SIM2K
Adapting Technology to Your Business Needs

March, 2023
Information you can use

SIMformation

SMBs Need Cybersecurity Awareness

The *Indianapolis Business Journal* recently posted this article from Michael Caliendo, a tech industry insider. There is considerable technological debt here. Small businesses feel they are not important enough to warrant an attack, yet that mindset is exactly what the threat actors are counting on. So SIM2K wanted to share his thoughts as we agree with his views on cybersecurity.

Small and medium-size businesses are the engines of economic prosperity on both a local and national level. According to a 2019 report from the U.S. Small Business Administration, these businesses generate 44% of U.S. economic activity. In Indiana, there are nearly 530,000 small businesses, which represent 99.4% of Indiana businesses. Battling back from the impact of the global pandemic, small businesses are now dealing with the added challenge of how to shore up cybersecurity.

In a 2021 survey of small-business owners, CNBC found that more than half were not concerned about being the victim of a cyberattack. The reality is, such businesses are at considerable risk of cyberattacks like phishing efforts, malware and ransomware. The government's Cyberstructure & Infrastructure Security Agency reported that, in 2021, 70% of ransomware attacks were levied against businesses with fewer than 500 employees.

Small businesses are ripe targets for a number of reasons: They frequently lack the level of protection large businesses have, they are gateways to attack larger companies (through supply chain access), and they deal in valuable personal data. While it might seem a daunting task, growing businesses would be wise to protect themselves now and take advantage of the same kinds of resources growing enterprises use.

Small businesses are not only more vulnerable to cyberattack, they are also likely less equipped to withstand the impact of an event. According to IBM's latest data, the average cost of a data breach to a business under 500 employees is up to $2.74 million. Even smaller incidents have a dramatic effect on the bottom line, incurring lost revenue and damaging customer trust and repeat business.

Today, a small or midsize business that has worked tirelessly and methodically to grow – by expanding its employee base, its geographic footprint, its technology capabilities and more – could be devastated by a single cybersecurity incident. But finding solutions is no easy task. Many small businesses do not have substantive in-house tech expertise, and finding security experts for hire is growing increasingly difficult as the industry experiences a cybersecurity talent shortage.

Increasingly complex networks and cloud operations render entry-level solutions like simple software, or even some outsourced tech support, insufficient to protect a burgeoning enterprise. And cost is always a crucial factor for small businesses that frequently maintain slim margins as they grow.

In better news, basic best practices are not costly, and more advanced cybersecurity resources are no longer one-size-fits-all solutions crafted for larger enterprises. A few immediate steps small and medium enterprises can take to fortify defenses include: making sure all software is up to date, conducting regular security trainings for employees to enhance their awareness of risks, establishing a virtual private network (VPN) and requiring two-factor authentication and regular password changes.

For a more thorough cybersecurity solution, hiring a third-party service provider is a smart choice. Aware of the increasing risk to businesses, reputable managed security services providers now offer solutions tailored specifically with the needs and budget of smaller enterprises in mind.

A security service provides 24-hour-a-day support, seven days a week, with a team of security professionals who are up to date on the latest threats and mitigations. They will ensure a network is optimized for security, monitor the network for potential problems, and spring into action to address security threats or breaches to minimize harm. They can also automate compliance and reporting functions, such as PCI (credit card transaction security) or HIPPA (patient information security).

The right security service, experienced in serving large, distributed enterprises, has great depth of talent and expertise and can also provide the affordable, flexible, scalable solutions smaller enterprises prefer. Some providers even bundle backup connectivity with ongoing security so that businesses will always have a strong connection to access cloud-based applications and preserve the ability to process transactions.

At any time, as business and network requirements grow, a security service can advise and adapt a cybersecurity solution to fit the business needs. A partnership with a security service eliminates the pressure to hire internal cybersecurity talent and allows businesses to focus on the growth and transformation of their enterprise with peace of mind. The threat of cyberattack is real for businesses large and small alike. But the cybersecurity industry is evolving as well. With solutions geared to businesses of all sizes, a security service can serve as a personal cybersecurity SWAT team to eradicate threats before they exact a painful cost.

