SIM2K
Adapting Technology to Your Business Needs

12•20
Information you can use

SIMformation

Happy Holidays from SIM2K

From all of us at SIM2K, we would like to wish you the best of the Season. Technology continues to march forward at a rapid pace and is taking on new approaches as the pandemic has made a shift of work habits into more "work at home" situations, requiring new security steps, VPNs and enhanced bandwidth. Cloud-based applications are seeing growth, too, to support the distributed workforce. Scammers are taking advantage of these unsettled times and ramping up ransomware attacks on major institutions across the world. SIM2K continues to add to our product lines in 2FA (two-factor authentication), Wi-Fi, security cameras, VOIP Phones as well as our long-time world class support as our team masters the latest in technology. As we say every year, we do appreciate the loyalty of our clients and strive to continue to be your IT provider. We look forward to serving you in the year ahead!

Ben FRED Christy Nick Chris Scott MELISSA

In memoriam - Mark Finegan

Pandemic-Inspired Trends for 2021

The events of 2020 are making the technology world re-think some ways of doing business, focusing more now on those relegated to "at-home" work rather than the traditional office environment. Here are three trends that should take off in 2021:

Branded office bundles

One problem with the rush to work and study from home is that support organizations have been hammered by problems resulting from that lack of consistency. To address this problem, vendors are putting together bundles that – at a minimum – include a router (where many support problems originate) to meet company standards regarding security, management, and reliability. Other than that, it isn't yet clear what the bundles might contain and whether they will be packaged together (more likely from an online vendor than in a store) or connected by brand, so employees can build their bundle from approved parts. (The latter would more likely be in-store.)

WAN-connected laptops

This is something likely to be a parallel effort to the WFH hardware bundle. People are working at home with spouses who are also working or streaming, and kids that are gaming, streaming, or studying. As a result, their internet bandwidth isn't adequate, causing videoconferencing to degrade or fail. The industry solution: more common WAN integration in laptops to guarantee more reliable connections and better videoconferencing meetings.

While backhaul issues are being reported regarding 5G deployments in the U.S., they're expected to be mitigated by mid-year. A dedicated WAN link that is secure and more reliable seems to be driving this trend. If you're planning to buy laptops in the year ahead, you may want to consider this option.

Improved cameras and sound

Another problem: laptops weren't set up to be a primary way to communicate. They have microphones, cameras, and speakers, of course, but the first two weren't used that often and the speakers were routinely tuned for entertainment more than work. Look for this trend to change in 2021. You can expect cameras that better handle employees who move while talking, automatically adjust their appearance so it looks as if they're focused on the camera and technology that creates a more attractive image.

Provisioning home offices and finding hardware that has been enhanced for remote work will be a lot easier next year. As the industry embraces the New Normal, the products and bundles they produce are evolving, too. From physical and virtual bundles for home offices that meet corporate needs to new laptops with 5G WAN, employees will be able to better connect safely from home.

FireEye Hacked

One of the US's leading cybersecurity firms, FireEye, says it has been hacked by a state-sponsored attacker. Hackers targeted and accessed the firm's so-called Red Team tools, which it uses to test customer security and find vulnerabilities. Now there's concern that the hackers could release these tools publicly or use them to attack others, though there is no evidence that this has happened yet. FireEye says that it does not believe any customer information was taken.

Although FireEye's statement does not say who is responsible, it says that the attacking nation has "top-tier offensive capabilities." The Wall Street Journal reports that Russia is a suspect, specifically its foreign-intelligence service known as the SVR. However, the investigation into who is responsible is ongoing. "This attack is different from the tens of thousands of incidents we have responded to throughout the years," FireEye sas, noting that the attackers "are highly trained in operational security and executed with discipline and focus." The disclosure did not say when the hack took place or when FireEye became aware of it.

"They operated clandestinely, using methods that counter security tools and forensic examination. They used a novel combination of techniques not witnessed by us or our partners in the past," said FireEye. The company is investigating the hack alongside the Federal Bureau of Investigation, as well as industry partners like Microsoft. "The FBI is investigating the incident and preliminary indications show an actor with a high level of sophistication consistent with a nation state," the FBI cyber division said in a written statement.

