SIM2K
Adapting Technology to Your Business Needs

5•21
Information you can use

SIMformation

Password Hall of Shame – 2020

A quiz: What has been the most popular — and therefore least secure — password every year since 2013? If you answered "password," you'd be close. "Qwerty" is another contender for the dubious distinction, but the champion is the most basic, obvious password imaginable: "123456." The full top 10 list includes:

123456
123456789
picture1
password
12345678
111111
123123
12345
1234567890
senha (Portugese for 'password')

Many employees have password fatigue, which in turn leads to lax password security. A study finds that users at larger companies (1,001 to 10,000 employees) have on average 25 passwords with which to contend. The problem is more acute for users at small businesses (25 or fewer employees), who have on average 85 passwords to juggle.

So how do you put in force strong passwords? There are three main ways in which passwords are compromised – guessing (by a human), cracking (by algorithmic brute force), and capturing (by gaining access to someplace where a password has been stored, whether that's in a database or on a sticky note). Each of the following techniques attempts to mitigate against one or more of those methods; for instance, passwords with personal information in them are easier to guess, and shorter passwords are easier to crack. Here are some tips:

Require the use of multifactor authentication (MFA). MFA factors include what you know (a password), what you have (a device, such as a smartphone), and who you are (a fingerprint or facial recognition scan). Using MFA to require verification, such as a code sent to a mobile device, in addition to the use of strong, unique passwords, can help provide better enterprise protection.

Don't let users create passwords with dictionary words. In a brute-force dictionary attack, a criminal uses software that systemically enters every word in a dictionary to figure out a password. To thwart such attacks, many experts recommend against using words that exist in a dictionary.

Length matters, and phrases are longer than words. That said, a longstanding emphasis on "special" characters that aren't found in normal words may be ignoring the bigger picture. Instead, "Length is strength," as longer passwords are much harder to break, cryptographically speaking, than shorter ones even when special characters are involved. A password like 'AN3wPw4u!' is much easier for an automated cryptographic cracker than a password like 'SnowWhiteAndTheSevenDwarves.'"

Steer users away from passwords that include information about them. Don't use the names of a spouse, pet, city of residence, birthplace or any other personally identifiable information in a password, as that information could be deduced from the user's social media accounts. A hacker is much more likely to guess your 'pet's name + 1234' as your password than they are to figure out a longer passphrase such as "ImgoingtorunBostonMarathon2022" that is tied to your personal goals but doesn't include easily researched personal info.

Educate users on what makes a strong password. A strong password doesn't appear anywhere else in the public realm (such as in dictionaries), doesn't appear anywhere in private (such as other accounts users have), and contains enough random characters that it would take an eternity to guess the password, even when using brute-force techniques.

Regularly perform password audits. Ideally, your organization should use an authentication system that allows for password audits. Look for things like passwords being reused across employees or use of common words or common words with simple character replacements.

Encourage users to vet their own passwords. There are a number of resources that will allow users to investigate how safe a potential password is before they put it into use. For instance, My1Login's Password Strength Test, which tells you how long it would take a typical algorithm to crack your password, or Have I Been Pwned?, which compares your password against a wide database of hacked credentials circulating on the dark web.

Security experts recommend giving users the option to make passwords visible when they're being entered; this makes users more likely to come up with longer and more complex passwords, which more than balances out the chance that someone might read the password over the user's shoulder. And asking for frequent password changes may lead to issues as the user will make minor substitutions to the base password, such as changing an "s" to "$" and not creating anything new.

The overall lesson is that your password policies need to evolve, just like the rest of your security program. SIM2K can help you with setting a password policy for your employees that will be easily managed yet offer protection against hacks and good guesses.

Cyber Insurance Market Tightening

SIM2K has been seeing a drastic change in the length, complexity and products mentioned in cybersecurity questionnaires we help clients fill out. For example, the old questionnaire was 4-5 questions – now it is up, in some cases, to 40 or more questions. Healthcare seems to be particularly affected, but law and financial services are being targeted as well.

We also had our first example of an insurance company hiring a 3rd party and "surprise auditing" the client's publicly facing hosts. In this case, an organization was running IIS 7 (which is Windows Server 2008, no longer supported as of January 2020,) on a system we do not maintain. To SIM2K, this marks a new chapter in "enforcement" of those policies which we would expect to continue and eventually be penalties levied and/or non-renewed coverage for lack of compliance.

