CHAMELEON

FOR OUR SMARTER WORLD

Security Threats and How Chameleon Can Prevent and Defend Them.

Contents

Overview

As current technology evolves every coming day it becomes easier to make more complex security systems with advanced encryption to defend our valuable information. However, with the evolution of security systems we have to consider the evolution of security threats and how they can be detrimental to the safety and wellbeing of the companies' assets and the employees. This report contains an overview of the current security threats chameleon could be vulnerable to if security standards are not upheld as well as how employees should perform during an attack and the steps the company will take to recover if an attack is successful.

Initial Prevention Countermeasures:

This section will provide a range of steps employees will take both in and out of the security department at the bare minimum to ensure solid security practices.

Methods

1. Avoid Sharing of unencrypted passwords.

Passwords under no circumstances should be shared between employees, via email, text or any other method, once a password is run through a network it is compromised and therefore susceptible to being intercepted by cybercriminals.

2. Multi-Factor Authentication

All employees will need to have MFA set up on a device to verify their identities. MFA is a standard security procedure in the workplace now and will need to be used to when logging on to any new device.

3. Avoid any work unrelated E-mails or Texts

Especially on work devices we ask that all employees do not respond or open any emails or texts from non-staff personnel or authorized clients. This is to ensure employee credentials are not stolen or dangerous viruses are not implemented onto the work system.

4. Use Company Provided VPN outside of the Office.

Employees who need to work from on certain occasions should sign into the company VPN to ensure all company information is on the company network and not on an employee on personal network, keeping it under chameleon security.

Failures to comply.

Employees who fail to comply with these regulations will be met with warnings and future security checks as well as having to meet with chameleon leaders about why they are not complying with these regulations.

Different Cyber Threats and Risks

Distributed Denial of Service Attacks (DDoS)

A DDoS attack is series of web requests targeted at a specific server to flood the website with traffic making the service times slow down often resulting in no access to its services for employees. If an attack is successful, it will more than likely boot the server offline, it is not necessarily used as the primary source for an attacker to cause damage rather as a distraction to implement other cyber intrusions or fraud.

Malware

Malware or malicious software or code, is a program designed to infiltrate company systems secretly and compromise integrity and accessibility of data. Malware can affect data, programs and operating systems often used to cause disruption. Specific malware types such as Spyware is becoming an increasingly more effective privacy threat that tracks user data to conduct financial fraud.

Ransomware

Similar to Malware ransomware is a malicious code implemented onto a system that Is used to encrypt a user's files and in which the attacker will demand a sum of money to remove the encryption giving access back the user. In a company environment this can be detrimental as it means sensitive information cannot be accessed but can also be duplicated by the attacker.

Cooperate Account Takeover (CATO)

CATO is cyber criminals impersonating a business and sending wire and ACH transactions to multiple banks of their own bank accounts resulting in huge losses for vulnerable companies.

How Threats Are Dealt With

Some of the basic and common ways of dealing with cyber threats is to make sure all software and devise are up to date and or regularly updated. Out of date software is more vulnerable to intrusion as it often does not comply with updated security functions.

Blocking DDoS attacks can be done by limiting the surface attack area can be done by sending traffic through to specific locations with a load balancer that will disperse traffic evenly over multiple servers or computers. Blocking unusual ports will also prevent traffic coming from an attacker as they will more than likely not have access to the main network ports.

Dealing with Ransomware and Malware is very similar, as mentioned above, avoid any unusual emails or texts messages which is what the malicious code or software is usually transported through. The next thing to manage is data by having a backup of all the data not connected to the same network, this can be extremely valuable during an attack.

Preventing CATO attacks primarily about looking out for the warning signs, this can include a spontaneous increase in the number of emails asking for personal information, unusual network activity as the attacker would be looking for weaknesses. Unwarranted password resets are key factor that the system has potentially been breached and should be alerted

straight away. Finally, any unauthorized transactions if not flagged, the attacker will be able to run away with the money.

What happens during an attack?

Each of these attacks have a different defence response that will need to be understood. When DDoS attack is occurring, you will notice a sudden spike in traffic or slowness of a service, if this is the case report immediately. If a DDoS attack is occurring beginning to flood the system, rate limiting should be applied to limit the amount of request however it will not be adequate enough to withstand a massive attack. When an attack is large enough admins should enable blackhole routing where all requests to a null route and be dropped from the network.

During a malware or Ransomware attack it is key to finding the affected device. Once the infected device is known, is it time to isolate said device. Isolating devices can be done by turning off any maintenance tasks that could spread the code or software to other devices. The device should then be dropped from the network for further analysis. It should be noted that during an attack all backup systems are to be kept offline as most malware/ransomware is now designed to hunt the backup systems almost instantly. Decryption tools are to be used for ransomware attacks once the device is dropped from the network to try and regain access to the files.

During CATO attack, the companies bank provider must be notified immediately, and any suspicious transactions are to be investigated and flagged to be sent to the bank.

How do we recover from an Attack?

Post threat it is important that all company passwords are to be updated on every single device.
All devices and software must have a security update and to be checked to see if they were up to date before the attack was initiated.
Security teams will go through a forensic analysis on the affected devices/servers, a security report is required to outline what happened during the attack and where the weaknesses in the system.
A follow up meeting will occur discussing potential security changes so that chameleon can avoid future threats.

Conclusion

It is important that all members of the chameleon company read and are aware of the security threats a stake and follow all necessary precautions to avoid having to go into a threat defence response.
The security team will need to be up to date on the threats and the plan when being attacked.

References:

Badman, A. (2024). *How to handle a ransomware attack*. [online] IBM Blog. Available at: https://www.ibm.com/blog/how-to-respond-to-ransomware-attack/.

Cloudflare (2024) *How to prevent DDoS attacks.* [online] Available at: https://www.cloudflare.com/en-gb/learning/ddos/how-to-prevent-ddos-attacks/

www.loginradius.com. (n.d.). *Corporate Account Takeover: Detecting & Preventing it | LoginRadius | LoginRadius Blog*. [online] Available at: https://www.loginradius.com/blog/identity/corporate-account-takeover-attacks/.