docs.github.com/en/authentication/keeping-your-account-and-data-secure/creating-a-strong-password

GitHub Docs. (n.d.). Configuring two-factor authentication. Retrieved from https://docs.github.com/en/authentication/securing-your-account-with-two-factor-authentication-2fa/configuring-two-factor-authentication

Goldberg, E. (2023, April 3). Do we know how many people are working from home? *The New York Times*. Retrieved August 3, 2023, from https://www.nytimes.com

Han, J. (2022). Advanced Surveillance Cameras for Enhanced Security: A Review. Journal of Information Security, 19(2), 45-60. Retrieved July 26, 2023.

Haan, K. (2023, July 30). Best Business VPN Of 2023. Retrieved August 3, 2023, from https://www.forbes.com/advisor/business/software/best-business-vpn/

Palmer, D. (2021). The importance of physical security in the workplace. Security Management, 24(6), 36-40. Retrieved July 26, 2023.

Rosencrance, L. (2021). Two-factor authentication (2FA). Retrieved from https://www.techtarget.com/searchsecurity/definition/two-factor-authentication?Offer=abt_pubpro_AI-Insider

Segal, E. (2022, March 16). Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report. *Forbes*. Retrieved August 3, 2023 from https://www.forbes.com

Steele, C. (2022). Time-based one-time password. Security. Retrieved from https://www.techtarget.com/searchsecurity/definition/time-based-one-time-password-TOTP?Offer=abt_pubpro_AI-Insider

Stewart, J. M., & Kinsey, D. (2020). *Network security, firewalls, and VPNs*. Jones & Bartlett Learning.