In this case, the client received the following notification from the 3rd party security company conducting the audit:

> *"This email provides an alert authorized by your cyber insurance company, Tokio Marine HCC. We believe you may be running unpatched software with critical vulnerabilities that exposes your operations to cyber-attacks. We are contacting you with the hopes of getting your immediate attention to this matter. Please reach out to your insurance broker if you suspect this email is not legitimate.*
>
> *Here's a bit of background and more detail that may help you. As part of your cyber insurance policy, Tokio Marine HCC has retained us to perform regular, non-intrusive scans of your internet-facing systems and applications, looking for certain vulnerabilities. This service benefits everyone by allowing you to fix any problems before hackers have attacked. We found indications you are running unpatched software with high-risk vulnerabilities. Please know due to issues with certain systems/software, false positives are possible; our scanning is only external – we can't see inside your network, so only you can verify the status of the software found unpatched."*

Todd Carbrey, of NSB Insurance in Carmel, noted that carriers are becoming more concerned about best practices for their policy-holders. "Just like insuring a building – you look for locks, alarms and cameras. Carriers want to see that your network is similarly protected." He noted that carriers are now drilling down further on levels of protection, for example, Two-Factor Authentication is now pretty much a baseline in coverage.

But, Todd also said that the audit discussed above is not yet the norm. "Most carriers want to work with clients in a partnership and help identify potential problems and be proactive in solutions, not play 'gotcha'. Working through an application for cyber insurance can be a great way to look at your security profile and spotlight areas where you can improve." And, if you are a policyholder, asking for an audit could help you get a discount on your cyber insurance policy.

No company is "to small" to escape being targeted by ransomware or other hacks. Malware is not just stealing credit card numbers or personal information, it can also be a virus that compromises your production line or freezes your shipping department. SIM2K will work with you and your insurance carrier and agent to strengthen your organization's security profile. Call Ben for more resources on cyberinsurance.

Password Manager Compromised

A common refrain among digital security professionals is for users to rely on the services of a strong password manager for their myriad account credentials online. Because, in lieu of that, too many people default to the convenience of memory and reuse passwords or create too many that are easily memorable (and, thus, easily guessable for hackers).

While using a password manager can be a strong deterrent for hackers, the downside is that the password manager program is then a target for hackers. Once "in" to the manager, it is a "target rich" environment for names, accounts and passwords for anyone relying on that site for passwords. And, as could be expected, enterprise password manager Passwordstate has reported a recent security incident.

As the company explains it, hackers apparently compromised a software upgrade that went out to customers last week. A malicious version of an otherwise legitimate update file was installed that would have been able to extract customer data for the attackers.

Passwordstate's advisories say the number of affected customers looks to be small, but it still doesn't hurt to assume that your password or passwords were included in this incident and to take this opportunity to just go ahead and change them anyway. By the way, data that may have been compromised in this incident includes things like usernames and passwords, as well as various other details about users and their systems. So if your company uses Passwordstate, you should have been notified, and if not, SIM2K recommends changing your stored passwords immediately.

Also troubling is a hack on a software auditing company, Codecov. Their software is used to help companies test their own software code for errrors and potential vulnerabilities that hackers could exploit. The breach supposedly took place in January but was just discovered in April. This means that the hackers had plenty of time to tamper with Codecov's software and inject their own back doors into software or to cover up Codecov's detection of their presence and thus let them roam free into a company's data. This is similar to the SolarWinds hack earlier this year that compromised their security audit software, giving the hackers a way to work around the defenses that SolarWinds would use to root out malware.

These exploits are a reminder that no digital system is impenetrable. While password managers are still better than relying on simple and memorable passwords that you come up with yourself, they are not infallible, nor is software designed to thwart the "bad guys" when the security company's own files are hacked. Security requires constant monitoring and layers of defenses. Call SIM2K for more information on password management programs and how we can strengthen your defenses against possible hacks.

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.

Something Fishy Going On

Secure your PC. Secure your laptop. Secure your smartphone. And now, secure your fish tank. What, you say? A fish tank?!

That was the lesson learned from the operators of a North American casino. According to a security expert, "The attackers used (a fish-tank thermometer) to get a foothold in the network. They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud."

