ISSUE
03
November
2019

MONTHLY
TECH TIPS

TechTalk

this issue

1.5 million new phishing sites are created every month. (Source: webroot.com)

The majority of data breaches are due to employee error.

The Internet continues to grow at a rate of 65% a year and we are just short of 2 billion websites. As the number of pages increase, so does the number of pages that are prone to infection. (www.websitehostingrating.com)

Team training is more important than ever. Make sure that your team is aware of social engineering and phishing scams.

Consider using solutions such as Cisco's "Umbrella" to monitor web traffic for team members that visit unknown websites for research.

Why the Increased Amount of Cyberthieves?

There is a new victim of ransomware every 14 seconds in 2019 and that is predicted to increase to every 11 seconds by 2021. **(Source: Cyber Security Ventures)**

The long time frustration criminals faced was how to pick up money without being traced.

Cryptocurrency has enabled for the first time in history to pick up a payment for a threat, extortion, blackmail, or ransom without being traced.

The issue of how to extort money was the equivalent of an unsolvable mathematic equation. Sometimes we will hear how some college prodigy has solved the mystery, well this is what has happened. Criminals now have a perfect way to extort money with very little fear of repercussion.

Cyberthieves are collecting well over $10billion this year, some are even boasting their retirement!

Here is where cyberthieves are really screwing up.
Recently, ASSI witnessed a large payment was made to cyberthieves, and the criminals provided a password to unlock the files. The password provided did not work and the criminals ceased all communication with the victims.

Many US companies refuse to pay a ransom. Why pay the money if the password might not work or if there is a possibility that your files will be locked again a week later?

A prime example of this lack of trust is told in the ransomware demand story for the City of Atlanta. The demand was for $51,000, which the City declined to pay and rather went on to spend an estimated $17 million in recovery costs.

Avoid the predicament of having to decide what to do in the heat of the moment and create your Disaster Recovery plan today!

Advanced Systems Solutions Inc.

What Does the CISA Do?

The Cybersecurity and Infrastructure Security Agency, CISA, is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

CISA Urges You To Be CyberAware During the Holiday Season

(click here for details)

CISA's National Cybersecurity and Communications Integration Center provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.

A Note from the U.S. Department of Homeland Security

Many Entities Share Tips and Tools That Help Increase Your Security Posture. The Department of Homeland Security is a Great Resource.

This month the CISA has highlighted increased activity from China and North Korea.

China is being highlighted for of their interests in obtaining details of American technologies. North Korea is making use of Malware such as the recent "Hidden Cobra."

Here are some tips to keep your organization secure.

Networks churn out massive amounts of event data, but most organizations do not review to the activity that these logs provide. Reason being is that it is very time consuming to corollate the data from all the various reports.

When Security Information and Event Management (SIEM) solutions first came to market, we were astounded by their ability to turn mountains of data into valuable insight. The issue was that the solutions were costly and required manual configurations.

Software as a Service and SIEM solutions are easier and more affordable than ever for businesses and their reports are gold.

These solutions allow you to corollate the data from all your network devices to see if cybercriminals are working to compromise your various devices and accounts.

Let me know if you have interest in discussing any of these solutions in depth, you know I love to talk technology!

Here are some more areas to consider when keeping yourself safe from outside threats:

- Implement 2FA

Four out of five data breaches could be avoided by using 2FA.

The majority of hacking-related breaches take place due to weak or stolen passwords. Since many users tend to use the same password everywhere, the risk grows tenfold when spear phishing is used.

- Principle of Least Privilege

Limit access rights for team members by assigning the bare minimum permissions they need to perform their work.

Limit service accounts to their respective tasks only and avoid granting all domain access.

- Logging

SolarWinds, Splunk, WhatsUpGold, all these solutions offer excellent analytics into the events that are happening within your network. Their ability to corollate data real-time is something that would take an IT team days to identify.

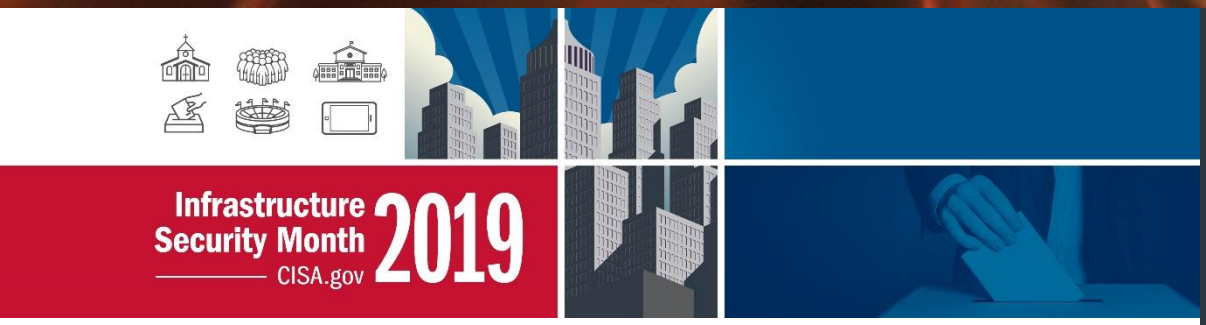
- User Account Activity

Monitoring of administrator accounts is critical on all network devices. A slow crawl of the network will avoid detection from traditional alerts. Consider the use of third-party software to provide oversight of the entire network.