SIM2K works to fill this cybersecurity void for our SMB clients. We offer security solutions, backups and technical expertise to adapt the various tools to best fit your company's security needs. And we are constantly evaluating new techniques and products to add to our cybersecurity menu to help stay ahead of this changing security landscape. Call us for more information so we can help boost your cybersecurity profile.

Apple to Move to USB-C?

Apple appears ready to replace Lightning ports and cables with USB-C in the iPhone 15, and when it does it will introduce a Made For iPhone (MFi) scheme for such products. The idea is that consumers will be able to purchase cables and other devices in full confidence that they will be compatible with their iPhone. At the same time, Apple is poised to make it more difficult to use cheap USB-C cables with its devices, and while it may well make a few dollars more from the purported plan, there are also good reasons to put the system in place.

According to some reports, the downside is that USB-C devices that aren't licensed under the MFi scheme may end up being penalized — they might not work at all, may only support a limited charging speed, and could be unable to share data. Apple critics will, no doubt, attack the company for greed, as MFi scheme members must pay for the privilege of the licensed status. That's going to mean iPhone users won't be able to use just any USB-C cable, and the ones they do get to use may cost more.

But it is not just greed driving this decision. It's the need to secure a user's iPhone and everything it contains. It also follows several attacks in which key industries have been targeted and systems infected using USB-C. Given Apple's commitment to secure the supply chain, this is a problem that needs to be resolved. The move may also reflect cross-industry preparations to bring the company in line with the EU Cyber Resilience Act, which will demand manufacturers take steps to secure all manner of electronic products before they're sold.

One big limitation of USB-C is that the cables themselves can be compromised and used to steal data from devices, and such attacks can be carried out by anyone with physical possession of your device. Malicious cables might contain GPS trackers, make calls, or steal user names, passwords and data from connected devices while turning the device into an entry route into the wider enterprise network.

There are increasing reports of USB attacks against key infrastructure providers in early 2022 — targets were tricked into connecting malware-laden USB drives to their machines — shows the lengths some take to penetrate enterprise endpoints. Other attacks exploit public USB-C access points; think what could happen if hackers had control of the USB-C slot you connect your iPhone to during an airport stopover — the damage might be done before you even touch down.

One reason computers are vulnerable to such attacks is that USB-C doesn't have a mandatory authentication system. The USB Implementer's Forum (on which Apple sits) does offer a voluntary authentication protocol for USB-C chargers, cables, devices, and power sources that will detect unfamiliar cables and verify the device is certified. But not everyone uses this.

However, in the context of national security and with the knowledge that USB cables are being actively exploited to engage in attacks against national infrastructure, it makes sense to ensure the USB-C devices connected to your iPhones aren't going to steal your digital existence, even if they cost a few dollars more.

So while Lightning cables may be on the way out, you won't be able to just pick up a new USB-C at the checkout counter at Walmart and expect it to work on your iPhone. But it is for your security and the protection of your network data.

AI Invades Microsoft's World

As part of the lastest Windows 11 feature update from Microsoft, users will be able to access the company's new AI-powered Bing directly from the taskbar. In a blog post announcing the update, said "the search box is one of the most widely used features on Windows" and therefore combining it with the new AI-powered Bing will empower users "to find the answers [they're] looking for, faster than ever before."

In order to access this new search box, users who are in the Bing preview will need to install the latest Windows 11 update. However, those who do not currently have access to the preview will need to sign up to the wait list.

Bing Chat allows users to ask questions and receive answers from GPT-4, the latest version of the artificial intelligence (AI) language model built by research lab OpenAI. However, while it has only been available to the public since February 7, a number of interactions with the chatbot have already made headlines, with the chatbot even professing its love to one New York Times reporter and telling him he should get a divorce.

