SIM2K
Adapting Technology to Your Business Needs

1•17
Information you can use

SIMformation

Ransomware Tops 2016 IT News

Ransomware is evil, and it continues to prey upon thousands of businesses every year. Most infections are fairly quiet affairs: A small business gets infected, almost always by some employee opening an e-mail attachment he or she mistakes as legitimate but that really contains the payload of a virus. Then several undetected hours later, all of the business' files – at least those the employee had access to, which in a lot of businesses without good security and permissions policies is all of the files – are encrypted, and demands for payment of a ransom in Bitcoin are made in exchange for the decryption key.

Of course, secure e-mail use and employee behavior is a problem in businesses of all sizes, and there have been some high-profile ransomware infections. One attack in the news affected the San Francisco Municipal Transportation Agency, which had to give free trips to all comers over Thanksgiving weekend while it worked to restore access to its machines. Here in Indiana, the Madison County government had its data encrypted by ransomware and ended up paying the ransom in order to decrypt files, and it has taken weeks to get the County fully back on line. This just proves that if government and large companies can get infected, then everyone can.

SIMformation has taken several looks at Ransomware in 2016, but felt it proper to again review steps you can take to help avoid being hit, as this problem is not going away in the near future.

First, understand that your existing antivirus solution is pretty much worthless at detecting ransomware. The ransomware creators have gotten very good at eluding most methods that today's anti-malware software uses to identify and quarantine threats. Unfortunately, far too many organizations think slapping a copy of Symantec Endpoint Protection or something similar on all of their workstations will prevent this kind of malware from infecting their network. This is simply not the case. Antivirus solutions are good at eliminating other threats, but they are extremely poor at detecting ransomware.

Backups are the only legitimate way to avoid paying the ransom. According to reports, this was the mitigation used by San Francisco. A spokesman said "Existing backup systems allowe us to get most affected computers up and running the next morning, and our IT team had the remaining computers functional in two days."

It is vital that you regularly and consistently test your backups by restoring them to spare hardware or a virtual machine to make sure they are good – otherwise you have not backed up. If a backup is made but there's no way to restore it, have you prepared for a disaster? In a word, no.

User education is also key for preventing ransomware. All of the technical solutions in the world will not help if your users still open up "XLS" and "ZIP" attachments that end up being anything but. Blacklisting and spam control can only go so far, and ransomware comes in with such a wide variety of payloads and covers that it can end up being counterproductive to try to ban, say, all ZIP files or all XLS files from coming into your organization over e-mail. Better to train your users to suspect all attachments are bogus, only open those they know are coming, and delete anything they are not absolutely sure about before opening – or call you first.

The ransomware being unleashed these days is much more sophisticated than the early variants that infected only mapped drives with assigned drive letters and did not know how to navigate beyond the traditional "C" drive. The newest strains of Cryptolocker and its cousins not only traverse the network, they infect the "previous versions," or shadow copies, that Windows makes of files. And it is even possible for unencrypted backups to also be infected and encrypted, rendering them absolutely worthless in any effort to avoid paying the ransom.

If you back up to a location that is still connected to the network, your backups are at risk – there is no way around it. This is typically why active backup strategies involving rotating hard drives are best when it comes to defending from these types of threats. Unfortunately, many businesses now rely solely on online backup strategies, backing up to a service in the cloud that by design must always have a network connection – so it is a very simple technical task on the part of the ransomware to encrypt those backups too.

As distasteful as it may be to reward this kind of hacking, there are some businesses without recent accessible backups that have been hit by Cryptolocker and its relatives that simply have no choice but to take a chance and pay the ransom.

How do you know the hackers will make good on their attempts? To date, there have only been a couple of instances when Bitcoins were transferred but the crackers did not make good on releasing decryption keys. To do otherwise would be tremendously short-sighted. The profit comes when users trust in the process enough that paying the ransom actually gets their files back. Word spreads, more computers are infected, more files are encrypted, and there are more opportunities to get ransom payments. If the crackers were to stop honoring the ransom payment, no one would have an incentive to pay, and this undeniably strong black market revenue source would dry up almost overnight. In the end, this is what Madison County did to regain access to their data files, and even then, news reports indicated the process did not go smoothly and it took weeks to restore the County to full functionality.

Ransomware will be an issue into 2017, so please consult with SIM2K for ways to help mitigate your exposure to this malware.

