SIM2K
Adapting Technology to Your Business Needs

6•21
Information you can use

SIMformation

Lessons From Pipeline Ransomware

The head of Colonial Pipeline told a Senate committee that hackers who launched last month's cyber attack against the company and disrupted fuel supplies to the U.S. Southeast were able to get into the system by stealing a single password.

Colonial Pipeline Chief Executive Joseph Blount said that the attack occurred using a legacy Virtual Private Network (VPN) system that did not have multifactor authentication in place. That means it could be accessed through a password without a second step such as a text message, a common security safeguard in more recent software. "In the case of this particular legacy VPN, it only had single-factor authentication," Blount said. "It was a complicated password, I want to be clear on that. It was not a Colonial123-type password."

The panel was convened to examine threats to critical U.S. infrastructure and the Colonial attack, which shut key conduits delivering fuel from Gulf Coast refineries to major East Coast markets. Cyberattacks also hit U.S. meatpacking plants owned by JBS, showing the breadth of infrastructure facing cyber threats.

The Colonial Pipeline hack demonstrated that much of the company's infrastructure remains highly vulnerable and the government and companies must work harder to prevent future hacks, senators said during the hearing. Security experts call the use of a single-factor login system a sign of poor cybersecurity "hygiene."" They recommend two-factor authentication, which requires a secondary measure like a mobile text or hardware token, and most major companies require this across all internal applications.

Senators questioned Blount about the company's preparations and the timeline for responding to the ransomware attack, which shut the line for days and led to a spike in gasoline prices, panic buying and localized fuel shortages. "I'm alarmed this breach ever occurred in the first place," said Senator Gary Peters, the committee's chairman. "Make no mistake: if we do not step up our cyber security readiness, the consequences will be severe."

The FBI attributed the hack to a gang called DarkSide. Some senators suggested Colonial had not sufficiently consulted with the U.S. government before paying the ransom against federal guidelines. Blount said he made the decision to pay ransom and to keep the payment as confidential as possible because of concern for security. "It was our understanding that the decision was solely ours to make about whether to pay the ransom," he said. Blount said even after getting the key from the hackers, the company is still recovering from the attack and is bringing back seven finance systems that have been offline since May 7.

Blount said Colonial did not have a plan in place to prevent a ransomware attack, but did have an emergency response plan. The company notified the FBI within hours.
Blount said Colonial has invested over $200 million over the last five years in its IT systems. When pressed to answer how much Colonial has spent to keep its pipeline cyber secure, Blount repeated that amount. A company spokesperson later clarified the $200 million was for IT overall, which includes cyber security.

In a later development, the Justice Department said it had recovered some $2.3 million in cryptocurrency ransom paid by Colonial Pipeline. Colonial Pipeline previously had said it paid the hackers nearly $5 million to regain access. The value of the cryptocurrency bitcoin has dropped, so as a result, while the government recovered about 60 of the 75 bitcoin paid, the value has decreased, falling short of the total dollar amount Colonial paid.

So the lesson from this hack is that security has to be in force for all possible avenues. In Colonial's case, one password, even if it was a complex password, got them VPN access. And once in the VPN, the hackers had all the resources needed to launch their attack. Companies need MultiFactor Authentication on the VPNs. This would have stopped the attack as well as alerted Colonial that their network was being probed, giving them time to reinforce their defense.

Our adversaries are intelligent, diligent and creative. SIM2K has ways to look for this, technical tools to disrupt this and training programs for staff to avoid this. We employ MFA for our own internal systems such as e-mail and VPNs, and we can do the same for your company. Please contact us for more information on how we can use these advanced tools to protect your network.

CyberInsurance Heats Up

Last month SIMformation discussed how some insurance carriers are running audits on policyholders' networks to assess their level of security and look for issues such as out-of-service or unpatched software running. Local insurance agent Todd Carbrey discussed how the application process for a cyberinsurance policy would help to reveal any potential issues with security that would impact coverage.