Earlier this month, Microsoft also updated its Edge browser with AI capabilities and two new functionalities: chat and compose. As a result, users can, for example, ask for a summary of a lengthy financial report, and then use the chat function to ask for a comparison with a competing company's financials.

A user can also ask Edge to help compose content, such as a LinkedIn post, by giving it a few prompts to get started. The ethics of AI-generated content are already being hotly debated, with the education nonprofit institution International Baccalaureate deciding this week that students can quote Chat GPT in their essays, as long as they cite the technology in the same way they would any other source and not try to pass the content off as their own.

The company plans to embed generative AI into most of its products and services, ranging from Windows to Office apps to cloud services and possibly beyond. Microsoft touted the chatbot's ability to provide more complete answers, refine search queries, provide actionable results, and provide a "creative spark" for content creation.

Keep in mind that generative AI is still in its infancy. The Bing chatbot does show real promise – capable of summarizing information clearly and succinctly and knowing how to ask the right follow-up questions. And as the chatbot continues to be trained, its answers will likely become more helpful. Microsoft may eventually allow companies to train the chatbot on their own data sources. In that case, it could be remarkably useful, because the information it mines will be precisely the information companies find useful.

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.

Last Pass at LastPass

We have been covering the issues involving password manager company LastPass over the past few issues of SIMformation, and how this presented a danger for any customer. Now, LastPass has revealed that hackers stole a master password that they used to access highly restricted corporate databases and information by targeting a senior engineer's home computer.

The password manager company first revealed that it had been hacked in August last year when it said attackers had accessed the development environment, taking portions of LastPass source code and some proprietary technical information.

At the time, LastPass said there was no evidence that the attackers gained access to customer data or sensitive encrypted vaults. But this changed last December, when LastPass revealed hackers had stolen vault data containing both encrypted and unencrypted data – including information about customers. The company has now said attackers used information stolen during the first attack – along with information stolen in other breaches and the exploitation of a cybersecurity vulnerability – to power a second attack.

This attack targeted one of only four senior DevOps engineers who had the required high-level security authentication necessary to use the decryption keys required to access the cloud storage service – and the attackers did so by targeting their home computer. The exact details of how the attack happened haven't been disclosed, but LastPass said the DevOps engineer's home computer was targeted by attackers exploiting what's described as "a vulnerable third-party media software package", which let the attackers gain the privileges required for remote code execution.

This tactic gave attackers the opportunity to install keylogger malware on the home computer, allowing them to monitor what the employee typed on their machine. They exploited this information to steal the master password to gain access to the corporate vault. According to LastPass, this access allowed the attackers to enter various shared instances, "which contained encrypted secure notes with access and decryption keys needed to access the AWS S3 LastPass production backups, other cloud-based storage resources, and some related critical database backups". Following the incident, LastPass says it "assisted the DevOps Engineer with hardening the security of their home network and personal resources".

LastPass has upgraded its multi-factor authentication (MFA) by applying Microsoft's conditional access PIN-matching MFA, and the company is now rotating critical and high-privilege passwords that were known to the attackers, to reduce the chance of an additional breach. The company is also examining how the breach has potentially affected customers. "There are several additional workstreams underway to help secure our customers, which may require them to perform specific actions," Lastpass said.

It is recommended that LastPass users change their master password. This password should not be used to secure any other accounts. It is also recommended that MFA is applied to the account to reduce the chances of it being accessed.

This also points out how security must extend to any work from home setting. Anyone doing company work from a home computer must be as diligent about security as if they were in the office. SIM2K can help with assessments for remote worker security.

