SIM2K

Adapting Technology to Your Business Needs

8•22

Information you can use

SIMformation

Cyber Insurers Crack Down

In what may be one of the first court filings of its kind, insurer Travelers is asking a district court for a ruling to rescind a policy because the insured allegedly misrepresented its use of multifactor authentication (MFA) – a condition to get cyber coverage.

According to a July 6 filing in U.S. District Court for the Central District of Illinois, Travelers said it would not have issued a cyber insurance policy in April to Decatur, Illinois-based, electronics manufacturing services company International Control Services (ICS) if the insurer knew the company was not using MFA as it said. Additionally, Travelers wants no part of any losses, costs, or claims from ICS – including from a May ransomware attack ICS suffered.

Travelers alleged ICS submitted a cyber policy application signed by its CEO and "a person responsible for the applicant's network and information security" that the company used MFA for administrative or privileged access. However, following the May ransomware event, Travelers first learned during an investigation that the insured was not using the security control to protect its server and "only used MFA to protect its firewall, and did not use MFA to protect any other digital assets."

Therefore, statements ICS made in the application were "misrepresentations, omissions, concealment of facts, and incorrect statements" – all of which "materially affected the acceptance of the risk and/or the hazard assumed by Travelers," the insurer alleged in the filing.

ICS also was the victim of a ransomware attack in December 2020 when hackers gained access using the username and password of an ICS administrator, Travelers said. ICS told the insurer of the attack during the application process and said it improved the company's cybersecurity.

Travelers said it wants the court to declare the insurance contract null and void, rescind the policy, and declare it has no duty to indemnify or defend ICS for any claim.

Insurers are increasingly making standards for coverage more stringent. Cyberattacks and data breaches have been occurring for many years, but the nature of these threats has evolved rapidly since the start of the covid pandemic. In 2020, as a huge number of companies around the world shifted their employees to remote work, cyber incidents, and in particular ransomware attacks, skyrocketed.

Needless to say, the consequences of these attacks have been severe, with ransom demands climbing ever higher. For example, Garmin paid $10 million for a cyberattack in mid-2020. The looming threat of ransomware has, in turn, led to an uptick in companies' seeking cyber insurance to compensate them in case of attack. A recent report stated that insured cyber losses of $1.8 billion in 2019 increased up by almost 50%.

There was a time not so long ago when businesses were able to obtain cybersecurity insurance without following any specific cybersecurity practices as a prerequisite. Given the sharp rise in the severity of cyberattacks over the last few years – and the corresponding growth of cyber insurance claims being filed – this is generally no longer the case. Colonial Pipeline, for instance, filed a claim with its cyber insurance carrier for the $4.4 million ransom it paid to its attackers. With huge claims such as this rolling in, it's no surprise that cyber insurance providers are demanding at least basic security hygiene from their customers.

Indeed, in today's heightened threat landscape, insurance providers are closely scrutinizing applicants and their existing security policies and enforcing more stringent guidelines for businesses seeking cybersecurity insurance. After President Joe Biden signed an Executive Order on improving the nation's cybersecurity earlier this year, multi-factor authentication (MFA) was mandated for all federal agencies in the United States. This further encouraged cyber insurance companies to also mandate MFA as a base requirement to get coverage for a cyberattack.

MFA increases security by minimizing the possibility of unauthorized access. An MFA-protected system is much harder to hack than one protected by passwords alone. This is especially true because humans are inherently terrible at creating and remembering passwords that are difficult to crack.

MFA alone is not a panacea, but it can very significantly lower an organization's cyber risk level. Considering its substantial impact, combined with the relative ease of enabling MFA, this added layer of authentication is becoming a baseline security feature rather than an add-on. Organizations that have not yet implemented MFA for its security benefits will be increasingly forced to do so if they wish to purchase cyber insurance.

SIM2K can help you with applying MFA for your organization, and in turn, assist with applications for cyberinsurance, auditing your network for compliance with the carrier's requirements. Call us for details.