People familiar with the investigation said the hackers were disciplined and used a rare combination of attack tools, some of which apparently hadn't been previously used in any known attacks on other victims – an unusual sign of sophistication and resolve – and were specifically dedicated to compromising FireEye. The hackers were also described as taking advanced measures to conceal their activity and identity. "This was a sniper shot that got through," a person familiar with the investigation said.

FireEye's disclosure of the attack, which the WSJ notes caused its shares to drop around 7 percent in after-hours trading, was praised by US Senator Mark Warner, who serves as vice chairman of the Senate Select Committee on Intelligence and co-chairs the Senate Cybersecurity Caucus. "I applaud FireEye for quickly going public with this news, and I hope the company's decision to disclose this intrusion serves as an example to others facing similar intrusions," he said, adding that the attack "shows the difficulty of stopping determined nation-state hackers."

In response to the attack, FireEye said it has developed over 300 countermeasures to help its customers and the cybersecurity community defend against the stolen tools. It's implemented these countermeasures into its own security products, shared them with "colleagues in the security community," and is making them publicly available. FireEye intends to share further countermeasures as they become available.

Protect Your PC from Ransomware

With all the talk of ransomware and need for security, there are measures built into Windows 10 to help protect your data. These are applicable to your home PC too, which may not have the same level of protection as your company device may have in place. Here are some steps you can take to further protect yourself.

Microsoft has an easy-to-configure anti-ransomware included in all versions of Windows 10 called Controlled Folder Access. It protects you by letting only safe and fully vetted applications access your files. Unknown applications or known malware threats aren't allowed through. By default, the feature is not turned on, so if you want to protect yourself against ransomware, you'll have to enable it. And you can customize exactly how it works by adding new applications to its whitelist of programs that can access files, and adding new folders in addition to the ones that it protects by default. To switch it on, you'll need to access Windows Security. There are several ways to get to it:

- Click the up arrow to the left of the taskbar's notification area, then click the Windows Security shield icon.
- Or, from the Settings app (click the Start > Settings), you can select Update & Security > Windows Security.
- Or, you can type windows security into the search box next to the Start button and select Windows Security from the flyout screen that appears on the right.

However you do it, once there, select Windows Security > Virus & threat protection. Scroll down to the "Ransomware protection" section and click Manage ransomware protection. From the screen that appears, under "Controlled folder access," toggle the switch to On. You'll get a prompt asking if you want to make the change. Click Yes.

This will now automatically protect your system folders and user-specific folders like Documents, Pictures, Music and Video. To add other folders you want protected, click the **Protected folders** link that appears after you switch on Controlled Folder Access. A prompt appears asking if you want to make the change. Click Yes. Click the Add a protected folder button that is on top of the list of protected folders that appears, then navigate from the screen that appears to the folder you want to protect and click **Select Folder**.

SIM2K has also stressed the importance of having backups of your data. However, you need to be careful about choosing the right backup technique and service. Microsoft suggests using a cloud-based storage and backup service rather than only backing up to a drive attached to your PC. If you back up to a drive attached to your PC, when your PC gets infected with ransomware, the backup drive will likely be encrypted along with any other disks inside or attached to your PC. Make sure that your cloud-based storage and backup uses versioning – that is, it keeps not just the current version of each of your files, but previous ones as well. That way, if the most current version of your files gets infected, you can restore from previous versions. Our SIM2K Backup Backstop service does use provisioning, so your company files meet this standard. Call us for more information on steps you can take to protect your data.

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 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

iOS Patches Critical

Apple has patched three vulnerabilities in iOS (and iPadOS) that were actively being exploited in targeted attacks. Vulnerabilities that are being exploited in the wild without a patch being available are referred to as zero-days. The vulnerabilities were found and disclosed by Google's Project Zero team, and patches have been released.

What has Apple patched in the update?

Publicly disclosed computer security flaws are listed in the Common Vulnerabilities and Exposures (CVE) list. CVE is a dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures. The goal of CVE is to make it easier to share data across separate vulnerability capabilities (tools, databases, and services).

The zero-days are listed under the ID numbers:

CVE-2020-27930: Affected by this issue is some unknown processing of the component FontParser. Manipulation with an unknown input could lead to a memory corruption vulnerability. This means a font could be created which leads to memory corruption, allowing for a remote code execution (RCE) attack .

