SIM2K
Adapting Technology to Your Business Needs

9•21
Information you can use

SIMformation

Three “Don’t Do This” Security Tips

Using unsupported software, allowing the use of default usernames and passwords and using single-factor authentication for remote or administrative access to systems are all dangerous behaviours when it comes to cybersecurity and should be avoided by all organizations. The warning comes from the US Cybersecurity and Infrastructure Security Agency (CISA), which is developing a catalogue of “exceptionally risky” behaviors that can put critical infrastructure at extra risk of falling victim to cyberattacks.

Use of single-factor authentication – where users only need to enter a username and password – is the latest risky behavior to be added to the list, with CISA warning that single-factor authentication for remote or administrative access to systems supporting the operation of critical infrastructure “is dangerous and significantly elevates risk to national security.” Using multi-factor authentication can help disrupt over 99% of cyberattacks. For critical infrastructure, it’s therefore particularly important to have it applied in order to help prevent cyber criminals from tampering with cyber-physical systems.

Alongside single-factor authentication as a bad practice is the use of known, fixed or default passwords, which CISA describes as “dangerous.” Default or simple passwords are good for cyber criminals because there’s a much higher chance of them being able to simply guess passwords to compromise accounts. CISA also warns against the use of passwords that are known to have been breached previously, as that means they also provide cyber criminals with a simple means of gaining access to networks.

The third bad practice listed by CISA is the use of unsupported or end-of-life software in critical infrastructure. By using software or operating systems that no longer receive security updates, there’s the risk that cyber criminals could exploit newly discovered security vulnerabilities that emerge because old software often doesn't receive security patches.

“The presence of these bad practices in organizations that support critical infrastructure is exceptionally dangerous and increases risk to our critical infrastructure, on which we rely for national security, economic stability, and life, health, and safety of the public,” CISA said.

CISA’s list of dangerous bad practices is designed as advice for organizations involved in running or supporting critical infrastructure – but it’s also useful advice for businesses because avoiding the use of single-factor authentication, default passwords and unsupported software will also help protect them from falling victim to cyberattacks.

As recent incidents such as the ransomware attack at Eskenazi Health Services has demonstrated, cyberattacks against critical infrastructure can have significant impacts on the critical functions of government and the private sector. Now a month after this attack, the IT systems at Eskenazi and Marion County Health are finally back on line and people can access records through websites as well as make appointments. But for a month, these services were not available as Eskenazi sorted out the ransomware attack and, for a time, diverted patients away from the hospital “out of an abundance of caution” according to a spokesman.

Ransomware attacks are successful because many organizations can’t afford for their network to be out of service for a sustained period of time, so many businesses are still taking what they perceive to be the quickest and easier route to restoring the network by giving into the ransom demands of criminals. A recent report by cybersecurity company Digital Shadows examined which industries were most targeted by ransomware during 2020. Industrial goods and services was the most targeted, accounting for 29% – or almost one in three – ransomware attacks. That number of attacks is more than those on the next three most targeted sectors – construction, technology and retail – combined.

Manufacturers and infrastructure can make a tempting targeted for ransomware attacks because the organizations in these sectors need to be in operation around the clock, whether that’s running a factory production line or operating a utilities plant. If they can’t provide these services, there can be wide-ranging impacts further down the supply chain.

All organizations should implement an effective cybersecurity program to protect against cyber threats and manage cyber risk. SIM2K is here to help you with your defenses against cyber threats. All three of these “don’t do it” items on the CISA list are some of the first things we can do for your company. We can implement Multi-factor Authentication for your network access, be it for remote access, e-mail access or however is needed. We also provide our Critical Update Service where we will review your current software and update it for you, ensuring you are up-to-date with the relevant patches and security. And, finally, we can review your passwords protocol and make recommendations and set up a schema for employees to follow to encourage use of more complex passwords.

Cyber security is a constantly-evolving field as new threats emerge and new defenses are brought on-line. SIM2K is always watching the developments in this area, and we add new products and services that we feel will best serve you and your security needs. Please call us for more information on how we can help you with protecting your network.

Move to the Cloud, they said...

Move to the Cloud was the pitch being made to companies as it is designed to offer better security than your own server. But now, Microsoft has warned thousands of its Azure cloud computing customers, including many Fortune 500 companies, about a vulnerability that left their data completely exposed for the last two years.

A flaw in Microsoft's Azure Cosmos DB database product left more than 3,300 Azure customers open to complete unrestricted access by attackers. The vulnerability was introduced in 2019 when Microsoft added a data visualization feature called Jupyter Notebook to Cosmos DB. The feature was turned on by default for all Cosmos DBs in February 2021.