- Firewall Settings

There are constant scans being performed from IP address all around the world. A bittersweet advantage of people sharing the details of compromised systems is that the IP addresses are identified.

Set your firewalls to block overseas traffic unless you have team members, clients, or residents who connect to your network from outside of the country.



Areas to Review This Month

November is Critical Infrastructure Security and Resilience Month, which focuses on the services we use such as power, water, transportation systems, first responders and hospitals, farms, stores, as well as the Internet and various communication systems.

One of the themes this year is "Managing risk to a converging cyber and physical world."

You can take the same steps that the CISA is focusing on to keep your organization running smoothly.

There are 4 areas of focus you can review:

Updates - Update your operating system and security software as soon as updates are available.

Online Passwords - Use complex passwords and don't share them. Make sure that all passwords are changed annually in the event of stale password lists being shared.

Training - Implement cyber training for employees. Provide education on what your employees can do to prevent phishing/ransomware attacks.

Soft Targets and Crowded Places.

In recent years terrorists and extremists have shifted tactics to focus on simple, low cost attacks using whatever is at hand.

Create the policies and procedures your organization needs to follow in an emergency and share the plan with staff and let them know what their roles are.

Ensure that all team members have alternative contact information for team leads.

This Month's Q&A Technology Tips

Q: Steve from Syracuse asks, "Why has there been such an increase of ransomware attacks this year?"

A: Spot on question Steve, thanks for asking!
Ransomware as a Service (RaaS) is largely to blame for the increase in numbers.
RaaS has been proven to be highly lucrative for cybercriminals without coding experience because the cyberthief doesn't need much capital or any technical expertise to start a campaign.

The operators provided a base ransomware executable that allows distributors to change the configuration: the types of files to target, the countries to target, the folders to encrypt, and other specifics. They also assist by suggesting how much ransom to charge victims in different countries. RaaS creators take a 20% cut of the profit, while the distributors get 80%.

Thanks again for the question Steve, I hope this helps!
Have a question? Ask us at info@advancedsystemssolutions.com

EYE ON IT

The Hot Trend of November

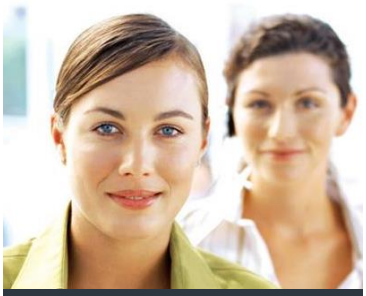
The trend that we are seeing is the increase of ransomware attacks.

Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

Ransomware can be devastating to an individual or an organization. Anyone with important data stored on their computer or network is at risk.

The important thing is that you prepare your data restoration plan now. Backup your data, then test your plan.

Don't forget the 3-2-1-Rule of Data Backups!



Stay Up to Date!

Don't forget to check out our additional tips to keep you secure! If you're not familiar with a Human Firewall you will want to check out our guides for keeping your organization secure.

http://bit.ly/ASSIBlog

Upcoming Events

- **Orlando Power Lunch Holiday Build.**

  Advanced Systems Solutions is proud to sponsor the Orlando Power Lunch. This month we are focusing on community involvement for the Holidays and have put together a team for a Holiday Build at Habitat for Humanity. Come join us!

  https://habitatorlando.rallybound.org/habitat-holiday-build/Team/View/123091/The-Grinch-Gang

- **T2 Tech Talk Podcast.**

  We have had some fantastic guests on the show lately, including experts who are at the top of their game. We know tech and marketing can be daunting, but we break it down into byte sized chunks. **https://www.t2techtalkpodcast.com/**

- **Microsoft Ignite Was Interesting as Always!**

  The Orlando event was a success! We look forward to sharing some of our thoughts in our December newsletter.

- **Enterprise Connect Registration is Still Open.**

  March 30th - April 2nd at Gaylord Palms. Come join us to see what the best options are for upgrading your communication solutions.

Tech Talk Issue 03 November 2019

Advanced Systems Solutions Inc.

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