CVE-2020-27932: A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of reports that an exploit for this issue exists in the wild. Using such a vulnerability could allow malware to bypass security restrictions on an affected system.

CVE-2020-27950: A malicious application may be able to disclose kernel memory. Apple is aware of reports that an exploit for this issue exists in the wild. Disclosed kernel memory may contain sensitive data like encryption keys and memory addresses used to defeat the address space layout randomization.

Update your iOS now

Since Apple has flagged that at least two of these vulnerabilities are being exploited in the wild and told us of the possible consequences, users should install the update as soon as possible.

So how concerned should you be? It's not known how actively these vulnerabilities are being exploited and whether they are targeted at specific individuals or the wider iPhone user base. After all, it wouldn't be sensible to share more details until everyone has updated their iPhones and iPads to iOS 14.2.

A researcher at Immersive Labs says the FontParser vulnerability is "worrying." However, he says: "There are few details to go off so it is unclear just how much of a risk this may pose." As for the kernel vulnerability, he says: "It is unclear how freely available this is, but this is perhaps the most worrying. The ability to read data and being able to execute code within the kernel is as bad as it gets, given that the kernel is essentially the heart of the operating system."

Owners of an iPhone or iPad are advised to update to iOS 14.2 and iPadOS 14.2 or iOS 12.4.9. You can always find the latest Apple security updates at its security updates site, **www.support.apple.com**

"Random Tid-Bytes"

Year End Tax Strategy

Are you trying to use up your budget before the end of the year? Section 179 Tax deduction of the IRS code can be a powerful incentive for your prospects. When you buy (or lease) communication equipment or software for your office now, you can deduct the FULL PURCHASE PRICE from the gross income on an accelerated depreciation basis in a single year as long as it's less than the deduction limit of $1,000,000. The pandemic this year has thrown off the budgets of many organizations and it is possible you have some unused dollars that you can use to improve your technology like servers or desktops, or invest in a new phone system like the Zultys Unified Communications that SIM2K markets. Call us for details.

Salesforce Takes up the Slack

Salesforce has acquired collaboration software vendor Slack in a deal worth $27.7 billion. The acquisition will integrate Slack's business chat app into Salesforce's cloud-based Customer 360 product. For Slack, the deal will mean access to more large-enterprise customers and greater clout as it competes with key rival Microsoft. "On the plus side, Slack gets an investor who can build out the service into what it may need to compete with Microsoft and Google," said an analyst at Moor Insights & Strategy. To truly compete with collaboration software suite vendors like Microsoft and Google, the analyst says Salesforce will need to further bolster its proposition around video and personal productivity.

Microsoft Updates the Edge Browser

Microsoft has released Edge 87, debuting automatic Internet Explorer-to-Edge redirection of specific sites and beefing up the new tab page with customizable feeds which display business-related content. Now, rather than letting IE render some websites, Microsoft will automatically close the tab in IE and then display a message asserting that the site 'oesn't work in the aged legacy browser. At that point, the same URL will be opened in an Edge tab and the user will be prompted to make Edge the default browser from a banner beneath the address field. Microsoft has also advanced its new tab page emphasis in Edge 87, which now blends the 365 elements with "personalized, work-relevant company and industry feeds." Users can customize the "My Feed" display with relevant content from both public options and from areas that the IT staff has selected. Personalization by the user is a straight-forward process of selecting from numerous choices. On the enterprise IT side, administrators can control the feed setting from the Admin Center. There, IT personnel can choose the appropriate industry and/or point to internally-generated news from the company itself. Finally, Microsoft flipped the default of ClickOnce to on; previously, ClickOnce had been set as off. The change brought Chromium Edge in line with the original Edge. ClickOnce is a Microsoft-made deployment technology that lets publishers, including enterprises, install apps directly from a web page.

Ransomware Takes Out Many Services

A series of ransomware attacks has taken out several Cloud-based services, specifically in web hosting and medical practice management.

