ISSUE
07
July
2020

MONTHLY
TECH TIPS

TechTalk

2FA Reduces the Chance of an Account Breach by 99%.

About a year ago, Alex Weinert from Microsoft wrote an article that had some great points.

Weinert said that old advice like "never use a password that has ever been seen in a breach" or "use really long passwords" doesn't really help.

He should know. Weinert was one of the Microsoft engineers who worked to ban passwords that became part of public breach lists from Microsoft's Account and Azure AD systems back in 2016. As a result of his work, Microsoft users who were using or tried to use a password that was leaked in a previous data breach were told to change their credentials.

this issue

The use of 2FA is More Important Than Ever.

According to Microsoft, there are over 300 million fraudulent sign-in attempts to their cloud services every day.

All it takes is one compromised credential or one legacy application to cause a data breach. This underscores how critical it is to ensure password security and strong authentication.

The SANS Institute stated recently that the most common vulnerabilities include:

Business email compromise:
where an attacker gains access to a corporate email account, such as through phishing or spoofing, and uses it to exploit the system and steal money. Accounts that are protected with only a password are easy targets.

Legacy protocols:
These can create a major vulnerability because applications that use basic protocols, such as SMTP, were not designed to manage Multi-Factor Authentication (MFA).

So even if you require 2FA, attackers will search for opportunities to use outdated browsers or email applications to force the use of less secure protocols.

Password reuse:
Common passwords and credentials compromised by attackers in past breaches are used against corporate accounts to try to gain access. Considering that up to 73 percent of passwords are duplicates, this has been a successful strategy for many attackers and it is easy to do.

They both agree that best thing to do is to turn on 2FA. This provides an extra barrier and layer of security that makes it incredibly difficult for attackers to get past and can block over 99.9 percent of account compromise attacks.

More Here:
https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ

Advanced Systems Solutions Inc.

Configuring IPsec Virtual Private Networks

"VPNs are essential for enabling remote access and connecting remote sites securely. However, without the proper configuration, patch management, and hardening, VPNs are vulnerable to many different types of attacks.

NSA Releases Guidance for Securiing Spsec Virtual Private networks

(click here for details)

To ensure that the confidentiality and integrity of a VPN is protected, reduce the VPN gateway attack surface, always use CNSSP 15-compliant cryptography suites, avoid using vendor defaults, disable all other cryptography suites, and apply patches in a timely manner. Following the steps identified in this paper will ensure the most secure VPN configurations."

A Note from the National Security Agency

The NSA released guidance this week suggesting that only CNSSP 15-compliant algorithms be used for VPN access.

VPNs are essential for enabling remote access and securely connecting remote sites, but without proper configuration, patch management, and hardening, VPNs are vulnerable to attack.

Avoid using default VPN settings

Due to the complexity of establishing a VPN, many vendors provide default configurations, automated configuration.

Administrators should then remove any non-compliant ISAKMP/IKE and IPsec policies. As a best practice, administrators should not utilize any default settings and ensure that all ISAKMP/IKE and IPsec policies are explicitly configured for the CNSSP 15-compliant algorithms.

Remove unused or non-compliant cryptography suites

It is very common for vendors to include extra ISAKMP/IKE and IPsec policies by default. These extra policies may include non-compliant cryptographic algorithms. Leaving extra ISAKMP/IKE and IPsec policies as acceptable policies creates a vulnerability to downgrade attacks.

Verifying that only compliant ISAKMP/IKE and IPsec policies are configured and all unused or non-compliant policies are explicitly removed from the configuration mitigates this risk.

Apply vendor-provided updates

Implement a patch management policy.

Over the past several years, multiple vulnerabilities have been released related to IPsec VPNs. Many of these vulnerabilities are only mitigated by routinely applying vendor-provided patches to VPN gateways and clients. Many network equipment vendors allow customers to sign up for notification emails for new security alerts. These notifications are an excellent way to stay up-to-date on relevant out-of-cycle patches.

