Q1 2021
Volume 1, Issue 1

M6 Digest IT

We Take "IT" Seriously

BDR - Backup and Disaster Recovery - Nick DeRose

With the never-ending evolution of cyber threats, data protection should be an integral part of any business. M6 Technologies, Inc. takes the responsibility of protecting its clients' data very serious. M6 continually trains its technicians to understand these constantly evolving threats and how to prevent them but, in the event of data corruption or hardware failure, backup solutions are in place to restore client data within hours.

M6 utilizes backup solutions provided by Barracuda Networks. A physical back-up unit is installed at each M6 client office location and is configured to backup client data file systems and physical server system states three to four times a day. These backups are then replicated to offsite Barracuda cloud data centers in the event of physical damage to, or hardware failure of, the backup unit.

If a file is deleted or missing, a version of that file can be restored and placed in the original file location within a few minutes. In the event of a server failure, these backups enable the restoration of the data to a repaired server or to another piece of hardware. It is also possible to spin up a virtual instance of the server directly from the cloud via an Internet connection and web browser. With M6 threat prevention tools in place, these features may not need to be used very often, other than restoring the occasional deleted or missing file, but the importance of this protection is immense.

Inside this Issue

Special Points of Interest

- BDR—Do you have a plan in place?
- Check out the Security Insights on page 2.
- See page 3 for our Employee Spotlight.
- From the Desk of...page 4.

Security Insights

M6 continuously monitors the Dark Web for the presence of its clients' Domains and email addresses. Call for a free scan and report on your Domain!

Secure passwords are critical. Compromised, weak and stolen credentials provide one of the most common vectors for cybercriminals. We've all heard it...at least 8 characters, at least 1 cap, 1 number and one special character! Phrases are now thought to be better, such as, "W3 have a gre@t IT T3am!"

Multi-Factor Authentication (MFA) provides an additional layer of security when accessing online or network resources. A user provides two pieces of information from different categories to access their account (i.e. password and pin or credentials and a code sent to a device). Providing two passwords is not considered MFA (passwords are one category).

"Next Generation" EndPoint Protection is a must on all network resources that M6 monitors for its clients. This tool not only protects PCs, laptops and servers from viruses and malware, but provides real time alerts and statistics for our technical support team. M6 EndPoint Protection includes content and URL filtering. It also protects devices when they leave the office (laptops and tablets).

Education, Education, Education! - M6 offers phishing campaign services with automated training if a user gets "hooked." On-site and virtual cyber security training is also offered. Consider 60% of compromises begin internally via human error. Remember the three "T"s...Train, Trick and Test!

Small Business Asks...Why Secure Passwords? Why Multi-Factor Authentication (MFA)? Why EndPoint Protection?

Cybercriminals are on the prowl more than ever. Last year, during the pandemic, estimates indicate attacks multiplied by at least 30%. Experts agree that this number is low since many people don't report these attacks to the proper authorities. Cybercriminals seek to obtain sensitive data including user credentials, credit card information and personal information (social security numbers, bank information, places of work - to name just a few).

They scour social media to determine work relationships, vacation and travel habits, shopping habits and more. Their tools and tactics are very sophisticated. The Cybercrime Industry is raking in about $1.5 TRILLION each year. That is more than Microsoft, Tesla, Apple, Amazon and Facebook combined! A lot of folks still believe cybercriminals are lone wolves parked in a back room with dark hoodies over their heads when in reality cybercriminal groups have executives, administrative staff and recruiting staff. They even have help desk support! Some even use public personas to promote their "good reputations."

Compromised credentials are typically obtained via "phishing" emails when a victim enters their logon credentials on a fake website. An email may contain a link that deposits malware or ransomware on an end point that encrypts data. The cybercriminal may use this to demand payment to unlock that data. They may also use it to obtain contact information from an application on the end point to use in a "spear phishing" attack. This is a "targeted" attack directed at individuals or companies (often referred to as CEO or CFO Phishing).

Small businesses share the same risks that large and enterprise businesses encounter. In fact, due to their limited IT budgets and possible lack of technical expertise, small businesses are more likely to be breached. Cybercriminals sell compromised credentials on the Dark Web to the tune of over $160 BILLION annually. Quite a lucrative enterprise.

How do we defend ourselves? (1) Use **Secure Passwords**. We all know what they are. Check out this link: https://www.youtube.com/watch?v=z_HmDP3lKMI (Yes, it is a safe link!)

(2) Implement **Multi-Factor Authentication (MFA)**. MFA should be added to all business as well as personal login accounts. It needs to be configured on remote access VPN connections and other perimeter network resources. It is becoming, if not already, a must.

And, lastly, (3) Ensure all PCs, laptops, servers and other network resources have sufficient **EndPoint Protection** applications. It's a no brainer!