2017 Crystal Ball

What milestones are IT professionals aiming for in 2017? Where should resources be directed? As is our tradition, SIMformation takes a look at what the experts believe to be the "hot" technologies for the year we are entering.

Security
High-profile corporate data breaches, politically charged cyberattacks like those against the Democratic National Committee and the October Denial of Service attack that took down much of the Internet have kept security front and center for 2017, prompting many in IT to ramp up strategies and add layers to their lines of defense. In Computerworld's Forecast 2017 survey, 47% of the IT professionals polled said they plan to increase spending on security technology in 2017, and 14% chose security as the most important technology project currently underway at their organizations.

Moreover, 15% of those surveyed said they expect security to be their top leadership challenge over the next 12 months, and another 15% said they're currently beta-testing enterprise security technologies. Even those not pursuing specific security initiatives have security on their minds: 19% of the respondents said their primary goal for their most important project is "to meet security, privacy or compliance goals."

Analytics
As companies double down on their efforts to get closer to customers, data has taken on critical importance, with analytics serving as a springboard for success. Organizations are stockpiling data on web traffic, customer preferences, buying behavior, real-world product performance and more, creating a potential gold mine of insights – if they adopt the right strategy and use the right analytics tools to make sense of everything they collect.

Some 38% of survey respondents said they plan to increase spending on data analytics (a category that includes big data, enterprise analytics, data mining and business intelligence tools) next year, and data analytics was No. 4 on the list of technology projects that respondents cited as their organizations' most important initiatives. Moreover, 21% of respondents said their organizations are engaged in a beta test of a big data project, and nearly 30% pegged big data/analytics as the disruptive technology most likely to impact their organization over the next three to five years.

XaaS
Another year in and there's no stopping the cloud computing juggernaut, especially as companies retool IT infrastructure for digital transformation. The "as a service" trend continues to gain traction, with 33% of survey respondents reporting that their organizatons are planning to increase spending on software as a service (SaaS) offerings next year, putting SaaS at #5 on the list of most important technology projects. At the same time At the same time, 24% of those polled said they intend to spend more on platform-as-a-service (PaaS) technologies and 27% said they will put more money toward infrastructure as a service (IaaS) in 2017. And finally, 29% of respondents expect cloud or SaaS systems to be the disruptive technology that has the most impact on their business over the next three to five years.

Mobile Apps
As smartphones and tablets become standard fare for consumers and employees alike, IT groups are racing back to the drawing board to retool existing applications to be mobile-friendly while creating new mobile apps to court customers and gain competitive advantages. In the Computerworld survey, 35% of those polled said they plan to increase spending on mobile systems next year. Nearly 10% said they are beta-testing mobile apps, while 21% of those with hiring plans said they hope to add people with mobile application and device management skills.

Virtualization
The march toward wholly virtualized IT environments rolls on. Companies are virtualizing more than just desktop systems these days and are beginning to expand their efforts to areas like servers, networks, storage and even mobile infrastructure. Some form of virtualization will be on the docket for 29% of survey respondents in 2017, and of those who are planning hiring increases next year, 18% said they will be looking for people with expertise in virtualization.

Desktop systems are still the most common targets of virtualization initiatives – 16% of respondents to the Computerworld survey said they currently have desktop virtualization beta tests underway. Storage is the second most common technology to be virtualized, with 11% of respondents saying they are beta-testing such systems, followed by server virtualization at 10%, mobile virtualization at 8% and network virtualization at 7%.

IT leaders are adopting and applying these five technologies with specific business outcomes in mind. One of the most important is customer satisfaction. Nearly half (48%) of the respondents to the Computerworld survey said improving customer satisfaction or the customer experience was the most important business priority for IT in the coming 12 months.

SIM2K continues to monitor where the IT industry is headed, and is already deeply involved in many of these 2017 trends, such as virtualization of servers and security of our customers' data and networks. We are always ready to meet with you to discuss where technology trends can mesh with your business goals in 2017, so please feel free to call Mark or Ben at SIM2K to discuss how we can partner with you for new technology applications in upcoming years.

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.

Bluetooth 5 Aids IoT

Bluetooth is aiming straight for the internet of things as the fifth version of the wireless protocol arrives with twice as much speed for low-power applications. Bluetooth Low Energy (BLE), which gains the most from the new Bluetooth 5 specification, can now go as fast as 2Mbps (bits per second) and can typically cover an entire house or floor of a building. This could help make it the go-to network for smart homes.