New Encryption Standards

The National Institute of Standards in Technology (NIST) has completed the third round of the Post-Quantum Cryptography (PQC) standardization process, which selects public-key cryptographic algorithms to protect information through the advent of quantum computers. A total of four candidate algorithms have been selected for standardization, and four additional algorithms will continue into the fourth round.

After careful consideration during the third round of the NIST PQC Standardization Process, NIST has identified four candidate algorithms for standardization. NIST will recommend two primary algorithms to be implemented for most use cases: CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures). In addition, the signature schemes FALCON and SPHINCS+ will also be standardized.

CRYSTALS-KYBER (key-establishment) and CRYSTALS-Dilithium (digital signatures) were both selected for their strong security and excellent performance, and NIST expects them to work well in most applications.

FALCON will also be standardized by NIST since there may be use cases for which CRYSTALS-Dilithium signatures are too large.

SPHINCS+ will also be standardized to avoid relying only on the security of lattices for signatures. NIST asks for public feedback on a version of SPHINCS+ with a lower number of maximum signatures.

NIST will create new draft standards for the algorithms to be standardized and will coordinate with the submission teams to ensure that the standards comply with the specifications. As part of the drafting process, NIST will seek input on specific parameter sets to include, particularly for security category 1. When finished, the standards will be posted for public comment. After the close of the comment period, NIST will revise the draft standards as appropriate based on the feedback received. A final review, approval, and promulgation process will then follow.

For the algorithms moving on to the fourth round, NIST will allow the submission teams to provide updated specifications and implementations (“tweaks”). The deadline for these tweaks will be October 1, 2022. Any submission team that feels that they may not meet the deadline should contact NIST as soon as possible. NIST will review the proposed modifications and publish the accepted submissions shortly afterward. As a general guideline, NIST expects any modifications to be relatively minor. The fourth round will proceed similarly to the previous rounds.

NIST will hold a 4th NIST PQC Standardization Conference on November 29 – December 1, 2022. The conference details have not yet been finalized.

The need for advanced protection of data is important as the attacks by cybercriminals get more sophisticated. NIST’s advancements on new standards is necessary in advance of new technology to protect data from day one, not in “catch-up” mode.

(Ok, Editor’s geek moment. On Star Trek, the starship Enterprise warp drive was powered by – wait for it – “dilithium crystals.” So ‘60s TV culture lives on in today’s tech world. Are we surprised?)

Hackers Target Healthcare

Of all the industries in the country, health care might be the juiciest for cyberhackers. And around central Indiana, institutions large and small are paying the price.

In the past few years, some of the region’s largest health care players – including Indiana University Health, Eskenazi Health and Elevance Health (formerly Anthem Inc.) – have seen patient or customer information compromised by hackers. So have some of the area’s smaller hospitals, including Hancock Health and Johnson Memorial.

Hospitals, health insurers and medical clinics are loaded with patient and employee data that can be mined for identity and medical theft. Hackers can shut down computer systems for days or weeks, holding hospitals hostage until ransom is paid.

One of the latest attacks became public in June when the Maine Attorney General’s Office disclosed that a software vendor to Indiana University Health and nine other U.S. health systems was attacked. The vendor, MCG Health, told authorities an “unauthorized party” obtained names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, birthdates and gender information for 1.1 million patients of about 10 hospital clients.

IU Health, the largest hospital system in Indiana, said it notified 60,000 patients about the breach, but declined to reveal details or answer further questions. “Because this is MCG’s data breach, we recommend you contact them for information. They would have specific details relating to the breach,” IU Health said in a brief statement.

MCG, based in Seattle, did not respond to e-mails and phone calls from local media. Multiple class action lawsuits have been filed against the software company, a subsidiary of Hearst Health, in a federal district court in Washington state. The lawsuits allege negligence, invasion of privacy, breach of confidence and violations of consumer protection laws. IU Health and the other hospital systems were not named as defendants.