"Random Tid-Bytes"

Important Update for Zultys SMS Users

Our unified communications partner, Zultys, has notified SIM2K that new 10DLC registration requirements and rules require that customers who send SMS messages through Zultys register with The Campaign Registry (TCR) by March 31 and provide a dedicated phone number to send SMS messages from. As part of our Unified Communications offering, Zultys previously provided some users with temporary phone numbers to send and receive SMS messages without the need for a dedicated phone number. But due to these new registration requirements imposed by mobile carriers, Zultys can no longer provide temporary phone numbers to users who do not have a dedicated number. Customers utilizing temporary phone numbers will need to order and assign dedicated phone numbers to each user who wishes to send and receive SMS messages by May 1. If this is not done, SMS messages will not be delivered after May 1. Zultys ZCS customers can order dedicated phone numbers through the company's portal at mxvirtual.com. Non-ZCS customers can order dedicated numbers through their carrier and port them to Zultys by submitting a Letter of Authorization (LOA) and proof of ownership. Zultys has sent out letters notifying customers who need to complete the Campaign Registry requirement, so please act by March 31. If you have any questions or concerns about this requirement or the TCR requirement deadline on March 31, please contact SIM2K.

Twitter Changes 2FA

Twitter is making some dramatic changes to its currently available security settings. Beginning March 19, users of Twitter won't be able to use SMS-based two-factor authentication (2FA) unless they have a subscription to the paid Twitter Blue service. If you use text-based 2FA, the important thing here is not to worry. You may be under the impression that Twitter is removing your 2FA ability altogether, but this isn't the case. There are alternatives, and they're quite a bit more robust than the SMS approach. In fact, they're referenced by Twitter repeatedly in the documentation regarding the removal of the text service for free Twitter users. This move is being blamed on fraudulent bot behavior in relation to the Twitter platform. From a Twitter blog post: "While historically a popular form of 2FA, unfortunately we have seen phone-number based 2FA be used - and abused - by bad actors. So starting today, we will no longer allow accounts to enroll in the text message/SMS method of 2FA unless they are Twitter Blue subscribers. The availability of text message 2FA for Twitter Blue may vary by country and carrier." Twitter has information on options that non-Blue subscribers may use to add 2FA to their free accounts such as an authenticator app.

Four-Day Workweek?

The world's largest trial of a four-day week has ended and 92% of the companies that participated plan to continue with the shortened work schedule because the benefits were clear. After the trial, 56 of 61 companies are continuing with their four-day week. Only two companies said they are "definitely not" doing so, while others three expect to continue, but have not confirmed it. "Some of the most extensive benefits of shorter working hours were found in employees' well-being," the study concluded. "Before and after data shows that 39% of employees were less stressed, and 71% had reduced levels of burnout at the end of the trial. Likewise, levels of anxiety, fatigue, and sleep issues decreased, while mental and physical health both improved." Women especially benefitted from the 4 day schedule. Something to consider??? Who knows.

Service Outages Show Dark Side of the Cloud

The benefits of the cloud are undeniable and include improved functionality, security, efficiency, and stability. In today's always-on, instant-everything world, it's hard to argue against using the cloud. But the cloud, and cloud providers, are not infallible.

Multiple Oracle Cloud Infrastructure (OCI) outages have hit users around the world recently, and coming after interruptions in Microsofts cloud services in February, are a reminder of the importance of site engineering for systems administrators whose businesses rely on cloud-based mission critical applications. The biggest OCI outage lasted for almost two full days, impacting customers across North and South America, Australia, Asia Pacific, Middle East, Europe and Africa.

Oracle said that the outage caused a variety of problems for customers. OCI customers using OCI Vault, API Gateway, Oracle Digital Assistant, and OCI Search with OpenSearch, for example, may have received 5xx-type error or failures (which are associated with server problems), Oracle said. Identity customers may have experienced issues when creating and modifying new domains.

In addition, Oracle Management Cloud customers may have been unable to create new instances or delete existing instances, Oracle said. Oracle Analytics Cloud, Oracle Integration Cloud, Oracle Visual Builder Studio, and Oracle Content Management customers may have encountered failures when creating new instances.

In an apparently unrelated incident, Oracle's NetSuite ERP suite suffered an outage at its data center in Boston at the same time, leading to downtime that stretched for nearly 24 hours.

