THE BEACON

Florida Fusion Center #22-054 May 2022 Issue #26

Table of Contents

CONTACT THE FIPC:
Phone: (850) 410-7645
Email: FIPC@fdle.state.fl.us

EDITOR'S CORNER

Time to Patch Things Up: Downloading Software Updates

When that notification on your computer or mobile device comes up saying a software update is available, do you update it right away or hold off on installing it?

Unfortunately, issues with software and devices may not be discovered immediately and devices can face vulnerabilities long before an update becomes available. To protect yourself and your devices, don't hit snooze! Make 2022 the year you install updates as soon as they become available.

You may think an update can wait, but there are many reasons why you should prioritize installing them as soon as they are available. This includes repairing functionality issues and "bugs" in programming to making the software less susceptible to malware. However, the main reason why you should keep your software as current as possible is because these updates often address weaknesses or vulnerabilities[a] that cybercriminals, including foreign nation-state actors like Russia, may exploit.[1] When these vulnerabilities are discovered, software companies and vendors issue "patches" that fix specific problems.

Cybercriminals are always looking for ways to infect devices with malware and/or gain access to them to steal data or launch cyberattacks. One of the main ways they can obtain access to devices is through exploiting vulnerabilities. Sometimes cybercriminals discover zero-day vulnerabilities[b] before software vendors know about them, which means there is no patch available to fix the flaw(s). The vulnerability can be exploited and can adversely affect your device until a patch is available and installed.[2] This is why it is so important to install patches and updates as soon as they are available.

In September 2021, a major technology company known for making computer devices issued operating system security patches for a zero-day vulnerability that could have allowed cybercriminals to install spyware without any user interaction. Additionally, a company responsible for a widely used computer operating system issued a patch for a zero-day vulnerability that could have led to remote code execution.[c 3] Another company known for a popular web browser issued security patches for at least 17 zero-day vulnerabilities in 2021, however, the details

of how those vulnerabilities were being exploited were not reported.[4]

Regularly installing updates can protect your devices, your data and even the network you're connected to.

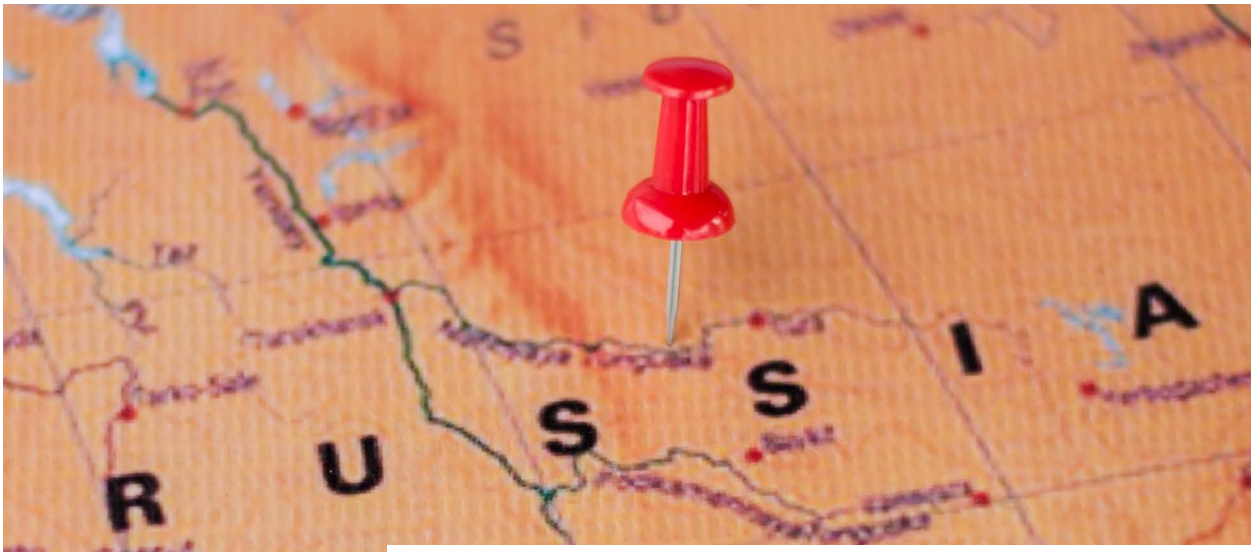
Sometimes important fixes are needed to address known software weaknesses that can put your devices at risk if not downloaded. These updates can help you protect your devices, your data and even the network you are connected to. If your device gets infected, you could pass it on to your friends, family or your workplace if you connect to their networks.[5] Next time you see that reminder to download a current version of software, do not ignore it. One of the best ways to protect yourself from cyberthreats is to download these updates and plug up those security holes.

