Secure Networkers®

IT NEWS BRIEF

AUGUST 2020

WATCH OUT for this THREAT

Zip File Attachments!

You probably already know that spoofed emails can carry dangerous files. And, because it is often hard to spot a spoofed email, sometimes you will open that email, access that attachment, and unzip that file before you realize that it is not what you thought it was.

Furthermore, did you know that MS Word documents, Excel files, and even Adobe files, can be the malware carriers in that zip file?

Many times, these common and accepted forms of documents are the culprits responsible for major malware exposure.

All these files are capable of containing macros and scripting able to unload a world of trouble for your work station or even your network. Usually they will be delivered to you in the form of a zip attachment.

How to prevent malcious macros.

You can prevent the automatic execution of malicious code in those unsuspecting email attachments. All you need to do is prevent the automatic run of macros. It's pretty simple to do: it just requires a adustment in your settings. Here are the links to official instructions to take care of this important safety measure:

TO DISABLE MACROS IN OFFICE FILES: CLICK HERE

TO ENABLE ADOBE FILE SECURITY: CLICK HERE

FOUR 'EITHER/OR's

FUNDAMENTAL LAWS OF KEEPING A SECURE NETWORK

> "LEARN THE FUNDAMENTALS OF THE GAME AND STICK TO THEM. BAND-AID REMEDIES NEVER LAST."
>
> – JACK NICKLAUS

There are several Either/Or statements that apply to network security. To know them is to know the fundamentals necessary to keep your network safe from intrusions and corruption. Here are the four to consider:

1 Strong Architecture:
Either disrupt
Or be disrupted

One of the strongest capabilities you can give your security posture is the fundamental of an architecture able to transform as needed to keep up with technology requirements. The bad guys trying to break into your system are perpetually innovating. The architecture of your network needs to likewise be able to change with changing needs.

2 Protect Network Uptime:
Either have continuity
Or pay for mitigation management.

Unplanned down time is the consequence of not caring for continuity. When the network goes down, it hits operations, IT management, and ultimately your pocketbook.

3 Digital Strategy:
Either a proactive IT team
Or Security that lags behind.

Ensure your IT administration team is up to speed with training. Properly digitized assets will make them more accessible. Lagging means the rising probability of losing sight of network security critical vulnerabilities.

4 Offensive Line in Cybersecurity:
Either hunt
Or be hunted.

The cost of a data breach is phenomenal: $7.91 million is the average cost in the US today [Forbes]. Proactively pen testing your network and general security operations is so important to the true strength of your security profile.

If you have these four focuses present in your organization's cybersecurity profile, you can have high confidence in the security of your network and its efficiency to conduct business. If you have questions about whether your artchitecture is nimble, or if your continuity plan is complete, whether your IT administration is up to speed on everything, or if you think it is time for that pen test to see how your network performs, we are always ready to help. Call us at 281.651.2254.

A STRONG NETWORK

Let's connect and follow each other in business! If you have a particular social network you use, please let us know so we can "Like", "Follow" and "Connect" with you. *FIND US AT:*

EVENTS | BLOG

EMAIL QUESTIONS TO:
Service@Securenetworkers.com

CALL US:
(281) 651.2254

WORK FROM HOME SECURELY!

Subscribe

PLEASE SUBSCRIBE