The home IoT field is pretty open right now because most consumers haven't started buying things like connected thermostats and door locks. Bluetooth starts out with an advantage over its competition because it's built into most smartphones and tablets. As the new protocol rolls out to phones, users should be able to control Bluetooth 5-equipped devices without going through a hub.

Bluetooth is in a gradual transition between two flavors of the protocol. The "classic" type is what's been linking cellphones to cars and mice to PCs for years. BLE, a variant that uses less power, can work in small, battery-powered devices that are designed to operate for a long time without human interaction. BLE devices now outnumber classic Bluetooth products and most chips include both modes. With Bluetooth 5, BLE matches the speed of the older system, and in time, manufacturers are likely to shift to the low-power version, experts believe.

Range has quadrupled in Bluetooth 5, so users shouldn't have to worry about getting closer to their smart devices in order to control them. Also, things like home security systems – one of the most common starting points for smart-home systems – will be able to talk to other Bluetooth 5 devices around the house.

Another enhancement in the new version will help enterprises use Bluetooth beacons for location. BLE has a mechanism for devices to broadcast information about what they are and what they can do so other gear can coordinate with them. Until now, those messages could only contain 31 bytes of information.
Now they can be eight times that size, making it easier to share information like the location and condition of enterprise assets, such as medical devices in hospitals.

The new, longer range is an improvement, but a "mesh" would be better, experts say. In a mesh configuration, each device only needs to connect with the one closest to it. That takes less power, and it's better than relying on each device's range to cover a home, because walls and other obstacles can keep signals from reaching their full range. This is something in development from the Bluetooth development group, according to insiders.

Consumers are also waiting for a high-fidelity audio connection to wireless headphones, a need that's getting more urgent as phone makers phase out physical jacks. This is coming from Bluetooth but not here yet. Although Bluetooth 5 makes strides that could help drive IoT adoption, the field is still open, experts believe.

Bluetooth technology will certainly help to expand the abilities of the IoT, especially for home-based use, so rapid acceptance of the Bluetooth 5 protocol should spark more connectivity options.

"Random Tid-Bytes"

Do You have a Yahoo! Account?

Security researchers are disturbed that it took Yahoo three years to discover that details on more than 1 billion user accounts had been stolen in 2013. The breach suggests that someone – possibly a state-sponsored actor – had access to one of the largest e-mail user bases in the world, without anyone knowing. The stolen database may have even included information on e-mails of U.S. government and military employees. Yahoo said in November it first learned about the breach when law enforcement began sharing with the company stolen data that had been provided by a hacker. At the time, the company was already dealing with a separate data breach reported in September involving 500 million user accounts. However, this hacker was apparently sitting on another mother lode of stolen Yahoo data, but it's still unclear how the theft occurred. If you have a Yahoo account and haven't changed your password, do it now!

Nokia Sues Apple

Mobile phone maker Nokia has filed lawsuits against Apple alleging that the smartphone giant has infringed on 32 of its patents. The lawsuits cover patents related to displays, user interfaces, software, antennas, chipsets, and video coding, Nokia said. Nokia has offered Apple a license for the encoder technology, but Apple has refused to pay, the company asserted. "Nokia has negotiated in good faith and made substantial efforts to enter into a license agreement with Apple on reasonable and non-discriminatory terms," its lawyers wrote. Nokia research has contributed to "fundamental technologies" used in Apple products. "After several years of negotiations trying to reach agreement to cover Apple's use of these patents, we are now taking action to defend our rights."

Russian Scam Detected

A $1 billion Russia-based criminal gang has been bilking online advertisers by impersonating high-profile Web sites like ESPN, Vogue, CBS Sports, Fox News and the Huffington Post and selling phony ad slots, but that's about to end. An online fraud-prevention firm is releasing data that will enable advertisers to block the efforts of the group and the scam that involves control over the buying and selling of video ads. The group has been ramping up its activities since October so that it now reaps roughly $3 million to $5 million per day from unsuspecting advertisers. When someone clicks on a video that's posted to a Web page, the video is often preceded by a short advertising video known as pre-roll. The pre-roll slot is sold realtime – within 100 milliseconds – via an automated auction. That click to request the video is what initiates the ad auction, and the browser directly receives the pre-roll from the advertiser that wins. The gang has created a robo-browser called Methbot that spoofs all the necessary interactions needed to initiate, carry out and complete the ad transactions. The system runs an instant auction, settles on an ad and sends it to Methbot, which verifies that it received it and played it. Then the advertiser pays the entity the website that the browser claimed to be visiting, but that entity resolves ultimately to the gang, not to the true provider.