[a] A software vulnerability is a security flaw, glitch or weakness found in software code that could be exploited by an attacker (threat source).
[b] A zero-day vulnerability is an unknown flaw or weakness that can be exploited and has not yet been patched.
[c] A remote code execution (RCE) attack happens when a cybercriminal illegally accesses and manipulates a computer or server without the owner's authorization. A system can be taken over using malware.

[1] https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html
[2] https://www.wired.com/story/update-ios-windows-chrome-zero-day-patch/
[3] https://www.bleepingcomputer.com/news/security/google-pushes-emergency-chrome-update-to-fix-zero-day-used-in-attacks/
[4] https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html

CYBER THREATS

Russia Cyber Threat Information



There is currently no known credible cyber threat to Florida from Russia. However, cyberattacks by Russia against Ukraine have the potential to spread. Tactics used in the past by Russian actors include phishing, malware deployment, distributed denial of service attacks and compromising remote desktop protocol.

For information on how to protect your organization from Russian cyber threats, visit Secure Florida's Russia Cyber Threat Recommendations and Resources site.

You can also visit the Cybersecurity and Infrastructure Security Agency's (CISA) Shields Up and Russia Cyber Threat Overview and Advisories sites for more information on foreign cyber threats, best practices, mitigation strategies and open-source intelligence products.

Double Extortion Equals Double The Trouble

Ransomware has been around since 1989, but the threat has grown significantly since internet use picked up in the early 2000s. This threat has gone from being deployed via floppy disks to now sometimes being deployed through virtual machines[a] controlled by cybercriminals.[1] These criminals are often located in foreign countries, and their tactics continue to evolve.[2] In 2017, after WannaCry and NotPetya ransomware attacks caused massive financial and reputational damage to organizations around the world, many businesses and organizations placed increased emphasis on data backups, restoration processes and stricter security measures. In an effort to circumvent these added security measures, cybercriminals came up with new strategies to pressure victims into paying.

Over 90% of ransomware incidents are believed to be initiated through phishing attacks that contain malicious files and links that lead to malware infections or account credential theft.

In late 2019, some ransomware groups began using a type of attack known as double extortion, which involves exfiltrating data obtained during the ransomware attack. Essentially, if an organization refused to pay after having their data encrypted, cybercriminals threatened to leak their information, sell it online or destroy it. Businesses and organizations should consider whether they need to make changes to their security posture to address these tactics and other evolving threats, even if they have robust backups and data recovery plans in place. The exfiltration process can lead to compromised intellectual property, reputational damage and compliance fines.[3] Therefore, it is crucial to defend against these attacks before they occur.

Use of the double extortion tactic continues to expand. As of June 2021, cybersecurity researchers have identified at least 35 ransomware variants that have used double extortion and the list continues to grow.[4] Ransomware groups have turned to this tactic because they believe it is more likely to get organizations to pay ransoms, especially if the organization is able to recover their information.[5] It is important to note that paying a ransom does not guarantee you will get your data back if you are the victim of double extortion. Cybersecurity researchers have also found that some ransomware groups have still posted or sold organizations' data even after receiving ransom payments.[6]

There are many precautions computer users and organizations can use to prevent double extortion attacks. Over 90% of ransomware incidents are believed to be initiated through phishing attacks that contain malicious files and links that lead to malware infections or account credential theft.[7] In order to defend against these

Organizations need to educate their staff regularly on how to identify and avoid phishing scams and practice good cyber hygiene.

attacks, organizations need to educate their staff regularly on how to identify and avoid phishing scams and practice good cyber hygiene.[8] Secure Florida offers FREE training for organizations looking to educate their users on cybersecurity best practices.