More Here:
https://bit.ly/ASSI_NSA

Areas for Review This Month

We recommend that you take this month to review legacy solutions.

Update fatigue is a real thing. Performing updates is never a fun task, but it is critical and is an effective way to strengthen your security posture.

In addition to performing patches, it is also important to not fall too far behind on your software versions.

A good example of this is that Office 2010 and 2016 for Mac will both expire in less than three months. This means that there will not be any further security updates released. Also update programs such as Adobe, 7zip, GoToMeeting, Zoom, and others. If you are not using a program anymore, simply uninstall it. ***Make sure you have license keys for any purchased software before removal.***

Monitoring

Face it, patching can be a huge pain in the ass if you are supporting multiple devices. For supporting an organization of more than 10 people, it can be obtrusive to the end-user trying to keep everything updated.

Try to consider using solutions that offer a management interface to view all devices. Using a single pane of glass to view all devices and see what version numbers are installed and if there have been any new additions.

There are much better uses of your time than spending it running to each computer manually!

Establish your baseline, add specialized departmental software, then plan to review the list on a schedule to ensure that all devices are compliant.

Most importantly, keep your firewall and switches up to date. All too often these devices are overlooked.

Let us know if you would like talk about patch fatigue, it is always free to talk!

This Month's Q&A Technology Tips

Q: Ryan from Richmond asks, "Is it true that I can use a VPN to purchase discounted airline tickets?"

A: Awesome question Ryan, thanks for asking!

By using a VPN to shop online, you can save on your airline ticket purchases and other items by changing your IP address to one in a different country. This is because airlines use local pricing, so a ticket in one country may be much cheaper than a ticket for the same flight in a different country.

Beware though, organizations are now monitoring which country is specified in a user's account settings, and only show prices in that country's currency. Using a VPN to disguise your location is against many online vendors Terms of Service, and could lead tc restrictions being placed on your account.

If you are an expat living abroad, keep these changes in mind so that you can plan to open a local bank accounts as needed.

Thanks again for the question Ryan, I hope this helps!

Have a question?

Ask us at - info@advancedsystemssolutions.com

EYE ON IT

The Hot Trend of July

The trend that we are seeing is an increased number of phishing attempts.

The attempts are increasingly sophisticated.

Recently we witnessed one where the domain name was changed ever so slightly.

They spoofed the name by using a single letter swap. Put that in the middle of a sentence and the odds are that most people will read right past it.

Implement a policy to ensure that communication is verified for financial transactions. A good policy will ensure that there is a second set of eyes, or some other mechanism, to ensure that requests are valid.

If a second person is not available, then a phone call should be made to verify each request.

Implementing a security Awareness program will help keep the team on the lookout for phishing attempts.

Stay Up to Date!

Don't forget to check out our additional tips to keep you secure! If you are not familiar with the new features is Edge, you will want to check out our guidelines for keeping your organization secure.

https://bit.ly/ASSI_Blog

Upcoming Events

- **FLGISA 2020 Annual Conference CANCELLED**

  As we are sure you have heard by now; the Florida Local Government Information Systems Association 2020 Annual Conference has been cancelled. We will miss seeing all of our friends and hope that everyone is staying safe.

  https://www.flgisa.org/events/

- **T2 Tech Talk Podcast**

  We know tech and marketing can be daunting, but we break it down into byte sized chunks.

  https://www.t2techtalkpodcast.com/

- **Orlando Power Lunch**

  The Orlando Power Lunch is a virtual luncheon that provides networking as well as tips from an informative speaker. August will feature Andy Young sharing his approach to finding and maintaining the ideal client so you won't want to miss this event!

  https://www.orlandopowerlunch.com

Tech Talk Issue 07 July 2020

Advanced Systems Solutions Inc.

1051 Winderley Place #307
Maitland, FL 32751
407-414-6626
www.advancedsystemssolutions.com