A Year of Windows 10 In Review

Windows 10 has been dogged by various controversies since soon after its release. Anger about Windows 10 rarely dies down for long, and this year Microsoft has faced backlashes about the OS's approach to privacy, upgrades and user control.

Here are the biggest storms that whipped up around the OS in 2016, and one example of how Microsoft sometimes does listen to its users.

"Tricking" users into switching to Windows 10

Early in the year, Microsoft faced a fierce backlash over changes it made to get Windows 7 and 8 users to upgrade to Windows 10.

The company was accused of effectively tricking people into upgrading to Windows 10 by changing the design of the user promot for its "Get Windows 10" app, the software that scheduled upgrades from Windows 7 or 8 to Windows 10. Microsoft altered prompt so that clicking "X" to close it caused the user to effectively agree to a scheduled upgrade to Windows 10, rather than dismissing the upgrade as had previously been the case. The change put Microsoft in violation of its own user experience guidelines for developers on how to design dialog boxes.

Following widespread criticism, Microsoft reversed the decision and changed the pop-up so clicking "X" once again dismissed the upgrade.

It wasn't the only unpopular decision Microsoft made this year, during the company's aggressive campaign to grow Windows 10's user base. The company also made Windows 10 a "Recommended Update" for Windows 7 and 8, which resulted in the upgrade process automatically initiating on most home machines without the user's knowledge.

Forced updates

Microsoft continues to face pressure from a group of Home users who want more control over when updates are applied to the OS.

The Home edition of Windows 10 doesn't allow users to defer installing updates to the OS. While Microsoft argues this approach helps keep users' machines up-to-date, some users are calling for greater control over when the updates are applied, without having to resort to software hacks to control the process.

While Windows 10 was updated to give Home edition users more control over which time of day updates are applied, this falls short of the level of control sought by a vocal group of users. They would like the Home edition to be able to defer updates in much the same way that most other editions can – thus allowing them to install updates once users are assured that these patches are bug free and will not crash their PCs. For example, those running Windows 10 Pro or Enterprise that come with the "Windows Update for Business" feature, can put off updates for up to eight months and security updates for up to four weeks, as well as have the ability to temporarily pause upgrades and updates.

Bugs, bugs and more bugs

The downside of not being able to say no to updates is that sometimes they can break things. At various points throughout the year there have been complaints of PCs going wrong after applying the latest Windows 10 updates.

A glut of complaints emerged in the wake of the Windows 10 Anniversary Update this summer. Following the major patch, groups of Home users reported frozen systems and broken webcams. Fresh updates continue to cause problems for users, most recently Windows 10 PCs not being able to connect to the Internet.

Cut Features

While Microsoft uses updates to add new features to Windows 10, these same patches have also been used to remove useful settings.

Following the Windows Anniversary Update this summer, it became a lot more difficult to disable Windows 10's built-in virtual assistant Cortana. The change saw a simple off switch in a sidebar replaced with a less-obvious, multi-step process or the need to use administrator-level tools.

Microsoft also altered the Windows Pro edition to prevent users from editing Group Policy settings to stop ads for apps showing in the Start menu and on the lockscreen, although these ads can still be disabled by individual users.

More and More Ads

Windows 10 has had ads for Windows Store apps since it launched, but over time Microsoft has made these ads more visible. In February, Microsoft began advertising Windows Store apps using the Windows 10 lockscreen, with users reporting seeing ads for the game Rise of the Tomb Raider. And following the Windows 10 Anniversary Update, new installs of Windows 10 began to show double the number of ads for Windows Store apps in the Start Menu. Luckily there are various options for disabling these ads.

Calls to Stop Snooping

Fair or not, Windows 10 has acquired a reputation for snooping on its users. The question of whether Windows 10 tramples user privacy was raised again this year, with the Electronic Frontier Foundation saying the OS forces users to "choose between having privacy and security." Much of the argument revolves around the large amounts of data Windows 10 collects by default from users of the Home edition. This includes information about how Windows and Windows apps are used, what you type, your contacts, your location, calendar appointments and more. If the virtual assistant Cortana is enabled, this data extends to web browsing history, voice commands and even more information about your activity.