One of the first attacks hit Managed.com, one of the biggest providers of managed web hosting solutions, resulting in the company taking down all its servers. The attack took place on Monday, November 16, and the ransomware impacted the company's public-facing web hosting systems, resulting in some customer sites having their data encrypted. At first, Managed.com said the incident only impacted a limited number of customer sites, which the company said it immediately took offline. But hours after the attack, Managed.com said it also took down its entire web hosting infrastructure, which the company is now working to restore. This included WordPress and DotNetNuke managed hosting solutions, email servers, DNS servers, RDP access points, FTP servers, and online databases.

Initially, the company passed the attack as unscheduled maintenance but eventually came clean in emails and messages provided by its tech support operators to an ever-increasing number of angry customers. The company says it is now working with law enforcement to identify the attackers and restore customer systems as soon as possible. But on online forums, Managed.com customers now fear that their sites will remain down for days or weeks. They cite a similar incident that took place at fellow web hosting provider A2 Hosting in May 2019, from which the company needed more than a month to recover, during which time a large number of customers had to wait for their sites and site data to be restored.

Multiple sources have reported that Managed.com was hit by the ransomware operation known as REvil. REvil is a Ransomware-as-a-Service that began infecting victims in April 2019 and has since grown to become one of the largest ransomware operations currently operating. According to a screenshot shared with an IT security company, REvil is demanding a $500,000 ransom in Monero to receive a decryptor. It is not known if the ransomware operation stole unencrypted files before encrypting devices.

In a recent interview with the public-facing representative of REvil, the ransomware operation claims to earn over $100 million a year in extortion payments. REvil has been responsible for large attacks in the past, including Travelex, Kenneth Cole, SeaChange, Brown-Forman, and celebrity law firm Grubman Shire Meiselas & Sacks (GSMLaw).

Then, earlier this month, a Cloud-based medical practice provider was forced to suspend services. After the shut down, it was discovered that ransomware had been introduced into the datacenter where the company's servers are hosted – Netgain. Ironically, the company chose them because they are one of the biggest and most secure data centers in the United States. They have security staff 24 hours monitoring and maintaining their servers. Yet even this major hosting company was impacted by ransomware.

A week after the first attack, Netgain was still working on getting all the cloud servers back online. In order to do so they need to recreate their domain controllers and scrub the network. They then began deploying scans on each individual server. This is a lengthy process as there are 1000s of servers across several locations in their network. The ransomware attacked the domain controllers that organized the 1000s of servers. Those servers have been replaced over the last few days and they have begun checking all the individual servers for any residual traces of the ransomware. Once cleared they will be returning the servers online. Currently they are automating the checking process.

These ransomware attacks are affecting cloud servers worldwide. Amazon's AWS servers were recently taken offline for a similar issue. Hospitals and schools server systems are currently being locked down due to attacks as well.

And, back in September, hospital and healthcare services provider Universal Health Services finally restored its network after being offline for more than a week in the wake of a massive cyberattack which forced it to shut down systems at locations across the US. The health system had disconnected the network to prevent the propagation of a malware attack.

According to Becker's Hospital Review, UHS is now in the process of restoring its EHR and back-loading data from the past week while hospitals were under downtime protocols.UHS, which runs more than 400 healthcare facilities in the US and UK, has more than 90,000 employees and cares for about 3.5 million patients each year. Its network appears to have been hit by a Ryuk ransomware attack which left a number of UHS hospitals in the US without access to computer and phone systems, including facilities in California, Florida, Texas, Arizona and Washington, D.C.

The Ryuk attack on UHS managed to disable multiple antivirus programs in place on the targeted systems. Once the antivirus software was disabled, the Ryuk malware caused the computers to log out and shut down, and if administrators attempted to reboot these systems, they simply shut down again. With their systems shut down, UHS clinicians were unable to access vital information, including data found in their EHR or PACS system.

It is critical for all businesses to be alert to the potential for a ransomware attack. This is continuing to be a major issue for security, as the "bad guys" are coming up with new techniques to inject ransomware into a system. The days of an infected false pdf-based invoice are long gone, so more robust security steps must be undertaken to harden a network against an attack. Also, comprehensive backups and an action plan readied – just in case. SIM2K can work with your company to look for vulnerabilities on your network and to audit your backups for content and ability to restore these files. We also can lead training for staff and conduct mock attacks to test staff understanding of what is a dangerous file. Please contact us for more information or to schedule a time to discuss anti-ransomware plans.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com