Cybercriminals will also look to exploit software vulnerabilities, unsecured remote desktop protocol ports and stolen account credentials from other data breaches to initiate double extortion ransomware attacks.[9] It is important to install patches and updates on software and devices as soon as they are released.

By using these preventative measures, organizations can avoid falling prey to these attacks and keep their data safe. Visit StopRansomware.gov for more information on how to prevent double extortion ransomware attacks.

[a] Virtual machines are software-based computers that exist within another computer's operating system, often used for testing purposes, backing up data or running certain applications. They provide the functionality of a physical computer.

[1] https://www.darkreading.com/threat-intelligence/vms-help-ransomware-attackers-evade-detection-but-its-uncommon/d/d-id/1341380
[2] https://www.fortinet.com/blog/industry-trends/analyzing-the-history-of-ransomware-across-industries
[3] https://www.darktrace.com/en/blog/double-extortion-ransomware/
[4] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
[5] https://www.cybereason.com/blog/rise-of-double-extortion-shines-spotlight-on-ransomware-prevention
[6] https://securityintelligence.com/news/when-cyber-gangs-disregard-ransomware-payments/
[7] https://hipaatrek.com/double-extortion-what-it-is-and-how-you-can-prevent-it/
[8] https://heimdalsecurity.com/blog/double-extortion-ransomware/
[9] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22

The Cost of Doing Business: Third-Party Attacks

Third-party cyberattacks have been increasingly making the news over the last few years. Third-party organizations include vendors, partners, contractors and others that provide services and expertise to organizations. Some may have access to your internal systems and sensitive data depending on the type of service provided.[1] A third-party attack, which is a type of supply chain attack, occurs when cybercriminals target outside partners or service providers in order to harm and compromise the organizations that they work with by exploiting their network access.

A third-party attack, which is a type of supply chain attack, occurs when cybercriminals target outside partners or service providers in order to harm and compromise the organizations that they work with by exploiting their network access.

Organizations rely on third-party software products every day, including antivirus, IT management and remote access software among others. These products may require privileged access[a] to operate and frequent communication between a vendor's network and their customers' networks.[2] Cybercriminals can target vulnerabilities in software, hardware, applications and other products developed by vendors.

These attacks are becoming increasingly common and are attractive to cybercriminals. By targeting widely used software, products or vendors, they can potentially gain access to a large number of enterprises[b] across industries with one single attack. One example is the March 2020 hack targeting a Texas-based IT management software development company, which has been since attributed to Russia. In this attack, the infiltrators injected malicious code into a software update that was downloaded by approximately 18,000 of their customers globally. This attack focused on the development and production phase of the software supply chain lifecycle, and as many as 250 organizations were reportedly affected, including U.S. government and enterprise networks.[3][4][5][6]

Cyberattacks on third parties can be costly to organizations, whether cybercriminals are conducting corporate espionage or trying to interfere with critical infrastructure. Working with third parties comes with risks, and ongoing collaboration with vendors to ensure cybersecurity is important. Here are some steps that can be taken to protect yourself and your organization.

1. Assess risk potential before granting access to your system and data – This can be done by having the vendor complete a questionnaire to find out what services will be provided, the location and level of data being accessed,

stored or processed and other factors that are related to potential security risks. You can create your own or find templates online.

2. Create a security matrix – Create a central repository of all of your third-party vendors, if you do not already have one, and assign risk ratings to vendors based on their level of access to your organization and the level of security or training you require. For example, you can classify vendors as high, medium or low risk. Depending on the level of risk, you may determine the need for specific risk management strategies such as multi-factor authentication or security awareness training.

3. Monitor your vendors continuously – A vendor's security posture can change over time. Relying on that initial risk assessment only could lead to future security issues if you have not been monitoring your vendor's security controls. Make sure that you work with vendors to regularly evaluate their security and access to your network.[7] [8]

Third-party risks will continue to evolve, especially as organizations' service needs change. Risks can be mitigated; however, this requires a high level of vigilance from customers as well as vendors.

Third-party risks will continue to evolve, especially as organizations' service needs change. Risks can be mitigated; however, this requires a high level of vigilance from customers as well as vendors.