Email is the "phisherman's" bait of choice

10 Surprising Small Business Cyber Security Facts!

1. Forty-three percent (43%) of cyber attacks target small businesses.
2. Sixty percent (60%) of small businesses that are victims of a cyber attack go out of business within six months.
3. Sixty-three percent (63%) of confirmed data breaches leveraged weak, default or stolen passwords.
4. There was more than a 420% increase in new small business breaches from 2019 to 2020.
5. Fifty-four percent (54%) of small businesses think that they are too small for a cyber attack.
6. Twenty-five percent (25%) of small businesses do not know cyber attacks would cost them money.
7. Eighty-three percent (83%) of small businesses have not set aside cash for dealing with a cyber attack.
8. Small businesses spend an average of $955,429 to recover from a successful attack.
9. Ninety-one percent (91%) of small businesses don't have cyber liability insurance.
10. Cyber attacks are projected to cause $6 TRILLION in damages in 2021!

Life Before a Computer

An application was for employment.
A program was a TV show.
A cursor used profanity.
And a keyboard was a piano!

Memory was something that you lost with age.
A CD was a bank account.
And if you had a three inch floppy,
you hoped nobody found out!

Compress was something you did to garbage, not something you did to a file.
And, if you unzipped anything in public,
you'd be in jail for awhile!

Log on was adding wood to a fire.
Hard drive was a long trip on the road.
A mouse pad was where a mouse lived.
And a backup happened to your commode!

Cut you did with a pocket knife.
Paste you did with glue.
A web was a spider's home.
And a virus was the flu!

I guess I'll stick to my pad and paper
and the memory in my head.
I hear nobody's been killed in a computer crash,
But when it happens they wish they were dead!

Contribution from our oldest team member...guess who?

M6 Employee Spotlight

Sandra Dorsch (Sandy)
Position: Assistant Client Services Coordinator

Sandy is the newest member of the M6 Technologies team. She joined M6 in June, 2020, the year of COVID-19. As Assistant Client Services Coordinator, Sandy is responsible for answering the phones, creating tickets in Autotask (M6 professional services automation tool), and dispatching these tickets to our technical team. She also maintains and updates IT Glue (M6 documentation platform). In addition to the above tasks, Sandy reviews daily client Backup Reports and dispatches any issues accordingly. She is the "phisherman" behind our phishing campaigns, better known as "BullPhishing," and pitches in with administrative duties. One might say she is M6's "Jackie of all Trades." Sandy comes into the office each day with a smile on her face and is always happy and upbeat. She has been a great addition to our team.
Prior to joining M6, Sandy worked at Bacharach for 22 years as a secretary, Marsh for 15 years and CIMG for four years as an Insurance Assistant. In her spare time, she pushes wheelchairs at the Airport for a company called Prospect.

M6

Digest IT

Core Pillars - Our Values

Compassion: We show compassion and caring for our employees and clients.

Integrity: We will be honest and truthful to our employees, clients and vendors.

Empowerment: We provide an environment where our employees become confident, responsible and accountable.

Community: We acknowledge the need for and encourage involvement in our communities.

Faith & Family: We respect the faith and lifestyles of our employees.

From the Desk of...

Bill Mulcahey

There is no doubt that this past year was very strange and unique. Our businesses have traversed difficult waters before but nothing like those encountered in 2020. Yet, as we drew closer to the end of last year, and I took a peek back to its start, I was and am still amazed and thankful for the resourcefulness, flexibility and dedication of the M6 team members.

The disruption that the COVID-19 pandemic forced upon everyone's routines had little effect on the support and services that our team members provided not only to our clients but to each other. When Jennifer, our Client Services Coordinator, decided back in March to send everyone home, no one missed a beat. A skeleton crew remained as staff members headed home to set up their home offices. Within a couple of hours, these "home offices" were up and running, and M6 was able to continue providing the support and services its clients deserve and have come to expect. We have a great group here! We were a tight-knit bunch before but, in a strange way, this pandemic has brought us even closer.

We all hope that this new year brings calmer waters. However, if it does not, know that M6 Technologies is here for you, and we'll ride whatever waves come our way...together!

Business Read: Team of Teams by General Stanley McChrystal, US Army Retired

Personal Read: Apocalypse Never by Michael Schellenberger

M6

10 E. Crafton Avenue
Pittsburgh, PA 15205

hone: 412.921.6811
E-mail: info@m6technologiesinc.com

Our Mission Statement

M6 Technologies strives to be the premier MSP and IT Service Provider for small businesses in the Pittsburgh, Pennsylvania region.

We will accomplish this by delivering expert and attentive support to our clients through well-trained, honest and accountable Client Service Advocates. We will continually educate ourselves on existing and new technologies so we can design, implement and manage the best IT solutions. M6 Technologies makes every effort to be your trusted strategic IT partner dedicated to your overall success.

M6 Technologies will be celebrating our 20th year of service in September of this year! Exciting announcements to follow.