ISSUE
02
February 2020

MANAGEDTEK
MONTHLY
JOURNAL OF
INFORMATION

TekTimes

This issue

Your Employees: Your First Line Of Defense P.1

Dark Web: Importance of Cybersecurity. P.2

Eye On It: What's Going On In Tech World P.3

Welcome!

Cyber-attacks have continued to grow in cost, size, and impact – causing 60% of SMBs to go out of business within 6 months of a cyber incident. Over 80% of data breaches leverage stolen passwords as the principal attack vector – often acquired on the Dark Web.

Continuous Network Intelligence

Knowledge is power. A critical component of cyber readiness is having on-demand insight of anomalous activities, suspicious changes, potentially harmful misconfigurations or any other malicious activities occurring internally on your network. Promptly detect and remove threats before they cause damage.

Your Employees: Your First Line Of Defense

Let us provide you a full picture of your company's security posture and potential risk, so the employees who were the weakest link in your defense can become its strongest point of protection. Because employees are the core of any business, they will be the main target for cyber criminals. Making sure your people stay up-to-date with cyber security knowledge, and teaching them to recognize threats, is imperative to the security of your business. The threat landscape is constantly evolving, and so should your approach to defense.

WHY YOU NEED AN INTEGRATED, ONGOING PROGRAM - Cyber-attacks are on the rise; particularly among small- and mid-sized businesses. z You may have the most up-to-date and strongest security systems in place, but this will be a wasted investment if you don't also train and test your staff. Threats are ever-evolving and become more sophisticated and harder to detect. Regular training on the latest criminal tactics will help mitigate risk.

Data is the lifeblood of every business. Unfortunately, the risks and threats to the protection, privacy and usability of that data are endless. Follow the 3-2-1 method for backups; a minimum of three unique copies of your data, two available locally and one off-site or in the cloud. Make sure to test your backups often for functionality and integrity.

DOES THE IDENTIFICATION OF MY ORGANIZATION'S EXPOSED CREDENTIALS MEAN WE ARE BEING TARGETED BY HACKERS? While we can't say definitively that the data we've discovered has already been used to exploit your organization, the fact that we are able to identify this data should be very concerning. Organizations should consult their internal or external IT and/or security teams to determine if they have suffered a cyber incident or data breach.

SOME OF THIS DATA IS OLD AND INCLUDES EMPLOYEES THAT ARE NO LONGER WORKING FOR US. DOESN'T THIS MEAN WE ARE NOT AT RISK? While employees may have moved on from your organization, their company issued credentials can still be active and valid within the 3rd party systems they used while employed. In many cases, the 3rd party systems or databases that have been compromised have been in existence for 10+ years holding millions of "zombie" accounts that can be used to exploit an organization. Discovery of credentials from legacy employees should be a good reminder to confirm you've shut down any active internal and 3rd party accounts that could be used for exploit.

ANY "BEST PRACTICES" FOR INDIVIDUAL USERS OR CORPORATE IT ON FREQUENCY OF PASSWORD CHANGE OR ACTUALLY CHANGING YOUR PERSONAL OR PROFESSIONAL EMAIL? Please refer to the National Institute of Standards and Technology's (NIST) Special Publication 800-63B Digital Identity. A link to SP800-63B can be found here: https://pages.nist. gov/800-63-3/sp800-63b.html