A listing of Azure Cosmos DB clients includes companies like Coca-Cola, Liberty Mutual Insurance, ExxonMobil, and Walgreens, to name just a few.

"This is the worst cloud vulnerability you can imagine," said a Wiz spokesman, the security company that discovered the issue. "This is the central database of Azure, and we were able to get access to any customer database that we wanted."

Despite the severity and risk presented, Microsoft hasn't seen any evidence of the vulnerability leading to illicit data access. "There is no evidence of this technique being exploited by malicious actors," Microsoft has said. "We are not aware of any customer data being accessed because of this vulnerability." Microsoft paid Wiz $40,000 for the discovery, according to Reuters. In an update posted to the Microsoft Security Response Center, the company said its forensic investigation included looking through logs to find any current activity or similar events in the past. "Our investigation shows no unauthorized access other than the researcher activity," said Microsoft.

In a detailed blog post, Wiz says that the vulnerability introduced by Jupyter Notebook allowed the company's researchers to gain access to the primary keys that secured the Cosmos DB databases for Microsoft customers. With said keys, Wiz had full read / write / delete access to the data of several thousand Microsoft Azure customers.

Wiz says that it discovered the issue two weeks ago and Microsoft disabled the vulnerability within 48 hours of Wiz reporting it. However, Microsoft can't change its customers' primary access keys, which is why the company emailed Cosmos DB customers to manually change their keys in order to mitigate exposure.

Today's issue is just the latest security nightmare for Microsoft. The company had some of its source code stolen by SolarWinds hackers at the end of December, its Exchange e-mail servers were breached and implicated in ransomware attacks in March, and a recent printer flaw allowed attackers to take over computers with system-level privileges. But with the world's data increasingly moving to centralized cloud services like Azure, today's revelation could be the most troubling development yet for Microsoft.

This just points out that no solution is 100% safe, which is why companies must keep a wary eye on how their sensitive data is stored and accessed. SIM2K can help you assess your protocols and make recommendations for improved security.

Government Acts on Cybersecurity

The heads of Apple, Google, Amazon, Microsoft and IBM are among the business leaders that met with President Joe Biden at the White House to discuss how the government and private sector can work together to improve the nation's cybersecurity, according to a senior administration official.

"Most of our critical infrastructure is owned and operated by the private sector, and the federal government can't meet this challenge alone," Biden said during a brief comment at the start of the meeting. "I've invited you all here today because you have the power, the capacity and the responsibility, I believe, to raise the bar on cybersecurity."

The government and business leaders made announcements in key areas that build on the administration's efforts to shore up the nation's cybersecurity. The tech CEOs also met with members of Biden's cabinet to look at ways to build more-enduring cybersecurity, while other executives will focus on critical infrastructure and the cybersecurity workforce.

In a press release, the White House said the National Institute of Standards and Technology "will collaborate with industry and other partners to develop a new framework to improve the security and integrity of the technology supply chain." Microsoft, Google and IBM are among the companies who have pledged to participate in the initiative.

At the meeting, Google CEO Sundar Pichai announced the search giant will invest more than $10 billion over the next five years in cybersecurity. The effort will include helping to secure the supply chain and strengthening open-source security. The investment will also expand "zero-trust" programs, in which organizations don't automatically trust any person or device when it comes to cybersecurity.

IBM also made a handful of announcements at the meeting. The company will train more than 150,000 people in cybersecurity skills over the next three years, CEO Arvind Krishna said in a post on LinkedIn. Krishna also called for establishing voluntary public reporting standards on cybersecurity practices.

At the same time, the bi-partisan Cyberspace Solarium Commission is calling for wide-ranging cybersecurity changes, including government reforms and better collaboration with the private sector. "A major cyberattack on the nation's critical infrastructure and economic system would create chaos and lasting damage exceeding that wreaked by fires in California, floods in the Midwest, and hurricanes in the Southeast," said organization's co-chairmen, Sen. Angus King of Maine and Rep. Mike Gallagher of Wisconsin. The solution is to deter more attacks to begin with, the lawmakers said. That means encouraging better norms around the world, taking away easy targets in US infrastructure, and finding new ways to retaliate against hacks. Among the recommendations are establishing a National Cyber Director and that Congress should pass a national data security and privacy protection law.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

New Attacks Detected

A new spear-phishing campaign is attempting to infect PCs with Trickbot, one of the most prevalent and potent forms of malware around today, a joint advisory from the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) has warned.

