ISSUE 017
MARCH 2023

in the HOOP

YOUR MONTHLY DOSE OF TECH TIPS & HOOP5 NEWS

MONTHLY UPDATE FROM MANDY

Vulnerabilities are an unfortunate side effect of all the technological advancements these days. Software developers rush out their next releases, then hackers comb that code for vulnerabilities they can exploit. In 2022, there were estimated to be over 22,500 IT security vulnerabilities worldwide.

These vulnerabilities act as gateways to cybercriminals. They use them to find backdoors into a system, elevate privileges, and enable other types of breaches. To stay on top of them takes a comprehensive vulnerability management strategy that begins with an assessment.

By proactively assessing, identifying, and fixing vulnerabilities in your network, you can greatly improve cybersecurity. It's also a requirement for complying with many types of data privacy regulations.

Would you like some help with a vulnerability assessment? Email us at info@hoop5.net to schedule a chat.

Until then, stay safe,

Mandy Irvine McClure

CEO - Hoop5 Networks

WHAT'S INSIDE?

DID YOU KNOW?

Did you know Google receives over 99,000 search results every single second!

02

SHOULD YOU SPY ON YOUR TEAM'S DAILY WORK?

Since the pandemic, employers around the world have needed to change. They've had to shift how their employees operate. Remote work is very much here to stay. Organizations and employees can both benefit from the work-from home and hybrid work revolution.

Cost savings is a driver for supporting remote work. Employee morale and productivity also can be higher when employers grant this flexibility.

A majority of organizations support some type of remote work. Statistics show[1] that:

- 16% of companies are completely remote
- 40% support hybrid office/remote working
- 44% don't allow employees to work remotely

While there are benefits, there are also challenges to this new environment. Employers worry about the cybersecurity risks of remote teams. Managers can find it more challenging to make sure employees are doing what they should do.

The remote and hybrid work environment has led to the rise of employee monitoring tools. These tools have mixed reviews from employees.

WHAT IS EMPLOYEE MONITORING SOFTWARE?

Employee monitoring software tracks digital movements. This can include everything from general clock-in clock-out tracking to taking screenshots of an employee's computer several times per hour.

Tracking tools like Hubstaff and BambooHR track many activities on a person's computer. The information is then sent in a daily or weekly report to the company.

Items that these tools can track are:

- Time clock
- Keyboard activity
- Keystrokes
- Mouse activity
- Websites visited
- Screenshots of the desktop
- Apps used and how long in use

The most invasive of tools can even track the sounds and video of the employee.

Tracking can be visible, so the employee knows about it, or the tracking can be completely hidden from the employee.

It depends on the tool used and the cultural and ethical considerations
of the employer.

This type of monitoring can benefit an organization worried about productivity theft." But it can also alienate good employees and torpedo morale and trust. Let's go through the pros and cons before you set up this type of system.

MONITORING TOOLS PROS

1. Understand Time Inputs

Knowing exactly how much time employees spend on a project can help with future with ROI projections.

2. Reduce Time Wasting

About half of monitored employees spend 3+ hours per day on non-work activities. When employees know that their boss is monitoring their app usage, they're less likely to goof off.

3. Billing Time Tracking

If you invoice your clients based on time, Monitoring Tools can help capture the teams time correctly so it's billed properly. This stops hours falling through the cracks.

MONITORING TOOL CONS

1. Hurts Team Morale

Many employees feel they are put in a cage when monitoring is introduced. Morale can plummet, which takes productivity and trust along with it.

2. Activity isn't Productivity

Many tools simply report on keyboard and mouse activity. But what if the employee must solve a workflow issue and needs to use their brain for a few hours, not their mouse?

3. Good Employees Leave

Nearly half (47%) of surveyed tech employees said they would quit if their boss tracked them.

Sources
1. https://squaretalk.com/remote-work-statistics/

03 IS THAT A REAL TEXT FROM YOUR CEO? OR A SCAM?

Imagine you're going about your day when suddenly you receive a text from the CEO.

The head of the company is asking for your help. They're out doing customer visits and someone else dropped the ball in providing gift cards.

The CEO needs you to buy six $200 gift cards and text the information right away.

The CEO promises to reimburse you before the end of the day. Oh, and by the way, you won't be able to reach them by phone for the next two hours because they'll be in meetings. One last thing, this is a high priority. They need those gift cards urgently.

Would this kind of request make you pause and wonder? Or would you quickly pull out your credit card to do as the message asked?

A surprising number of employees fall for this gift card scam.

There are also many variations. Such as your boss being stuck without gas or some other dire situation that only you can help with.

Without proper training, 32.4% of employees are prone to fall for a phishing scam[1].

Variations of this scam are prevalent and can lead to significant financial losses, both personally and in the business.

In one example[2], a woman from Palos Hills, Illinois lost over $6,000 after getting an email request from who she thought was her company's CEO about purchasing gift cards for the staff.