Is this possible? It certainly is, thanks to the Internet of Things (IoT). We have discussed the IoT in SIMformation in the past, but as a refresher, this is the term for devices like machinery, elevators, appliances and vehicles that have some sort of sensor or can connect to the Internet. And apparently, that includes fish tank thermometers, as well. It is estimated that by 2025 there will be 31 billion connected devices worldwide. Some consider this is a good thing, because the "smarter" you make these objects, the more information we can glean from them to ward off issues and optimize their use. Rolls Royce is using IoT airplane engines to report performance data on the fly. ThyssenKrupp is creating "smart buildings" by connecting their elevators to monitoring stations to warn of potential problems. And many climate monitoring systems, alarms and such are IoT-enabled. Same for manufacturing robots and other machine tools – and apparently the temperature of water in a fish tank. After all, those huge tanks in casinos can be tough to manage 24/7.

But all of these connected devices are creating an enormous opportunity for hackers. That's because many of them aren't equipped with the kinds of security protections seen in laptops, servers, phones and tablets. And unfortunately, many companies are not aware of the risks. The industrial sector is facing a new set of challenges when it comes to securing an IT-OT environmennt. Cybersecurity used to be focused just on IT assets like servers and workstations, but now this increased connectivity requires expanding knowledge of all devices that might touch your network.

So how do business owners address this problem? The only tactic is just to stay ahead of it. Which is why it is important to do a complete assessment of your network security. And you need to make sure that such an assessment includes evaluating any and every connected device. That means building heating controls, smart speakers, smoke detectors, alarm systems, overhead lighting and even the coffee machine in the break room. SIM2K can work with you to conduct these assessments and identify any device that might be connecting to your network. From there, we can help put in proper security to protect your network and company data.

And that includes the fish tank.

"Random Tid-Bytes"

Congratulations to our Nick Bartolone!

SIM2K congratulates Nick on having completed the qualifications to be a Zultys Certified Systems Expert. This means Nick is now certified to install and support our Zultys Unified Communications clients and their VOIP phone systems. Nick joins Ben, Fred and Chris as ZCSE's so we have a full complement of Zultys-qualified systems engineers to back you up.

Improvements To Our E-Mail Security

In the coming weeks, new capabilities are being introduced to SIM2K's Hosted Exchange e-mail security service to provide enhanced protection against targeted attacks using artificial intelligence (AI) technology for your customer sub-accounts. These capabilities are provided by a new "AI Guardian" option that will be included with our Hosted Exchange e-mail protection. As part of our cutting-edge email protection strategy, we are integrating an innovative third-party AI-based security engine into our e-mail protection service that will review patterns and structure in each user's email communications to help identify phishing and other types of targeted attacks. You will be notified when the AI Guardian capability has been enabled for your account. No action is required on your part to activate AI Guardian. When AI Guardian is activated for your Exchange, additional tags will be applied to suspicious e-mails to notify and educate users about potential threats. AI Guardian is an option and can be disabled if you so desire, but SIM2K recommends accepting this added level of security on your Exchange accounts. Call us if you have any questions or concerns.

LinkedIn Hack Releases Half-billion Names

We just dealt with a massive Facebook data leak, and now LinkedIn is reportedly facing a similar situation. An archive containing data purportedly scraped from 500 million LinkedIn profiles has been put for sale on a popular hacker forum, with another 2 million records leaked as a proof-of-concept sample by the post author. The four leaked files contain information about the LinkedIn users whose data has been allegedly scraped by the threat actor, including their full names, e-mail addresses, phone numbers, workplace information, and more. While users on the hacker forum can view the leaked samples for about $2 worth of forum credits, the threat actor appears to be auctioning the much-larger 500 million user database for at least a 4-digit sum, presumably in bitcoin. The author of the post claims that the data was scraped from LinkedIn and investigators have been able to confirm this by looking at the samples provided on the hacker forum. LinkedIn states the data for sale was not acquired as result of a data breach, but rather, is "an aggregation of data from a number of websites and companies." However, if you are a LinkedIn member, you may wish to change your password immediately.

Facebook Workplace Adds Features

Facebook announced new updates to its Workplace enterprise social network, including new video features and improved integrations with third-party applications. This includes a Live Q&A feature where a presenter can obtain details of the person asking a question to better personalize the response. Facebook also now integrates with Cisco's Webex video platform offering the ability to broadcast directly into Workplace's Live video feature without switching apps. Other updates include the ability to sync Workplace events with external calendar tools, including Outlook and Gmail.