Nationally, cybersecurity breaches in the health care sector hit an all-time high in 2021, with nearly half of all hospitals in the country reporting an attack, according to a report from cybersecurity company Critical Insights. All those attacks exposed protected health information for a record number of patients. In 2021, 45 million people were affected by health care attacks, up from 34 million in 2020, according to Fierce Healthcare, a trade news site. And it’s not just hospitals that are feeling the heat. Attacks against health plans jumped nearly 35% from 2020 to 2021. And attacks against business associates, or third-party vendors, increased nearly 18% from 2020 to 2021.

In fact, a SIM2K employee’s family was recently notified that a breach occurred at a local large medical practice that may have exposed personal information, and offered a year’s monitoring. So hackers can strike anywhere and anyone.

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.

Wi-Fi 7 is Coming

Intel is planning to install its next-generation Wi-Fi 7 (802.11be) technology in devices by 2024. Wi-Fi 7 is the successor to Wi-Fi 6E (802.11ax), bringing two times faster data processing speeds of 5.8 Gbps and more stable 6 GHz bandwidth stability, as well as support for up to 36 Gbps when working with data.

Intel plans to expand its Wi-Fi 7 development efforts ahead of its introduction to the market in 2024 and intends to apply its technology predominantly in laptops before expanding to other devices.

“We are currently developing Intel’s Wi-Fi ‘802.11be’ in order to obtain the Wi-Fi Alliance certification, and it will be installed in PC products such as laptops by 2024. We expect it to appear in major markets in 2025,” a vice president in Intel’s wireless solutions division, said at a recent press conference in Asia.

“Wi-Fi 7 almost doubles the frequency bandwidth of 802.11ax (170 MHz) to 320 MHz and doubles the speed of Wi-Fi. Since there is more than a year left before the release of 802.11be, there is still a chance that we could improve the processing speed even further,” he added.

Also coming is multi-link operation (MLO) technology. MLO aggregates multiple channels on different frequency bands at the same time to allow network traffic to still flow seamlessly even if there is interference or congestion on the bands.

Meanwhile, Apple is on the cusp of transitioning its devices to Wi-Fi 6E. While it was heavily rumored to debut with the iPhone 13 lineup last year, Apple has yet to release any devices with support for Wi-Fi 6E. That is expected to change this year starting with the iPhone 14.

Apple’s long-rumored mixed-reality headset is also expected to feature Wi-Fi 6E. An Apple analyst said that head-mounted display devices in 2022, 2023, and 2024 will offer Wi-Fi 6/6E, Wi-Fi 6E/7, and Wi-Fi 7, respectively, but it is unclear if this information was related to Apple’s product roadmap specifically.

Wi-Fi 6E offers the features and capabilities of Wi-Fi 6, including higher performance, lower latency, and faster data rates, extended into the 6 GHz band for processing speeds of 2.4 Gbps. The additional spectrum provides more airspace beyond existing 2.4GHz and 5GHz Wi-Fi, resulting in increased bandwidth and less interference.

Last year, the FCC adopted rules that make 1,200 MHz of spectrum in the 6 GHz band available for unlicensed use in the United States, paving the way for the introduction of new devices with Wi-Fi 6E support. Several other companies, like Broadcom and Qualcomm, are also rolling out Wi-Fi7 products in the near future.

It will be interesting to see actual “in the field” performance of these Wi-Fi7 products when actually released. SIM2K will evaluate this technology and keep you informed.

“Random Tid-Bytes”

Microsoft Finds Russian Cyber Spies

Russian hackers have engaged in “strategic espionage” against governments and other groups in 42 countries supporting Ukraine, according to a Microsoft report. Nearly 2/3 of the targets were NATO members. Half of the organizations targeted are government agencies and 12% are humanitarian groups. Telecommunications, defense and energy companies were also targets. Microsoft also noted an increase in Russian disinformation and propaganda, a 216% increase in Ukraine and 82% in the US. Microsoft did note that Ukraine has set an example in data safeguarding, moving data stored in servers in governmental buildings – vulnerable to bombing attacks – to the Cloud in data centers across Europe.