Oracle did not detail reasons for the Boston data center outage, but media stated that "smoke was reported at a data center site used by Oracle NetSuite, coming from electrical equipment in a power room." Firefighters turned off power to the site and evacuated it, the Register reported.

Customers reported that they were unable to recover data that been recorded for a half hour before the outage began, with one user posting a statement said to have been sent by NetSuite, confirming that the "restoration point was about 30 minutes prior to the outage." The statement noted that in such cases, NetSuite typically provides users with a report or list of transactions that were created during the period for which data could not be retrieved by customers.

The user who posted the NetSuite statement said that "based on this, we're assuming we'll have to manually slog through the missing data and then selectively import it into our 'new' NetSuite instance (which is now hosted in Santa Clara, not Boston)."

In yet another separate incident, Oracle's US Ashburn 2 data center experienced an outage for about an hour.

Oracle claims that NetSuite had 99.96% availability over the past 12 months, and the outages this week come just months after Oracle CEO Larry Ellison, in the company's second quarter earnings call in December, indirectly took a dig at Amazon Web Services, which suffered a major outage that month. Ellison said that a major telecom company told him that Oracle is different from other clouds as it "never ever goes down," CNBC reported.

Over the last few months there have been other major cloud outages. Most recently, on February 7, Microsoft Outlook and Teams suffered a global outage. That outage came two weeks after a Microsoft outage in January that affected not only Outlook and Teams, but services including Exchange Online, SharePoint Online and OneDrive for Business. The outages impacted users around the world.

Although the cloud giants have redundant data centers and servers in almost every region, data loss has been commonplace for many outages. "Cloud based solutions, like their on-premise equivalents, need to be architected for true high availability and continuity," said an analyst at market research firm Forrester. "Having a cloud foundation and a global footprint does not immediately give you 100% uptime for an application. Especially for applications with a long on-premise history and heritage."

The Forrester analyst added that other factors that lead to outages include client choices, such as data residency configurations that may constrain how much data replication and backup a cloud provider can implement on its data center network.

"Add this to increasingly global network complexity, the risk of multiple factors – some human error – and you have a perfect storm in terms of an outage with real data loss potential. It's this risk that has driven uptake of site reliability engineering," Forrester concluded.

Site reliability engineering (SRE) is the practice of maintaining that programmable infrastructure and maximizing the availability of the workloads that run on it. At a base level, SREs bring software engineering principles to infrastructure and operations problems, with the goal of creating highly scalable and reliable systems. A SRE function will typically be measured on a set of key reliability metrics, namely: system performance, availability, latency, efficiency, monitoring, capacity planning and emergency response.

So these outages provide the caution to anyone looking to move critical functions to the Cloud. When cloud services stop working, everyone panics, and with good reason. Many businesses depend on constant access to their cloud-based mission-critical products and services, so cloud downtime can stop work in its tracks. In the best-case scenario, downtime lasts only a few minutes and affects a few minor services; in the worst case, businesses are paralyzed for half a day or even longer, and the effects can be highly detrimental.

Outages are a reality that technology-dependent companies should plan for in advance. In general, you can trust that reputable cloud service providers have put huge amounts of money into ensuring uptime, while also acknowledging the fact that outages can and will happen. To limit the impact cloud outages can have on your operations and finances, you can place your cloud services in one of the more stable regions, use redundancy measures, or transfer your risk by purchasing insurance coverage, or employ a combination of all three methods. Whatever you decide to do, don't neglect this issue because the damages can be significant to both your business continuity and your reputation.

The rise of "Software as a Service" and use of hosted applications all relate back to the Cloud, so businesses need to be aware that the Cloud is not just something for large enterprise companies or data storage use. There are many touchpoints for the Cloud in today's IT environment. SIM2K can help you identify where your technology may intersect with the Cloud, what the +/- of this may be, and strategies to protect your critical functions from outages such as we have been seeing recently. Call us for more information.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com