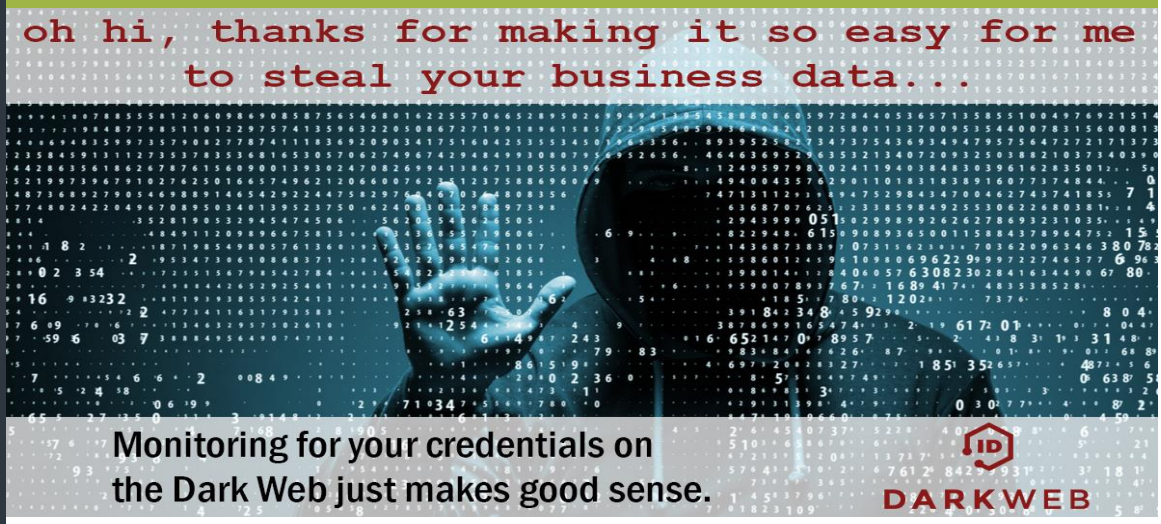
YOUR BUSINESS CREDENTIALS: ARE THEY FOR SALE ON THE DARKWEB?

Cyber-attacks have continued to grow in cost, size, and impact – causing 60% of SMBs to go out of business within 6 months of a cyber incident. Over 80% of data breaches leverage stolen passwords as the principal attack vector – often acquired on the Dark Web.

IT Hygienne Practice

IT Hygiene is a reference to the practices and steps that users of computers, and other devices, take to maintain system health and improve online security. These practices are often part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. These include regular software patches, password changes, and firewall and antivirus updates.

To add value to our customers, ManagedTek, provides solutions that include Security Awareness Training and Anti-Phishing platforms.



Dark Web:Importance Of Cybersecurity

WHAT IS THE DARK WEB?

In last months newsletter, we explained in detail that The Dark Web is a hidden universe contained within the “Deep Web”- a sublayer of the Internet that is hidden from conventional search engines.

HOW ARE THE STOLEN OR EXPOSED CREDENTIALS FOUND ON THE DARK WEB:

Dark Web ID focuses on cyber threats that are specific to our clients’ environments. We monitor the Dark Web and the criminal hacker underground for exposure of our clients’ credentials to malicious individuals. When a credential is identified, we harvest it. While we harvest data from typical hacker sites like Pastebin, a lot of our data originates from sites that require credibility or a membership within the hacker community to enter. To that end, we monitor over 500 distinct Internet relay chatroom (IRC) channels, 600,000 private Websites, 600 twitter feeds, and execute 10,000 refined queries daily.

I SEE FAKE EMAILS (FALSE POSITIVES). WHY IS THIS IMPORTANT?

Fake email accounts are routinely created by employees as a “throw away” when wanting to gain access to a system or piece of data. However, fake email accounts are frequently created to facilitate well-crafted social engineering and/or phishing attacks. Often, the identification of fake email accounts indicates that an organization has been targeted by individuals or groups in the past.

WHAT YOU CAN DO TO PROTECT YOUR BUSINESS?

By utilizing Dark Web ID™, a combination of human and sophisticated Dark Web intelligence with search capabilities, you are able to identify, analyze and proactively monitor for your organization’s compromised or stolen employee and customer data.

HOW DARK WEB ID PROTECTS YOUR BUSINESS:

- Connects to multiple Dark Web services including Tor, I2P and Freenet, to search for compromised credentials, without requiring you to connect to these high-risk services directly.
- Provides intelligent awareness of compromised credentials before breaches occur.