SIM Swapping Latest Scam

A new scam known as SIM swapping has led to people having their bank accounts cleaned out without their knowledge. It happens when hackers first steal your personal information online, then contact your mobile phone carrier and trick them into activating a SIM card. Once that occurs, the scammers can get control over your phone, passwords and pretty much everything else. Pretending to be you, the scammer then contacts your bank and transfers all the cash out of your account. Many people now have a banking app on their phone, with stored user ID and passwords, making this an easy task for the scammer. Here are some ways to protect yourself:

- If you receive a one-time passcode you didn’t request, don’t give the code to anyone who contacts you for it.
- Use known links to access businesses online.
- Verify any phone, text or e-mail contacts are legitimate before sharing information such as your account number, security word, PIN, User ID or password.
- Be leery of requests to download apps to fix issues or that allow access to your device.

SIM2K recommends using tools like our Duo multi-factor authentication for added protection against unauthorized access to accounts. Call us for more information.

Android Payment System Hacked

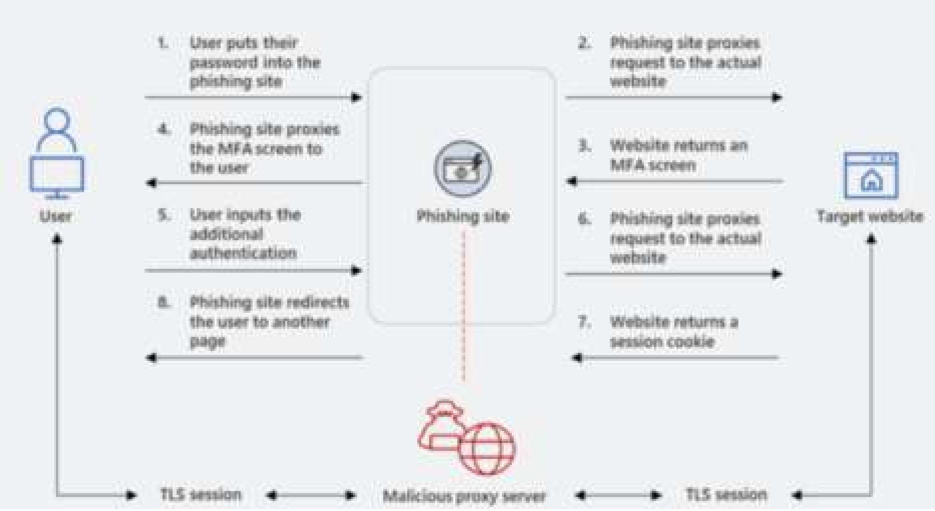
A security firm revealed hackers had access to dashboards used to remotely manage and control thousands of credit card payment terminals from digital payments giant Wiseasy, a popular Android-based payment terminal maker used across the Asia-Pacific region. Wiseeasy’s cloud service can remotely manage, configure and update customer terminals over the internet. Employee passwords used for accessing Wiseasy’s cloud dashboards – including an “admin” account – were found on a dark web marketplace. The report showed two cloud dashboards that were not protected with basic security features like two-factor authentication allowing hackers to access 140,000 Wiseasy payment terminals around the world. The “admin” user gave remote access to Wiseasy payment terminals and allowed anyone to view names, phone numbers, e-mail addresses and access permissions, including the ability to add new users. Payment systems are targeted by hackers with the aim of skimming credit card numbers for committing fraud. Wiseasy says it has added 2FA among other steps to protect users.

Can MFA Be Hacked? Maybe...

Microsoft has detailed an ongoing large-scale phishing campaign that can hijack user accounts when they're protected with multi-factor authentication measures designed to prevent such takeovers. The threat actors behind the operation, who have targeted 10,000 organizations since September, have used their covert access to victim email accounts to trick employees into sending the hackers money.