[a] Privileged access is a term used to designate special access or abilities above and beyond that of a standard user. An example would be a super user account used by IT system administrators to make changes to a system or application.
[b] An enterprise is an organization of any size with many systems and users to manage.

[1] https://www.upguard.com/blog/third-party-vendor
[2] https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[3] https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html
[4] https://www.zdnet.com/article/solarwinds-hacking-group-nobelium-is-now-targeting-the-global-it-supply-chain-microsoft-warns/
[5] https://www.forbes.com/sites/chuckbrooks/2021/10/24/more-alarming-cybersecurity-stats-for-2021-/?sh=334b1aa04a36
[6] https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
[7] https://www.csoonline.com/article/3634375/6-steps-for-third-party-cyber-risk-management.html
[8] https://www.upguard.com/blog/prevent-third-party-data-breaches

Cybercriminals Forcing Their Way Into Networks: A Look at Brute Force Attacks

When cyberattacks occur, complex tactics or technology may come to mind. However, that is not always the case. Some attacks can be the result of a generally unsophisticated, yet commonly used method, known as a brute force attack. A brute force attack is a trial-and-error method used by cybercriminals to attempt to gain unauthorized access to a system or an account by repeatedly entering account credentials manually or by using automated software. The goals of criminals in these types of attacks are usually to uncover passwords to compromise accounts, find sensitive data or information that may be hidden or to initiate other types of cyberattacks like ransomware.

A brute force attack is a trial-and-error method used by cybercriminals to attempt to gain unauthorized access to a system or an account by repeatedly entering account credentials manually or by using automated software.

Brute force attacks can be time consuming as cybercriminals have to discover the correct usernames, emails or passwords, especially if they are doing so manually. As a result, many cybercriminals have turned to automated tools that check many different password combinations until the correct one is found. Some also leverage leaked credentials from corporate data breaches.[1] [2]

Cybersecurity researchers detected 55 billion new brute force attacks between May and August 2021 alone, which was more than double the attacks detected between January and April 2021. Cybercriminals can use different variations in an attempt to access users' emails, remote desktop protocol, banking accounts or other systems. Types of brute force attacks include simple brute force attacks,[a] dictionary attacks,[b] hybrid brute force attacks,[c] credential stuffing[d] and password spraying,[e] among others.[3] In July 2021, several U.S. federal intelligence agencies in collaboration with a foreign intelligence agency reported that a Russian military cyber unit was behind a widespread brute force attack campaign that targeted hundreds of government and private-sector organizations worldwide from mid-2019 to early 2021. The campaign was likely conducted to exfiltrate data, access credentials, maintain persistent network access and more.[4] [5]

A key indication of an attempted or ongoing brute force attack is the amount of failed login attempts, particularly from a single IP address. A dramatic increase in failed login attempts for either a single account or across several accounts may indicate an attack. Additionally, the cybercriminal may attempt to log in to accounts in a systematic way, either by account name or number. Reports of failed login attempts with an alphabetical or numerical pattern

may be an indicator as well. Finally, an administrator may look at the times in which the failed login attempts occurred. If the usual login attempts were made outside of normal business hours, this may indicate the need for additional research to determine whether they were the result of a potential brute force attack.[6]

All passwords should be at least 15 characters long, where possible, and include a combination of upper- and lowercase letters and special characters.

The first line of defense against a brute force attack is a strong password. All passwords should be at least 15 characters long, where possible, and include a combination of upper- and lowercase letters and special characters. As the complexity of a user's password increases, the difficulty of discovering a correct password increases as well. Cybercriminals often rely on weak and reused passwords to easily access systems and domains.[7] Users should also make sure they follow their organizations' security policies and keep their passwords private.

From an organizational standpoint, time-out and lock-out features can be enabled to temporarily disable accounts after a set number of consecutive failed login attempts. Organizations can also consider implementing multi-factor authentication and CAPTCHAs[f] to provide an added level of protection in case a password is guessed correctly. Finally, organizations can explore using the highest available encryption[g] rate for passwords, which could make it harder for even some of the most powerful computers to guess the correct passwords.[8] [9]

[a] A simple brute force attack occurs when a hacker attempts to guess a user's login credentials manually without using any software.
[b] A dictionary attack tries combinations of common words and phrases.
[c] A hybrid brute force attack combines a dictionary attack method with a simple brute force attack.
[d] A credential stuffing attack uses stolen login combinations across a multitude of sites.
[e] Password spraying involves trying to apply one common password to many accounts in an effort to avoid getting caught by lockout policies that limit the number of password attempts.
[f] A CAPTCHA is a type of challenge-response test used in computing to determine whether or not a user is human.
[g] Encryption is a cybersecurity tactic that scrambles data so it appears as a string of random characters.