WHY IT’S IMPORTANT:

- Compromised credentials are used to conduct further criminal activity.
- Employees often use the same password for multiple services, such as network login, social media, and SaaS business applications, exponentially increasing the potential damage from a single compromised credential.
- Limited visibility when credentials are stolen; over 75% of compromised credentials are reported to the victim’s organization by a third party, such as law enforcement.

Eye On It: What's Going On In Tech

IT trends for 2020 and how to apply these trends to small, and midsize, businesses.

Human Augmentation: Current **tool** integration and unified **workflows across all supporting products**.

Hyper-automation: IT automation, which is basically guided by policies to standardize technology processes.

Multiexperience: Managing IT on the go by providing technicians with the option to manage service tickets more quickly by accessing information while remote, or offsite .

Democratization: IT technology **ease of use** and instinctive user borders for a improved user experience.

Updating your device creates a vulnerability to cyber security attacks is one of the worst myths that we have heard! While updates often introduce new or enhanced features into your apps, programs and systems, they also install security and performance fixes known as patches. Undiscovered defects or flaws can leave your systems exposed. Hackers will exploit any vulnerability or security gap they find. Keeping your systems updated is vital for keeping your business cyber ready.

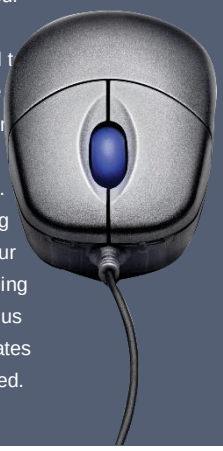
FB LIVE – We are very eager to attend our first FaceBook live session this month. We will keep you updated on our prospected date, so please continue to check our page. We are looking forward to a positive response to our February FB live session. We are focusing on educating our clients on the most common vulnerabilities that are attacking businesses throughout the world. We are big on educating and continuing to learn how to serve our customers and friends. Please feel free to email us any questions, or topics of interest.

This Month's Q&A TeK Tip

Q: What is "Phishing?"

A: Phishing is the act of attempting to manipulate a recipient into opening an email and engaging. A sender of a malicious email intends to deceive a victim by making the email seem important and from a reputable source. These phishing emails may include harmful attachments, like PDF or Word documents, which once opened can cause harm to the user's computer by installing forms of malware, ransomware, or other unsavory software. Phishing emails can also contain malicious links in the body that can lead a user to a fraudulent site. These sites are used to collect confidential information such as usernames and passwords, or to install malware onto a device. Once the victim's information has been obtained, scammers will monetize the data by selling it to the highest bidder on Dark Web sites.

At ManagedTek, ensuring confidential data remains secure isn't just about databases, networks, and end points. It applies to your physical workspace too. Spam mail and phishing attacks can often be detrimental t an organization, these attacks can cause breach of personal or clientele informatio or a loss of funds. Educate yourself, and your employees, and you'll catch a phish. We offer our Security Awareness Training platform in order to train yourself, and your employees, to recognize and avoid phishing attacks tarketing human vulnerability.Let us automate and optimize your system updates and patches. Contact us now to get started.



Cyber Awareness Strategies:

Have a Cyber Readiness Plan.

Establish Strict Policies and Procedures.

Keep Updates Up to Date.

Deploy a Multi-Layer Security Strategy.

Force Authentication.

Back Up Everything.

Don't Neglect Compliance.

Continous Network Intelligence.

Security Awareness Training.

Combat the Password Crisis.

Don't't Skip the Insurance.

Reduce Supply Chain Vulnerabilites.

Upcoming Events:

New Office Location Grand Opening – TBT

SecuirtyNext - Feb. 9-11, 2020

YAAC CEO Success Tour 2020 - Feb. 22, 2020

Patriot Boot Camp – Mar. 5-7, 2020

ConnectIT Global – May 4-7, 2020.

Wingman2020 - June 3-5, 2020

GlueX 2020 – Sep. 27-29, 2020

ManagedTek
1090 Adams St.
Suite G
Benicia, CA 94510
info@managedtek.com
www.managedtek.com |