Multi-factor authentication – also known as two-factor authentication, MFA, or 2FA – is the gold standard for account security. It requires the account user to prove their identity in the form of something they own or control (a physical security key, a fingerprint, or face or retina scan) in addition to something they know (their password). As the growing use of MFA has stymied account-takeover campaigns, attackers have found ways to strike back.

Microsoft observed a campaign that inserted an attacker-controlled proxy site between the account users and the work server they attempted to log into. When the user entered a password into the proxy site, the proxy site sent it to the real server and then relayed the real server's response back to the user. Once the authentication was completed, the threat actor stole the session cookie the legitimate site sent, so the user doesn't need to be re-authenticated at every new page visited. The campaign began with a phishing e-mail with an HTML attachment leading to the proxy server.


1. User puts their password into the phishing site
2. Phishing site proxies request to the actual website
3. Website returns an MFA screen
4. Phishing site proxies the MFA screen to the user
5. User inputs the additional authentication
6. Phishing site proxies request to the actual website
7. Website returns a session cookie
8. Phishing site redirects the user to another page
User
Phishing site
Target website
TLS session
Malicious proxy server
TLS session

To keep the hacked employee from discovering the compromise, the threat actors created inbox rules that automatically moved specific e-mails to an archive folder and marked them as read. Over the next few days, the threat actor logged in periodically to check for new e-mails.

"On one occasion, the attacker conducted multiple fraud attempts simultaneously from the same compromised mailbox," Microsoft reported. "Every time the attacker found a new fraud target, they updated the Inbox rule they created to include these new targets' organization domains."

The report shows how easy it can be for employees to fall for such scams. The sheer volume of e-mails and workload often makes it hard to know when a message is authentic. The use of MFA already signals that the user or organization is practicing good security hygiene. One of the few visually suspicious elements in the scam is the domain name used in the proxy site landing page. Still, given the opaqueness of most organization-specific login pages, even the sketchy domain name might not be a dead giveaway.

Nothing in Microsoft's account should be taken to say that deploying MFA isn't one of the most effective measures to prevent account takeovers. That said, not all MFA is equal. One-time authentication codes, even when sent by SMS, are far better than nothing, but they remain phishable or interceptable through more exotic abuses of the SS7 protocol used to send text messages.

The most effective forms of MFA available are those that are compliant with standards set by the industry-wide FIDO Alliance. These types of MFA use a physical security key that can come as a dongle from companies like Yubico or Feitian or even an Android or iOS device. The authentication can also come from a fingerprint or retina scan, neither of which ever leave the end-user device to prevent the biometrics from being stolen. What all FIDO-compatible MFA has in common is that it can't be phished and uses back-end systems resistant to this type of ongoing campaign.

FIDO authentication is based on the use of public/private key pairs. When a user registers with a site, the FIDO authenticator generates a unique key pair for that user for that site. The site gets the public key, and the private key stays with the client authenticator. When a user authenticates with a site, the site sends a challenge to the authenticator. The first thing the authenticator does is make sure the name of the site (the origin) matches the name of the site the user registered with. If they don't match, the authentication fails. For example, if the user registered with goodbank.com and got a phishing request from g00dbank.com, the authentication would fail because the site names don't match. Origin spoofing is protected by HTTPS.

If the site names match, the user unlocks the private key in the authenticator with their biometric (or PIN), and the private key is then used to sign the challenge and send the response to the site. The site then compares the signed response with the public key it got during registration to ensure the response came from the correct user. No secrets are sent during the authentication process, so there are no credentials to reuse.

If the authenticator uses biometrics, there is no risk of phishing because the biometrics comparison is done locally, and the result is only used to unlock a FIDO credential (private key). The biometric data is not shared with the site and is not used as an authentication credential itself.

Use of some secondary authentication, be it 2FA or biometrics, is becoming a "bare minimum" standard for security in today's environment (as discussed in the Insurance story on page 1.) Obviously the cybercriminals are seeking ways to circumvent this protection, as Microsoft reports, but this is an isolated case that, now detected, can be countered by security experts. Call SIM2K for more information on multi-factor authentication techniques and what may be best to protect your company's digital assets.

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