Windows 10-only Hardware

Those wanting to stick with Windows 7 on new PC hardware had their hopes dashed. Microsoft announced that Windows 7 and 8.1 will not be updated when running on PCs powered by upcoming processors. These newer machines will need to be running Windows 10 to continue to receive updates.

Obviously we are stuck with Windows 10, but SIM2K still believes Windows 7 is entirely appropriate for our customer base so don't be in a rush to update existing PCs.

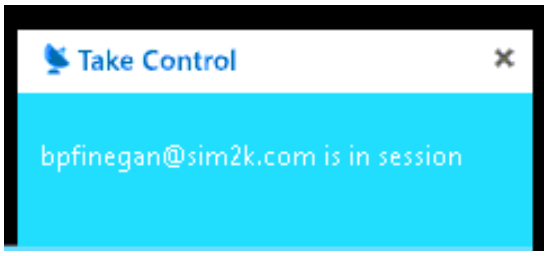
SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com

Tech Talk - from the Support Team

One of the ways that SIM2K works with our clients is through our ability to remotely connect directly to your workstation to help troubleshoot issues or work directly with software on your machine. This way we can more quickly address your problem without having to take the time to travel to your office.

We want to make our customers aware of an option they have for how we connect to their computers remotely. Our goal is to continue to make sure they are comfortable with our level of access, since we will be able to "see" what is on that computer at the time and what files may be stored locally. First of all, if a SIM2K employee is on the phone, we will always ask for permission to connect to their machine before initiating a support session. Once approved, we will then activate our remote connection.

Customers will always see this icon, with your particular Support Tech's name displayed, when we connect with our Agent:



If necessary, there are additional settings that can be put in place to set boundaries on our interaction with your workstation. These include:

Request user permission – we can enable a setting where the end user must approve our connection to their computer. Example: the user might want to close a confidential document before we connect.

Allow remote control after request timeout – we can also enable a setting where we connect after the connection request times out (such as a user is away from their desk or not paying attention).

Windows credentials – regardless of our remote connection, their computer will still be protected by their Windows credentials. If the machine is locked, we would have to know credentials to unlock it.

In some cases where our agent is not available, we may need to direct the client to an alternative way to connect whereby they will start the connection from an Internet browser. In that case, the user is prompted to make the connection with us as well as grant us control of their computer. Here we will have to be in contact with the user to coach them through this process.

Having the ability to connect remotely is an excellent way for SIM2K to be able to quickly "get in and fix it" for most workstation problems. However, we understand that we must work within your company's policies on workplace interruptions, so that is why we will always either ask to connect or ask to set a good time for us to complete this task.

Amazon Dominates Holiday E-Shopping

Although retailers know only too well how incredibly massive a rival Amazon has become – it's annualized revenue last year hit $131 billion, which is almost pure online dollars – it's scope is sometimes difficult to grasp. Holiday statistics from Slice Intelligence gave Amazon an amazing 46% of all U.S. e-commerce dollars, which is three percentage points more than the prior year.

This trashes the generally accepted assumption in e-commerce that Amazon would dominate for a time but that major chains such as Walmart, Target and specialty players such as Apple would slowly increase their collective market share.

Instead, we have numbers that show Amazon growing its market share by 3%. Put another way, the total of ***all other*** retailers combined lost online market share. OK, 46% is a remarkable figure, but are the others even close? No. The study had the next top retailer's market share, Best Buy, at 2.9%, followed by Walmart and Apple(2.6%), Target (2.4%) and down from there.

Two things are driving shoppers to Amazon: brand trust and shipping speed. And brand trust and shipping speed, for a holiday shopping season, are everything. The most regular and loyal Walmart shopper will trust the chain to handle in-store purchases in the traditional Walmart way. But Walmart's store-first-and-always approach to almost everything means that it is sending a message to its shoppers that its online experience will be substandard. This attitude is sending shoppers to Amazon. When they want online, they go a retailer that they know cares about online.

Plus, Amazon delivered packages within 3 days during the holiday season, so shoppers are getting their goods quickly. Amazon has put far more marketing muscle into its same-day deliveries than anyone else. That sent a signal of confidence, one that was reinforced by lots of favorable social media experience reports about Amazon's same-day deliveries.

Amazon has retail chains beat at speed and reputation. Once it fully dominates on everyday purchases, the game may be close to over for brick-and-mortar retailers.

Need Help? Send support requests to:

tickets@sim2k.com