[1] https://www.fortinet.com/resources/cyberglossary/brute-force-attack#:~:text=%20What%20is%20the%20Motive%20Behind%20Brute%20Force,A%20hacker%20may%20simply%20want%20to...%20More%20
[2] https://www.varonis.com/blog/brute-force-attack/
[3] https://www.crowdstrike.com/cybersecurity-101/brute-force-attacks/
[4] https://therecord.media/fbi-nsa-russian-military-cyber-unit-behind-large-scale-brute-force-attacks/
[5] https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF
[6] https://securitytrails.com/blog/brute-force-attacks
[7] https://www.forcepoint.com/cyber-edu/brute-force-attack
[8] https://www.fortinet.com/resources/cyberglossary/brute-force-attack#:~:text=%20What%20is%20the%20Motive%20Behind%20Brute%20Force,A%20hacker%20may%20simply%20want%20to...%20More%20
[9] https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

Pro-TECH Yourself and Avoid This Scam

Have you ever received calls, emails, texts or pop-ups on websites telling you there is a problem with your computer or that your antivirus software is out of date? This is known as the tech support scam, which is a common scam that aims to either trick computer users into paying for unneeded services or steal money or data from the victims. A well-known antivirus company reported that their company alone blocked 12.3 million tech support URLs from July through September 2021, which was approximately 88% of the total phishing attempts they blocked during that time.[1] [2] This demonstrates the ongoing prevalence of tech support scams and the importance of being able to recognize if you're being scammed.

Tech support scammers often attempt to impersonate a well-known company either by using a spoofed phone number or using their name or logo.

Tech support scammers often attempt to impersonate a well-known company either by using a spoofed phone number or using their name or logo. If they make contact with a potential victim, the scammer may use scare tactics such as telling someone they will lose all of their files if they do not act immediately. Criminal actors may use technical terms in an effort to appear legitimate and may have well-rehearsed responses to questions. Lastly, the criminal actor will typically request remote access or ask the operator to install an application, which gives them access to the computer. Once this happens, the criminal actor has access to all files on the computer including banking, social media and other personal information. This also gives them the opportunity to make fake error messages or alerts appear on your screen.[3] [4] [5]

Criminal actors may request payment using pre-paid gift cards or reloadable cash cards, wire transfers and even ask for credit card details after "fixing" your computer.[6] Additionally, they may use other tactics to request payment, such as:

- Attempting to enroll you in a computer maintenance or warranty program.
- Using professional-looking advertisements or directing you to spoofed websites to enter banking or other personal information.
- Requesting payment for fraudulent services they claim to provide.
- Attempting to sell services that are otherwise free.

Another tactic the criminal actor may use is installing malware on your computer through the applications they asked you to install

or granting themselves access to sensitive information such as names and passwords.[7] [8]

There are ways to avoid becoming a victim of this scam.

There are ways to avoid becoming a victim of this scam. First, keep in mind that legitimate tech companies will not contact you by phone, email or text message to tell you there is an issue with your computer. Security pop-up warnings from real tech companies will also never ask you to call a phone number. Never call the phone number provided, and if the criminal actor calls you, hang up or do not answer.[9] You should also avoid clicking on any unsolicited links because they may lead to illegitimate sites or download malware on your computer. Lastly, if you believe there is a problem with your device, update your security software and run a scan. If it turns out you need assistance with resolving a problem, find someone you know and trust to assist you, such as contacting the software company for specific applications or the store where you purchased your software, computer or other device.