We have some examples to share. The first is from The Travelers. This is from their application and shows the types of questions to expect:

The controls described above and listed below are the minimum controls that must be in place in order to be eligible for a Cyberrisk policy. Because of the importance of the controls in preventing ransomware attacks the following attestation should be completed with the assistance of the person(s) in charge of network security. If network security is outsourced to a managed security provider or other 3rd party please complete the attestation below with their assistance.

MULTI FACTOR AUTHENTICATION ATTESTATION

1	Multi-Factor authentication is required for all employees when accessing e-mail through a website or cloud based service.	☐ Yes ☐ No ☐ Email is not web based
2	Multi-factor authentication is required for all remote access to the network provided to employees, contractors, and 3rd party service providers.	☐ Yes ☐ No
3	In addition to remote access, multi-factor authentication is required for the following, including such access provided to 3rd party service providers:	
	All internal & remote admin access to directory services (active directory, LDAP, etc.).	☐ Yes ☐ No
	All internal & remote admin access to network backup environments.	☐ Yes ☐ No
	All internal & remote admin access to network infrastructure (firewalls, routers, switches, etc.).	☐ Yes ☐ No
	All internal & remote admin access to the organization's endpoints/servers.	☐ Yes ☐ No
4	The signer of this form has done so with the assistance of the person in charge of IT security.	☐ Yes ☐ No

Executive Officer Signature: X | Name, Title, and email address: | Date (month/dd/yyyy):

Executive Officer is defined as the applicant's chief executive officer, chief financial officer, chief information security officer, risk manager, in-house general counsel, or the functional equivalent.

As you see, they are requiring Multi-Factor Authentication (2FA) in about any situation where someone will come into contact with their network, from e-mails to network equipment. An IT security person is also required to be consulted when completing this, whether an internal or third-party (like SIM2K).

The second example is from Tokio Marine. This is the carrier we discussed in last month's issue that was conducting unannounced audits on policy-holder networks, probing for any security issues.

6. EMAIL SECURITY CONTROLS		
	If the answer to any question in this section is "No", please provide additional details in the "Additional Comments" section	
a.	Do you tag external emails to alert employees that the message originated from outside the organization?	☑ Yes ☐ No
b.	Do you pre-screen emails for potentially malicious attachments and links?	☐ Yes ☑ No
	If "Yes", do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if they are malicious prior to delivery to the end-user?	☐ Yes ☐ No
c.	Have you implemented any of the following to protect against phishing messages? *(Please check all that apply)*	
	☑ Sender Policy Framework (SPF)	
	☐ DomainKeys Identified Mail (DKIM)	
	☐ Domain-based Message Authentication, Reporting & Conformance (DMARC)	
	☐ None of the above	
d.	Can your users access email through a web application or a non-corporate device?	☑ Yes ☐ No
	If "Yes", do you enforce Multi-Factor Authentication (MFA)?	☑ Yes ☐ No
e.	Do you use Office 365 in your organization?	☐ Yes ☑ No
	If "Yes", do you use the Office 365 Advanced Threat Protection add-on?	☐ Yes ☐ No
ADDITIONAL COMMENTS *(Use this space to explain any "No" answers in the above section and/or to list other relevant IT security measures you are utilizing that are not listed here.)*		

This application is a bit more direct in the questions they are asking, going beyond just the use of 2FA and looking for advanced security options such as sandboxes to scan incoming mail prior to release to defend against phishing attacks as well as more robust security tools like tagging externally-received mail so the recipient knows it is from outside the company and thus be treated with more care.

SIM2K has now seen more examples of Insurance carriers who are running internal audits of client networks and generating modified premiums (read as more $$$) based on those audits.

And, in an extreme situation, this client's existing carrier dropped them. Having on-premise Exchange was an automatic decline for another carrier. The March Microsoft Exchange hack was a wake-up call for security experts. A month later experts were reporting that 99,000 servers were still running un-patched Exchange. The FBI's action to access private networks to remove potential malware installed in this hack as they felt that many companies did not have the requisite IT skills to detect and remove the web shells was another indication of the vulnerabilty. Thus, it is very evident that on-premesis Exchange is a non-starter for cyberinsurance coverage.