Trickbot started life as a banking trojan but has become one of the most powerful tools available to cyber criminals, who are able to lease out access to infected machines in order to deliver their own malware – including ransomware.
Now its authors are using a new tactic to attempt to deliver it to victims, warns the joint FBI and CISA alert – phishing e-mails that claim to contain proof of a traffic violation, scaring them into opening the e-mail. The malicious e-mail contains a link that sends users to a website hosted on a server compromised by the attackers that tells the victim to click on a photo to see proof. When they click the photo, they actually download a JavaScript file that, when opened, connects to a command and control server that will download Trickbot onto their system.

Trickbot creates a backdoor onto Windows machines, allowing the attackers to steal sensitive information including login credentials, while some versions of Trickbot are capable of spreading across entire networks.

A coalition of cybersecurity companies attempted to disrupt Trickbot in October last year, but the malware didn't stay quiet for long, with its cyber-criminal authors quickly able to resume their operations. “To completely remove Trickbot from the landscape would be extremely difficult and likely require a coordinated international law enforcement effort like we saw with Emotet. In fact, after the actions of October 2020, we saw Trickbot campaigns resume within weeks, and it has been active continually since,” said a security expert.

Trickbot remains a powerful tool for cyber criminals and a clear danger for enterprises and organizations of all sizes – but there are measures recommended by CISA and the FBI that can be taken in order help protect networks from the malware.

Providing social-engineering and phishing e-mail training to employees can help them to avoid threats by being wary of certain types of messages. Organizations should also be implementing a proper cybersecurity programs with a formalized security patch management process, so cyberattacks can’t exploit known vulnerabilities to gain a foothold on the network. It is also recommended that multi-factor authentication is applied across the enterprise, so malware that steals login credentials to move across the network can't do so as easily.

These are all steps that SIM2K will implement for your company. We provide training and security like MFA, so call us for help.

“Random Tid-Bytes”

Fortinet Logins Leaked

A threat actor has leaked a list of almost 500,000 Fortinet VPN login names and passwords that were allegedly scraped from exploitable devices last summer. While the threat actor states that the exploited Fortinet vulnerability has since been patched, they claim that many VPN credentials are still valid. This leak is a serious incident as the VPN credentials could allow threat actors to access a network to perform data exfiltration, install malware, and perform ransomware attacks. The list of Fortinet credentials was leaked for free by a threat actor known as “Orange,” who is the administrator of the newly launched RAMP hacking forum and a previous operator of the Babuk Ransomware operation. An analysis of this file shows that it contains VPN credentials for 498,908 users over 12,856 devices worldwide, with 2,959 devices located in the USA. It is unclear why the threat actor released the credentials rather than using them for themselves, but it is believed to have been done to promote the RAMP hacking forum and the Groove ransomware-as-a-service operation.

Windows 11 Release Date Confirmed

Microsoft says that it expects to begin shipping Windows 11 on Oct. 5 for new and existing PCs. The update will roll out in a measured and phased approach and will only be offered on existing PCs if they are eligible by meeting Windows 11’s system requirements. Windows 11 features a set of new system requirements that Microsoft has set to ensure all Windows 11 PCs are performing optimally in both security and stability departments. The minimum system requirements are as follows:

- A modern 1GHz 64-bit dual-core processor
- 4GB RAM
- 64GB drive
- 9-inch display
- 1366x768 resolution
- UEFI, Secure Boot & TPM 2.0 compatible
- DirectX 12 compatible graphics/WWDM 2.x

One of the biggest changes to the system requirements with Windows 11 is that the OS is now only available on 64-bit processors. Microsoft is not releasing a 32-bit version of the OS, although 32-bit apps will continue to work just fine. Microsoft is also limiting officially supported Windows 11 PCs to those on Intel 8th-generation (or equivalent) and above. This means if you have a CPU older than 8th Gen Intel, you likely won’t be able to officially run Windows 11 when it is released later this year.

Apple Backs Off Monitoring

In a surprise announcement, Apple said it will take more time to improve its controversial child safety tools before it introduces them. The company says it plans to get more feedback and improve the system, which had three key components: iCloud photos scanning for CSAM (Child Sexual Abuse Materials), on-device message scanning to protect kids, and search suggestions designed to protect children. Ever since Apple announced the tools, it has faced a barrage of criticism from concerned individuals and rights groups from across the world. The big argument the company seemed to have a problem addressing seems to have been the potential for repressive governments to force Apple to monitor for more than CSAM. Critics said these tools could be exploited or extended to support censorship of ideas or otherwise threaten free thought.

On-Line Privacy – Does it Even Exist?