[1] https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/tech-support-scams
[2] https://investor.nortonlifelock.com/About/Investors/press-releases/press-release-details/2021/Norton-Consumer-Cyber-Safety-Pulse-Report-Finds-Tech-Support-Scams-are-the-No.-1-Phishing-Threat/default.aspx
[3] https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/tech-support-scams
[4] https://support.microsoft.com/en-us/windows/protect-yourself-from-tech-support-scams-2ebf91bd-f94c-2a8a-e541-f5c800d18435
[5] Ibid.
[6] https://www.aarp.org/money/scams-fraud/info-2019/tech-support.html
[7] https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/tech-support-scams
[8] https://blogs.microsoft.com/on-the-issues/2021/07/21/tech-support-scams-adapt-2021-microsoft-study/
[9] https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

CYBER HIGHLIGHTS

The Least of Your Worries: Why We Need The Principle of Least Privilege

The principle of least privilege is a concept in information security that helps prevent cyber threat actors from compromising entire systems after a successful cyberattack.

Cyber actors are constantly developing new techniques to try to gain access to computer networks and information, which makes even the most secure networks vulnerable to cyberattacks. One way to mitigate the impact of a successful cyberattack is by implementing the principle of least privilege.[a] The principle of least privilege is a concept in information security that helps prevent cyber threat actors from compromising entire systems after a successful cyberattack. The principle can be traced back to 1975 and has been an important cybersecurity tenant for decades.[1] It operates similarly to the security principle of only sharing information with those who "need to know." It encourages organizations to limit user access or permissions to the minimum level necessary to reduce the risk of a cyberattack spreading throughout the network.[2]

Cybercriminals will use multiple attack vectors to attempt to compromise privileged accounts and steal their credentials. This includes deploying malware, phishing emails and sometimes capitalizing on insider actions (intentional or accidental) to get into networks.[3] Privileged accounts are often targeted in these attacks. Cybercriminals covet their credentials because they have high levels of access and can be used to access vital systems and deploy widespread ransomware or other viruses.

Most users only need limited permissions to perform their daily tasks, and limiting their network access to align with their responsibilities can help minimize the effects of an attack. For example, if one user is solely accessing a database for data entry, that user only needs permissions high enough to enter data. If that user's computer is infected with malware or is compromised in another way, the cybercriminal is limited to data entry as well. However, if that same employee had administrator permissions on their account, the attack could spread throughout the whole database.[4]

You can take steps to implement the principle of least privilege

in your IT environment by checking to see which users need administrator privileges to perform their duties and removing privileges from users who do not need them. It is also important that users with elevated privileges have another account with lower privileges for day-to-day use, only accessing the higher-level privileges when necessary. Additionally, some entities choose to implement a just-in-time access process that enables users to retrieve temporary credentials from a password vault when they need to access the system at a higher level of privilege. This will not only increase security, but also reduce IT service calls and help maintain user productivity. After implementing any or all of these practices, it is essential that you regularly audit your IT environment for unnecessary access and review user privileges. Remember to rescind privileges if they are no longer necessary.[5]

The principle of least privilege won't prevent cyberattacks, but it can help to mitigate the impact on your network.

The principle of least privilege won't prevent cyberattacks, but it can help to mitigate the impact on your network. By limiting the number of administrator privileges granted and minimizing the number of systems users have access to, it lowers the risk of a successful cyberattack spreading throughout the network. Individual users with elevated privileges can also do their part by following Secure Florida's Best Practices for Employees.

[a] Privilege provides the authorization to override, or bypass, certain security restraints, and may include permissions to perform actions such as configuring networks or systems, creating user accounts and installing software.

[1] https://web.mit.edu/Saltzer/www/publications/protection/Basic.html
[2] https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege
[3] https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam
[4] https://www.cyberark.com/what-is/least-privilege/
[5] https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance

All Things (or Factors) Considered, Is Your Account Safe from Being Taken Over?

While strong passwords are an important factor in making the authentication process more secure, organizations and individuals should consider using additional security methods for user verification when signing into accounts.

Is a password enough to keep your accounts secure? Cybersecurity professionals have reported that 99% of cyberattacks involve compromised passwords.[1] While strong passwords are an important factor in making the authentication[a] process more secure, organizations and individuals should consider using additional security methods for user verification when signing into accounts.[2] Multi-factor authentication (MFA) is an extra layer of security that can be used to prevent becoming a victim of cybercrime. MFA is becoming increasingly common on platforms, websites and devices and requires individuals to use at least two separate credential types when logging into accounts.