SIM2K had a meeting with Traveler's insurance where they reported their research shows that MFA stops almost 90% of ransomware incidents. If you don't have cyber insurance, you need to consider it. We will be hosting a seminar this summer with cyber insurance providers (teaser).

We also have the ability to implement and manage all of the standard and widely accepted technical controls and training programs. These things do cost money. The cost is manageable and the unfortunate alternative can be much worse up to and including closing down.

SIM2K is also seeing the need for companies to segment the network through use of VLANs (virtual local area networks) to keep "watertight compartments" where hackers cannot proceed willy-nilly through a network. Every device that connects to a corporate network should be considered a potential server and potential weak point for a hack attack. Segmentation will help reduce the exposure. However, as the Titanic's sinking showed, watertight compartments are not infallible. Plus, patch management is not optional, it is required. Insurance carriers are insisting that companies follow best practices religiously, not on a "do it when we think of it" basis.

We are also seeing that defenses such as EDR (Endpoint Detection Response) and NGAV (Next Generation Anti-Virus) are requirements. SIM2K offers Bitdefender for EDR and Cylance for NGAV protection. And, we are constantly evaluating new solutions as they come to the market to add to our portfolio of security solutions such as our new partnership with Huntress and their managed detection and response platform.

Cybersecurity is paramount. "The first thing we have to recognize is this is the reality and we should assume, and businesses should assume, that these [Ransomware] attacks are here to stay and if anything will intensify. Just last week, the White House sent out a letter broadly to the business community, urging the business community to do more," Gina Raimondo, the U.S. Commerce Secretary, said last week. Any company seeking insurance coverage needs to realize that this is serious business and that there needs to be enhanced security in place prior to any application. SIM2K can help audit your network and help you complete these applications. Call Ben for details.

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.

Somebody Broke the Internet

June 8 will be remembered as the day the internet broke – before swiftly being fixed again. Early in the morning, websites including Amazon, Reddit, Spotify, eBay, Twitch, Pinterest and CNET went offline due to a major outage at a service called Fastly. Everywhere on the Web there were 503 errors and people complaining they couldn't access key services and news outlets. After an investigation into what went wrong, Fastly published a blog post describing exactly what went down – and it turns out the whole incident was triggered by just a single, unnamed Fastly customer.

In mid-May, Fastly issued a software deployment that contained a bug, which if triggered in specific circumstances could take down vast swaths of its network. The bug lay dormant until June 8, when one Fastly customer inadvertently triggered it during a "valid configuration change," which caused 85% of the company's network to return errors.

Early morning, Fastly's status update page noted an error, saying "we're currently investigating potential impact to performance with our CDN [content delivery network] services." Shortly thereafter, reports emerged on Twitter of major news publications including the BBC, CNN and The New York Times being offline. Rather than isolated incidents affecting individual sites, it turned out this was a massive outage that had brought much of the Internet to its knees. Across the world, people were receiving Error: 503 messages as they tried to access sites, including some vital services, such as the UK government's gov.uk web properties.

To make sure the problem doesn't repeat itself, Fastly has said it is taking a number of actions. It is deploying a bug fix across its network, while also conducting a complete post-mortem of the processes and practices it followed during the incident. The company is also going to be figuring out why it didn't catch the bug during its own testing processes and evaluating ways to improve remediation time.

Many people speculated on Twitter that the outage was caused by a cyberattack, but we now know that this wasn't the case. There are many technical reasons a CDN can fail, and cyberattacks are just one of them. It is concerning, however, to see quite how vulnerable they can be. "CDNs are part of the Internet's critical infrastructure and if threat actors hadn't already cottoned on to this as a direct attack vector to bring down the Internet, they will now after monitoring this event," said one cybersecurity specialist.