Need Help with Employee Phishing Awareness Training?

Give us a call today to schedule a training session to shore up your team's defenses.

TIPS FOR AVOIDING COSTLY PHISHING SCAMS

1. Always Double Check Unusual Requests

Despite what a message might say about being unreachable, check in person or by phone anyhow.

If you receive any unusual requests, especially relating to money, verify them.

Contact the sender through other means to make sure it's legitimate.

2. Don't React Emotionally

Scammers often try to get victims to act before they have time to think.

Just a few minutes of sitting back and looking at a message objectively is often all that's needed to realize it's a scam.

Don't react emotionally, instead ask if this seems real or is it out of the ordinary.

3. Get a Second Opinion

Ask a colleague, or better yet, your company's IT Service Provider, to take look at the message. Getting a second opinion keeps you from reacting right away. It can save you from making a very costly judgment error and only takes a few extra minutes.

Sources

1. *https://itsupplychain.com/1- in-3-employees-fall-forphishing- attacks-withouttraining/*
2. *https://abc7chicago.com/scam-email-fake-boss-from/5901884/*

04 4 PROVEN WAYS TO MITIGATE THE COSTS OF A DATA BREACH

No business wants to suffer a data breach. But unfortunately, in today's environment, it's difficult to completely avoid them. Approximately 83% of organizations have experienced more than one data breach.

(IBM Security 2022: https://www.ibm.com/reports/ data-breach)

The global average cost of a data breach is now $4.35 million, up 2.6% from last year.

Companies don't need to resign themselves to the impending doom of a breach. There are some proven tactics they can take to mitigate the costs.

Cybersecurity Tactics to Reduce the Impact of a Breach

1. Use a Hybrid Cloud Approach

Breaches in both the public cloud and private cloud cost more than those in organizations using a hybrid cloud approach.

2. Put in Place an Incident Response Plan & Practice It

Having a practiced incident response plan reduces the cost of a data breach. It lowers it by an average of $2.66 million per incident.

3. Adopt a Zero Trust Security Approach

Organizations that don't deploy zero trust tactics pay about $1 million more per data breach.

4. Use Tools with Security AI & Automation

Data breach expenses lower by 65.2% thanks to security A.I. and automation solutions. These types of solutions include tools like Advanced Threat Protection (ATP).

Need Help Improving Your Security & Reducing Risk?

Working with a trusted IT partner takes a lot of the security burden off your shoulders. Give us a call today to schedule a chat about your Cybersecurity Roadmap.

05 STOP FRAUD WITH YOUR ONLINE BANKING

Millions of dollars are stolen from small business bank accounts around the world every single month (and the threat is increasing every day).

As hackers get smarter and build new ways to break into your systems, you need to work hard to stay one step ahead of them so you don't fall victim.

Here are some essentials you need to have in place with your Online Banking:

- Have a Strong & Unique Banking Password
- Turn On Two-Factor Authentication
- Set Up Banking Alerts
- Install Next-Gen Antivirus & DNS Filtering On Your PC
- Enroll your Team in Phishing Training Classes
- Setup Multi-User Payment Approval
- Call your Bank and ask what other Security Measures you can turn on

06 COOL WINDOWS 11 FEATURES YOU MIGHT LOVE

Every time Microsoft releases a new Operating System, some people love it and some people hate it.

(although I think we can all agree that everyone hated Windows Vista)

Here are some areas in Microsoft's latest Operation System, Windows 11, that Microsoft has focused on to help you work easier and faster:

- Snap Layouts
- Master Search
- Clipchamp Video Editor
- MS Teams Video, Audio & Text Messaging
- Accessibility Features
- Collections in Microsoft Edge
- Microsoft Defender SmartScreen

You'll also notice they have redesigned and centred the Start Menu / Task Bar, perhaps taking inspiration from Apple's Mac.

Call us today if you want help planning your businesses Windows 11 Roll-out.

07 6 WAYS TO PREVENT ONE OF THE MOST COMMON SOURCES OF DATA BREACHES

Misconfiguration of Cloud Solutions is often overlooked when companies plan Cybersecurity Strategies. Cloud apps are typically quick and easy to sign up for so users often assume that they don't need to worry about Security because it's handled.

This is a bad assumption because Cloud Security is a shared model. The Provider/ Vendor handles securing the backend infrastructure. But the user/client is responsible for configuring security settings in their account.

Here are some tips to improve your Cloud Security:

- Enable Visibility Into Your Cloud Infrastructure
- Restrict Privileged Accounts
- Put in Place Automated Security Policies
- Use a Cloud Security Audit Tool (Like Microsoft Secure Score)
- Set Up Alerts for When Configurations Change
- Run Regular Security Setting Audits
- Ensure each user has their own Account (no sharing of Accounts)
- Have a Cloud Expert Check Your Cloud Settings