MFA credential verification types fall into three categories; something you know, something you have and something you are. To count as MFA, verification would have to come from at least two of the three categories.[3]

Examples of authentication credentials:

- **Something you know:** Passwords, pins or security question answers, etc.
- **Something you have:** Security tokens from an app, a verification code from an email or text message or a smart card, etc.
- **Something you are:** Biometrics such as voice, facial or fingerprint recognition, etc.[4]

Why should you use MFA? Cybercriminals are known to use passwords leaked from past data breaches to break into users' accounts. MFA can help mitigate against many different types of cyberattacks including phishing, credential stuffing[b] and brute force attacks. For example, cybercriminals may have access to the account owner's password, but they may not have the other sign-in credential required by MFA, such as a verification code sent to the account owner's cell phone through text messaging.[5] Unless they have access to the user's cell phone or the victim provides them with the code, they will not be able to get past the second step required to access the account.

There are multiple options for deploying MFA, and you can choose which method works best. For instance, you could use email codes, SMS or text messages or authenticator apps. It is important to note there are some potential risks with each method. Email

While MFA may not protect against all types of cyberattacks, it still offers an extra layer of data security and reduces the potential for a successful cyberattack.

accounts can be compromised through hacking methods, and SMS messages can potentially get intercepted by cybercriminals who trick wireless carriers into giving them access to your phone. Even with these risks, using any form of MFA is always more secure than using a password alone, and it requires minimal effort.[6] [7]

Individuals should set up MFA for their devices and accounts, when available. In addition to the methods mentioned above, there are also software and security devices that can be purchased for MFA, such as hardware tokens like smart cards. Biometric readers can also be used. Additionally, some companies offer software or apps that can be used by individuals for MFA.[8] Organizations should consider implementing MFA for all account users to ensure that data within the organization has an extra level of protection. Organizations can work with their IT or software providers to discuss available options and decide which best fit the organization. While MFA may not protect against all types of cyberattacks, it still offers an extra layer of data security and reduces the potential for a successful cyberattack.[9]

[a] Authentication is a process used to recognize the identity of a user.
[b] Credential stuffing is the automated use of collected usernames and passwords, usually from data breaches, to gain fraudulent access to user accounts.

[1] https://www.zdnet.com/article/multi-factor-authentication-use-it-for-all-the-people-that-access-your-network-all-the-time/
[2] https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661
[3] https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication
[4] https://www.fortinet.com/resources/cyberglossary/multi-factor-authentication
[5] https://its.ucsc.edu/mfa/cyber-attacks.html
[6] https://www.varonis.com/blog/two-factor-authentication/
[7] https://www.techrepublic.com/article/two-factor-authentication-cheat-sheet/
[8] https://www.inap.com/blog/mutifactor-works/
[9] https://its.ucsc.edu/mfa/cyber-attacks.html

DISPATCH HIGHLIGHTS

This section highlights articles from past issues of FIPC's *The Dispatch* that our analysts think are noteworthy based on trends we're seeing in Florida. *The Dispatch* is a list of open-source articles compiled for the law enforcement, cyber intelligence and information security communities that is sent out twice weekly. To sign up for the *The Dispatch*, visit SecureFlorida.org and click "**Get Connected**" at the top of the homepage or send an email to **FIPC@fdle.state.fl.us**.

RUSSIAN HACKERS REPORTEDLY HID BEHIND AMERICANS' HOME NETWORKS TO MASK THEIR CYBER ESPIONAGE

https://gizmodo.com/russian-hackers-reportedly-hid-behind-americans-home-ne-1847941076

- In 2021, Russian nation-state actors used a special technique to mask their IP addresses using American residential IP addresses.
- This technique allowed for the ability to launder their internet traffic through an unsuspecting home user and avoid appearing to originate from Eastern Europe.

Analyst Note: Russian nation-state actors continue to look for access points in U.S. networks using a variety of tactics. Organizations should take action to protect themselves from malicious activity. Tips can be found on Secure Florida's website.