Government Secretly Accesses Private Networks

A court-approved FBI operation was conducted to remove web shells from compromised US-based Microsoft Exchange servers without first notifying the servers' owners.

As we have discussed in past issues of SIMformation, on March 2nd, Microsoft released a series of Exchange security updates for vulnerabilities being exploited by a hacking group. Collectively known as ProxyLogon, these exploits installed web shells on compromised Exchange servers that provided remote access to the servers used to exfiltrate e-mail and account credentials.

Over the following weeks, government agencies released guidance, and Microsoft released a variety of scripts and tools to help victims determine of they had been compromised and to remove these web shells. SIM2K was quick to follow Microsoft's guidelines and installed these patches on all our hosted Exchange accounts.

However, other threat actors began using the Microsoft Exchange vulnerabilities to install ransomware, cryptominers and further web shells on those servers that were not patched.

In a Department of Justice press release, the FBI states they used a search warrant to access the still-compromised Exchange servers, copy the web shell as evidence, and then remove the web shell from the server.

The FBI requested this warrant because they believed that the owners of the still-compromised web servers did not have the technical ability to remove them on their own and that the shells posed a significant risk to the victim.

"Based on training and experience, most of these victims are unlikely to remove the remaining web shells because the web shells are difficult to find due to their unique file names and paths or because these victims lack the technical ability to remove them on their own," the FBI stated in an affidavit in support of a search warrant.

As there was concern that notifying the owners of these servers could compromise the operation, the FBI requested that the warrant be sealed and that notification of the warrant be delayed until the operation was finished.

"Accordingly, the United States requests approval from the Court to delay notification until May 9, 2021, 30 days from the first possible date of execution on April 9, 2021, or until the FBI determines that there is no longer need for delayed notice, whichever is sooner," the affidavit requested.

They further requested permission to search at any time of the day to avoid detection by threat actors. "Because accessing such computers at all times will allow the government to minimize the likelihood of the actors' detection and deployment of countermeasures that could frustrate the authorized search, good cause exists to permit the execution of the requested warrant at any time in the day or night," states the affidavit.

To clean the identified Microsoft Exchange servers, the FBI accessed the web shell using known passwords utilized by the threat actors, copied the web shell as evidence, and then executed a command to uninstall the web shell from the compromised server.

"FBI personnel will access the web shells, enter passwords, make an evidentiary copy of the web shell, and then issue a command through each of the approximately web shells to the servers to delete the web shells themselves," the FBI explained in the affidavit.

A court in Houston granted the search warrant on April 9th and permitted the FBI to remove web shells from the listed Exchange Server over the next 14 days. The court also allowed the FBI to delay providing notice to the Exchange Servers' owners being searched. The DOJ stated that this operation was successful and hundreds of web shells were removed from compromised Exchange servers.

However, the FBI stated that the operation only removed web shells and did not apply security updates or remove any other malware that threat actors may have installed on the server.

The FBI is now in the process of notifying victims whose Exchange servers were accessed during the operation. The FBI will send these notifications via email from an official FBI.gov e-mail account, or if contact information is not available, by using a service provider (ISP) to contact the victim.

"(Today's) court-authorized removal of the malicious web shells demonstrates the Department's commitment to disrupt hacking activity using all of our legal tools, not just prosecutions," said Assistant Attorney General John C. Demers for the Justice Department's National Security Division. "Combined with the private sector's and other government agencies' efforts to date, including the release of detection tools and patches, we are together showing the strength that public-private partnership brings to our country's cybersecurity. There's no doubt that more work remains to be done, but let there also be no doubt that the Department is committed to playing its integral and necessary role in such efforts."

"This operation is an example of the FBI's commitment to combatting cyber threats through our enduring federal and private sector partnerships," said Acting Assistant Director Tonya Ugoretz of the FBI's Cyber Division. "Our successful action should serve as a reminder to malicious cyber actors that we will impose risk and consequences for cyber intrusions that threaten the national security and public safety of the American people and our international partners. The FBI will continue to use all tools available to us as the lead domestic law enforcement and intelligence agency to hold malicious cyber actors accountable for their actions."

However well-intentioned the actions of the government, it is still a gray area if any entity can breach a private computer network and modify any software without prior notification. And, the fact that the FBI could conduct this operation without consent and using "known passwords" is disturbing as it sets a precedent for conducting subsequent intrusions into private networks. It is one thing when a hacker is moving through your software, let alone it being the federal government. Just saying.

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