This is another example of a Cloud-based service that has far-reaching impact on the Internet and content we expect to see when we log onto a website. That a customer could trigger such an outage, or that a company had a bug they had not addressed, shows how quickly things can go wrong and impact millions.

"Random Tid-Bytes"

New Features in Chrome OS/Android

One new Chrome OS feature is the "Nearby Share" system for sending and receiving files wirelessly between multiple Chromebooks or Chromebooks and Android devices. Click or tap the clock area in the lower-right corner of a Chromebook's screen to open up the Chrome OS Quick Settings panel. Look for an option there called "Nearby visibility" and click that to see the actual Nearby Share settings configuration tool. There, you can initiate the system and opt to make your Chromebook visible to all of your contacts or just to a specific selection of people whenever the Chromebook is on and unlocked. There is also a toggle that will make the device visible to anyone in your area immediately for a five-minute window. Another new feature is easy VPN connections. Chrome OS has technically supported the use of VPNs for quite a while now but this has involved a bit of an awkward setup that relied almost entirely on third-party add-ons. Now Google has added in a form of system-level support that makes it easier to switch any VPN you like on or off right from the regular Chrome OS interface. First, you'll need to have an active VPN service available and installed on the device. Once you do, click or tap the clock area in the lower-right corner of your screen to open up that Quick Settings panel once more. Look for the "VPN" toggle. There, you should see all available VPN options present and waiting to be enabled. Just click the plus sign next to whichever VPN service you want. You will still be taken into that service's app to activate the VPN and get it going, but once you do, you'll see its status right there in the Quick Settings panel. Finally, Google is rolling out Live Caption to Chromebooks. This has been available for Android users for awhile, but now you can get real-time captions for audio tracks (like a podcast or video clip) on Chromebooks, as well.

Microsoft Dumps Windows 10X

Microsoft has admitted that it would not, after all, launch Windows 10X – the concept OS it first touted in 2019 and months later morphed into a competitor to Chrome OS. "Instead of bringing a product called Windows 10X to market in 2021 like we originally intended, we are leveraging learnings from our journey thus far and accelerating the integration of key foundational 10X technology into other parts of Windows and products at the company," said a Microsoft executive. Windows 10X began as an October 2019 announcement, when Microsoft called the future operating system "the best of Windows 10 built to enable unique experiences on multi-posture dual-screen PCs." It was supposed to power a fresh hardware category of two-screen, foldable, tablet-notebook hybrids that Microsoft and its partners were to design. In May 2020, Microsoft released a different story, saying at the time that because "the world is a very different place than it was last October when we shared our vision for a new category of dual-screen Windows devices" – presumably referring to the COVID-19 pandemic and subsequent remote working, remote schooling – the new OS would be used to "pivot our focus toward single-screen Windows 10X devices that leverage the power of the cloud." To many, that sounded like a call to compete with Chrome OS and Chromebooks. Now, Microsoft is dropping this project completely. Either they believe they can't compete against Chromebooks or that Surface tablets are an equal to Chromebooks without the need for a "lite" version of Windows powering them.

Colonial Pipeline Paid – The Ethics of Ransomware

Adapted from commentary by the IU Ostrom Workshop for Cybersecurity and Internet Governance

It took little over two hours for hackers to gain control of more than 100 gigabytes of information from Colonial Pipeline last month, causing the firm to shut down its fuel distribution network and sparking widespread fears of a gasoline shortage. The decision to pay off the attackers was also made with apparent speed, but the ethical arguments involved are age old and the implications could reverberate well into the future.

Cyberattacks, including those on critical infrastructure in the U.S., are nothing new. Ransomware has been a component of the cyberthreat landscape since the mid-2000s. But the Colonial Pipeline breach raised the stakes and highlighted the ability of ransomware to interrupt the vital services on which Americans rely.