IT'S ALREADY ATTACKED 'MINECRAFT': THE RACE IS ON TO FIX THE BIGGEST PC VULNERABILITY IN YEARS

https://mashable.com/article/log4shell-biggest-computer-vulnerability

- In December 2021, a flaw known as "Log4Shell" was discovered in a widely used open-source Java logging library typically found on Apache web servers.
- Some cybersecurity researchers have indicated this may be the most severe software vulnerability seen in the last 5 years.

Analyst Note: According to cybersecurity researchers, this flaw could be easily exploited by cybercriminals and affects many different products developed by several major software companies. Organizations should patch and protect any affected systems as soon as possible when severe vulnerabilities are identified.

EX-US INTEL OPERATIVES ADMIT HACKING AMERICAN NETWORKS FOR UAE

https://www.reuters.com/world/us/american-hacker-mercenaries-face-us-charges-work-uae-2021-09-14/

» Three former U.S. intelligence operatives reportedly admitted to hacking into American networks and illegally selling cyber intrusion technology to a foreign country.

Analyst Note: This case has prompted U.S. lawmakers to explore controls and reporting requirements for former U.S. intelligence employees seeking work overseas.

'CYBER EVENT' KNOCKS DAIRY GIANT SCHREIBER FOODS OFFLINE AMID INDUSTRY RANSOMWARE OUTBREAK

https://www.cyberscoop.com/schreiber-foods-cyber-event-ransomware-agriculture-food/

» A cyber incident forced a multibillion-dollar dairy company based in Wisconsin to shut down some of its plants and distribution centers.

» This event subsequently affected organizations with ties to producing and/or distributing several different dairy products.

Analyst Note: In 2021, the food and agriculture sector was significantly impacted by cyberattacks including a major meat supplier and two grain cooperatives.

CYBERCRIME COSTS VICTIMS $318B ANNUALLY

https://www.infosecurity-magazine.com/news/cybercrime-victims-318-billion/

» A research company analyzed cybercrime data reported by 67 countries worldwide from approximately 2018 to 2020.

» The countries that experienced the highest losses due to cybercrime were the United States ($28B), Brazil ($26B), the United Kingdom ($17.4B) and Russia ($15.2B).

Analyst Note: It is estimated that 71.1 million people fall victim to cybercrime each year. Users should ensure they continue to stay up-to-date on cybersecurity awareness practices to protect themselves at home and at work.

7 OF THE MOST IMPACTFUL CYBERSECURITY INCIDENTS OF 2021

https://www.darkreading.com/attacks-breaches/6-of-the-most-impactful-cybersecurity-incidents-of-2021?slide=1

» More vulnerabilities (approximately 18,439) were disclosed in 2021 than in any previous year-to-date.

Analyst Note: Organizations must remain vigilant when it comes to training their employees and continue to improve their cybersecurity defenses, including installing updates and patches as soon as they become available.

WHAT IS TLP?

The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colors to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s).

This *Beacon* is TLP: WHITE and is intended for wide distribution. If you would like to read past issues of the *The Beacon*, visit the Secure Florida website.

The following is from the United States Computer Emergency Readiness Team (US-CERT):

RED	Recipients may not share **TLP: RED** information with any parties outside of the specific exchange, meeting or conversation in which it is originally disclosed.
AMBER	Recipients may only share **TLP: AMBER** information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Recipients may share **TLP: GREEN** information with peers, partner organizations and with their sector or community, but not via publicly accessible channels.
WHITE	Recipients may share **TLP: WHITE** information without restriction, subject to copyright controls.

THE BEACON

ABOUT THE FIPC AND *THE BEACON*

The Florida Infrastructure Protection Center (FIPC) was established in 2002 to anticipate, prevent, react to and recover from acts of terrorism, sabotage, cybercrime and natural disasters.

The Beacon is the Florida Fusion Center's cyber and critical infrastructure publication, produced by the FIPC. Designed to highlight information of interest, *The Beacon* features events and trends that occur in Florida or specifically affect Florida.

This addresses DHS HSEC-SIN-1; FDLE SINs 1.1.1, 1.1.4, 1.1.6, 1.2.1, , 1.2.2, 1.8; and FFC-SINs 1.1, 1.2, 1.3, 1.5