Back in 1999, Scott McNealy of Sun Microsystems said, "You have zero privacy anyway. Get over it," Despite the hue and cry his remarks caused, he's been proven largely correct. Cookies, beacons, digital signatures, trackers, and other technologies on websites and in apps let advertisers, businesses, governments, and even criminals build a profile about what you do, who you know, and who you are at very intimate levels of detail.

The technology to monitor everything you do has only gotten better. And there are many new ways to monitor you: always-listening agents like Amazon Alexa and Apple Siri, Bluetooth beacons in smartphones, cross-device syncing of browsers to provide a full picture of your activities from every device you use, and of course social media platforms like Facebook that are designed for you to share everything about yourself and your connections so you can be monetized.

When speaking of online privacy, it's important to understand what is typically tracked. Most websites and services don't actually know it's you at their site, just a browser associated with a lot of characteristics that can then be turned into a profile. Marketers and advertisers are looking for certain kinds of people, and they use profiles to do so. For that need, they don't care who the person actually is. Neither do criminals and organizations seeking to commit fraud.

When companies do want that personal information – your name, gender, age, address, phone number, company, titles, and more – they will have you sign up. They can then correlate all the data they have from your devices to you specifically, and use that to target you individually. That's common for business-oriented websites whose advertisers want to reach specific people with purchasing power.

The browser has been the focal point of self-protection online, with options to block cookies, purge your browsing history or not record it in the first place, and turn off ad tracking. But these are fairly weak tools, easily bypassed. For example, the incognito or private browsing mode that turns off browser history on your local computer doesn't stop Google, your IT department, or your internet service provider from knowing what sites you visited; it just keeps someone else with access to your computer from looking that history on your browser.

The "Do Not Track" ad settings in browsers are largely ignored. And blocking cookies doesn't stop Google, Facebook, and others from monitoring your behavior through other means such as looking at your unique device identifier and noting if you sign in to any of their services – and then linking your devices through that common sign-in.

Because the browser is a main access point to internet services that track you (apps are the other), the browser is where you have the most centralized controls. Here is a ranking of mainstream desktop browsers in order of privacy support, from most to least – assuming you use their privacy settings to the max.

- Apple Safari
- Microsoft Edge
- Mozilla Firefox
- Google Chrome

Safari and Edge offer different sets of privacy protections, so depending on which privacy aspects concern you the most, you may view Edge as the better choice for the Mac, and of course Safari isn't an option in Windows, so Edge wins there. Chrome should be avoided if privacy matters to you.

So what can you do to maximize your safety? In your browser's privacy settings, be sure to do the following:
Turn on the Do Not Track Although it is often ignored, turn it on it for those sites that do honor it.
Block third-party cookies. To deliver functionality, a site legitimately uses first-party (its own) cookies, but third-party cookies belong to other entities (mainly advertisers) who are likely tracking you in ways you don't want. Don't block all cookies, as that will cause many sites to not work correctly.
Set the default permissions for websites to access the camera, location, microphone, content blockers, auto-play, downloads, pop-up windows, and notifications to at least Ask, if not Off.
Turn off trackers. If your browser doesn't let you do that, switch to one that does, since trackers are becoming the preferred way to monitor users over old techniques like cookies. Plus, blocking trackers is less likely to render websites only partially functional, as using a content blocker often does.

Additionally, take these precautions when browsing:
Use DuckDuckGo as your default search engine, because it is more private than Google or Bing. You can always go to google.com or bing.com if needed.
Don't use Gmail in your browser (at mail.google.com). Once you sign into any Google service, Google tracks your activities across every other Google service, even if you didn't sign into the others. If you must use Gmail, do so in an e-mail app like Microsoft Outlook or Apple Mail, where Google's data collection is limited to just your e-mail.
Never use an account from Google, Facebook, or another social service to sign into other sites; create your own account instead. Using those services as a convenient sign-in service also grants them access to your personal data from the sites you sign into.
Don't sign in to Google, Microsoft, Facebook, etc. accounts from multiple browsers, so you're not helping those companies build a fuller profile of your actions. If you must sign in for syncing purposes, consider using different browsers for different activities, such as Firefox for personal use and Chrome for business.

Some other tips:

- Don't use Social Networks, and if you do, share as little as you can;
- Don't use voice assistants like Alexa or Siri – they too build a profile of your interactions that can help identify you on-line;
- Turn off location services for all apps that truly don't require knowing where you are;
- Don't sign in for on-line stores when just researching, only sign in when purchasing;
- Review all you privacy setting on all devices, including smartphones, tablets, voice assistants as well as PCs.

Protecting your personal information and browsing habits on-line will help shield you from malicious activity up to a point, but it will take your in-depth involvement to secure your data. Call SIM2K for help in maximizing your privacy profile on-line.