It has been widely reported that the Colonial Pipleline CEO Joseph Blount agreed to pay a US$4.4 million ransom to DarkSide, the Russia-based group behind the cyber attack. In describing his decision, which he said did not come lightly, Blount argued that it was justifiable given that it was "the right thing to do for the country."

This raises the issue of the legal and ethical questions surrounding ransomware payments – just because paying off cyberattackers may be lawful in some contexts, that still doesn't make it the morally correct thing to do.

Official guidance from government security experts has always been to not pay. In October 2020, the Treasury Department warned that ransomware payments are a violation of its rules and would only encourage future demands. Although there is no federal legislation, such states as California, Texas and Michigan have cyber-extortion laws on the books that discourage ransomware payments.

Often, though, the decision of whether to pay falls in a legal and ethical gray area. CEOs can turn to three main schools of ethics in guiding decisions about whether to pay ransoms based on virtues, duties and consequences.

Under virtue ethics, people make decisions based on a set of virtues or character traits such as honesty and loyalty. In and of itself, the tradition does not help in situations that require weighing one virtue against another, such as not wishing to reward criminal activity against preventing disruption to the wider American public. For example, Colonial Pipeline CEO Blount expressed a moral distaste in paying "people like this," but ultimately decided to override that concern based on other factors.

Another way to approach challenging ethical decisions is by the view that actions are good or bad as determined by a clear set of rules. Here the question is "How does doing so align with recognized universal duties?" The problem with cybersecurity is that, given the rapidly changing technological and regulatory environment, it is not always clear what the "golden rules" are, or even if any have been established. Some business leaders may even perceive a duty to pay as Blount did, especially in the case of critical infrastructure such as pipelines on which so many people rely.

The ethics of ransomware payments can also be viewed through the consequences of the decision to yourself, your organization and, as Blount suggested, the country and the world - invoking what is the greatest good for the greatest number of people. This is often described in boardrooms and policy circles as cost-benefit analysis. Yet it's not always clear where to put that next dollar of investment to maximize the good and minimize the harm in the long term. In dealing with ransomware, for example, backing up data is key, as is practicing zero-trust security, an approach in which companies assume that their networks are already compromised and act accordingly.

But what are the pros of paying? In practice, business leaders use all these ethical tools, and more, in deciding whether or not to pay – and there isn't much time to weigh the options. Colonial Pipeline CEO Blount's decision reportedly came almost immediately. And it isn't universally accepted that Colonial Pipeline came to the right decision.

Some cybersecurity professionals want to ban paying out ransoms to halt the growing problem of malware attacks for profit. Others say banning payments would be a "horrific game of chicken" in which cyberattackers up the stakes until the consequences of not breaking the law are greater for the companies involved than the impact of the breach. And banning ransom payments outright would place an impossible burden on smaller businesses or organizations that do not have the resources to protect against malicious actors.

The thinking behind banning payments is that attacks might stop if they don't yield payments. Yet if the attack has the capability of paralyzing an entire entity, paying up is often the economically rational decision in the short term. Cybersecurity experts estimate that companies hit by attacks take an average of 287 days to fully recover to normal operations.

The rapid proliferation of attacks has been fueled by a new business model known as "ransomware as a service." Ransomware developers sell personalized variants to "affiliates" – cybercriminals who deploy the ransomware. With the emergence of ransomware as a service, ransomware can be profitable for both the developers of the variant and the affiliates.

Not all affiliates and ransomware developers are governed by the same moral code. DarkSide, which conducted the Colonial Pipeline attack, says it will not attack certain targets, such as medical services, the educational establishment and nonprofit organizations, and says it will completely leave a network alone after ransom is paid. The FBI discourages payment, partly on the grounds that it is not a guarantee that a company will not be hit again.

But the message is mixed. Law enforcement agencies encourage victims not to pay, but paying ransom is not illegal, and even police departments have been known to pay up when their systems have been compromised. And while the Treasury Department has been investigating new financial penalties against payment of ransoms, to date none have been levied. But even without the threat of legal sanction, payment of ransomware will continue to pose a moral dilemma.

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