E-NEWS

www.E-Safetech.om | 1-412-944-2402 |

November 2017

In this issue…

What is "serverless" computing?

Thanks to economies of scale, cloud computing resources are cheaper and more stable than those on a local area network, but the cloud is still made up of servers that require expert configuration. Serverless computing is one way to reduce management burdens.

What is it?

Outsourcing workloads to the cloud -- like websites and apps -- requires just as much hardware as if the computations were performed in an on-site server. The only difference is the location of the server.

Office 365 or Google Docs are great examples of this model. Thousands of servers are set up to run these apps so there is always enough capacity to handle the millions of people who use these apps at any given moment. Microsoft and Google need to manage and maintain these servers 24/7 to keep up with demand so they're always on and always ready to handle more workloads, even during off-peak hours.

Serverless computing changes everything by allowing developers to create apps and websites that use cloud resources only when they're needed. So, if you were to create a web app, you wouldn't need to pay for a dedicated cloud server. The cloud provider would host your app's programming code and run it only when a user requested it. The cloud provider would take care of allocating the appropriate resources and charge by the second for what you use.

Who can benefit from it?

Serverless computing is for users who use cloud resources for processing power. If you're using the cloud only to store files, serverless services aren't going to help you. However, if you use the cloud to process information and turn it into something more useful, serverless computing will help you immensely.

An everyday example of this is Amazon's Alexa. Every command the AI assistant responds to is nothing more than an app that sits dormant until a user tells Alexa to run it. Small businesses are creating apps in Amazon's cloud that can be processed by the voice assistant without the burden of setting up a dedicated server.

Serverless computing isn't about *getting rid of servers*; it's about using their raw computing power without being forced to fine tune them first. It falls under the umbrella of virtualization technology and is another step in the right direction for small businesses working with limited budgets.

For more information about how virtualization can help you lower costs and increase efficiencies, give us a call today.

Hackers Exploit Vulnerable Office Feature

As the world's most popular productivity suite, Microsoft Office tends to receive much attention from cybercriminals. Generally, hackers embed malware in authentic Office files to trick users into unleashing it onto their machines. However, the most recent exploit proves to be much more dangerous than any Office hack we've seen.

What's the new Office threat?

The Office exploit takes advantage of Microsoft's Dynamic Data Exchange (DDE), a protocol that sends messages and data between applications. For example, DDE can be used to automatically update a table in a Word document with data collected in an Excel spreadsheet.

The problem with this is hackers can create DDE-enabled documents that link to malicious sources rather than to other Office apps. Theoretically, this allows hackers to launch scripts that download Trojan viruses from the internet and execute it before the user is even aware of the attack.

And unlike most malware-embedded Office files, which are usually blocked by security protocols from Microsoft, DDE exploits are instant. Once a compromised Word file is opened, it automatically executes the hack.

Outlook at risk

What's even more alarming are the DDE vulnerabilities in Outlook. Recent reports found that hackers can embed malicious code in the body of an email or calendar invite, allowing them to perform phishing scams without a file attachment.

Fortunately, Outlook DDE attacks are not as automated as Word or Excel DDE attacks. Two dialog boxes will usually appear when you open the email asking if you want to update a document with data from linked files and start a specific application. Simply clicking 'No' on either of these boxes will stop the attack from executing.

Defending against DDE attacks

Beyond saying no, you can protect yourself by following these security best practices:

- Evaluate the authenticity of unsolicited emails before interacting with them and don't open attachments from unfamiliar contacts.
- View emails in plain text format to completely stop DDE attacks embedded directly in emails from running. Note that this will also disable all original formatting, colors, images, and buttons.
- Use a strong email security system that prevents phishing emails, spam, and other unwanted messages from reaching your inbox.
- Get in the habit of checking for Microsoft updates, as they're usually quick to release patches after vulnerabilities have been discovered.

Last but not least, consider working with our team. We're Microsoft Office experts who can keep you safe from the latest threats. Call us today to get started

A special VMware Lab Day this November! E-Safe is having a special VMware lab day for our customers on November 30th from 9am-11am at our office. Come spend the morning with us and learn from our experts as we cover great topics at this event.

Learn how to:

- Deploy and use VMware products that are free o Update Manger

o vSphere Replication

o vSphere Date Protection

- Optimize Windows operations systems for VMware

- Maximize reporting and notification functions from your vSphere environment

Register today to reserve your space at this upcoming event!

REGISTER HERE

Event Details

When and Where:

November 30th

9am-11am

E-Safe Office: 300 Bilmar Dr.
Suite 240
Pittsburgh, PA 15205

Register at:
http://www.e-safetech.com/labday-2017/

KRACK hacks: What you need to know

You've heard of ransomware, denial-of-service attacks, and even phishing, but one hacking technique you may not have heard of is the KRACK exploit. This attack takes advantage of a vulnerability in WiFi networks, which puts any device with a wireless connection at risk. Here's everything you need to know about KRACK.

What is KRACK?

Simply put, KRACK, short for 'key reinstallation attack,' allows hackers to bypass WPA2 -- a security protocol used by routers and devices to encrypt activity -- and intercepts sensitive data passing between the mobile device and the wireless router, including login details, credit card numbers, private emails, and photos.

In extreme cases, KRACKed devices can be remotely controlled. For example, hackers can log in to your surveillance systems and shut them down.

What's worse, Internet of Things devices -- like smart thermostats and IP cameras -- rarely receive security fixes, and even if some are available, applying patches are difficult, as these devices tend to have complex user interfaces.

The good news, however, is you can do several things to mitigate the risks.

Download patches immediately

According to recent reports, security patches have already been released for major platforms, including iOS, Windows, and Android. Router manufacturers such as Ubiquiti, Mikrotik, Meraki, and FortiNet have also issued firmware updates, so make sure to install them as soon as possible.

Although IoT patches are rare, consider getting your smart devices from reputable vendors that push out updates regularly. It's also a good idea to contact a managed services provider to install the updates for you.

Use Ethernet connections

Some wireless routers don't yet have a security patch, so while you're waiting, use an Ethernet cable and disable your router's wireless setting. Turn off the WiFi on your devices as well to make sure you're not connecting to networks susceptible to KRACK.

Stay off public networks

Free public WiFi networks -- even ones that are password-protected -- in your local cafe should also be avoided because they usually don't have holistic security measures in place, making them easy targets for cybercriminals.

Connect to HTTPS websites

If you do need to connect to a public WiFi hotspot, visit websites that start with "HTTPS," and stay away from ones that are prefaced with "HTTP." This is because HTTPS websites encrypt all traffic between your browser and the website, regardless of whether the connection is vulnerable to KRACK

Hop on a Virtual Private Network (VPN)

You can also use a VPN service to hide all network activity. Simply put, VPNs encrypt your internet connection so that all the data you're transmitting is safe from prying eyes.

Although the potential impact of a KRACK hack is devastating, security awareness and top-notch support are the best ways to stay safe online. Want more security tips? Contact us today.