Talk Nerdy To Me

New Cyberthreats Remind Us Of The Need For Hyper-vigilance

In recent weeks, we've seen a number of significant cybersecurity threats emerge. Microsoft's revelation that its Exchange servers had been compromised has raised concerns across users around the world. Meanwhile, leaks of audio files from hot-shot social media start-up Clubhouse has reminded everyone that those wanting to hack data will use any opportunity to do so. Currently in Asia, they have their own home-grown threat to deal with: ObliqueRAT. They first alerted the world to the malware targeting organizations across South Asia in February 2020 but in recent days, we've seen those behind the attack change tack.

In previous attacks, the malware was delivered via Microsoft Office documents. This time around, the payload is not contained in documents but in 'adversary-controlled' websites which infect machines when users visit. This change in tactic perfectly illustrates the challenge we all face as threat actors quickly and effectively change their techniques to evade detection.

Keeping pace with new security threats has become even more critical now that so many organisations have put in place remote working in response to the pandemic. Not only are we more reliant than ever on technology but a distributed workforce broadens what we call the 'attack surface' in cyber security and can often make rolling out new procedures and policies extremely difficult.

So, aside from ensuring you keep operating system and applications updated with the latest security patches, what else can you do to combat these threats? Firstly, you really do need to make sure that you have a tried and trusted crisis management plan ready to roll out that enables you to keep the organization running and communicate the situation with the relevant stakeholders if the worst happens. That plan needs to be updated at least quarterly to ensure it is relevant to the evolving nature of your business, and the threat environment.

As a business, you also need to step up monitoring for any unusual signs on your network. Every person in your IT team needs to be hyper-vigilant and recognise that anything unusual – even mundane-looking, end-user issues – could be a sign of intrusion. There are several monitoring tools today that can be used to provide automated visibility across your network and applications. As organisations adopt increasingly hybrid IT models running on both on-premises and cloud-based networks and involving multiple solutions, an integrated approach to cyber security will help ensure that you are able to protect, detect, respond to and remediate any threats within your environment.

This hyper-vigilance needs to be extended across the entire workforce so that you have multiple "pairs of eyes" looking for potential issues while also keeping up everyone's guard to ensure a simple slip-up does not put your organization at risk.

Finally, I would also say that there has never been a better time to start your journey to a zero-trust cyber security strategy. This involves building an architecture which continuously ensures that only trusted users and devices may enter the network from any location. I know we all have a lot on our plates coping with a distributed workforce and a potential return to office strategy but, as we have seen over just the last three weeks, the threat has never been greater and we have an opportunity today to ensure that our data, users and applications are secure.

Source: computerweekly.com

2

April 2021

What Is Business Continuity And Why Is It Important?

Business continuity is an organization's ability to maintain essential functions during and after a disaster has occurred. Business continuity planning establishes risk management processes and procedures that aim to prevent interruptions to mission-critical services, and reestablish full function to the organization as quickly and smoothly as possible.

The most basic business continuity requirement is to keep essential functions up and running during a disaster and to recover with as little downtime as possible. A business continuity plan considers various unpredictable events, such as natural disasters, fires, disease outbreaks, cyberattacks and other external threats.

Business continuity is important for organizations of any size, but it might not be practical for any but the largest enterprises to maintain all functions for the duration of a disaster. According to many experts, the first step in business continuity planning is deciding what functions are essential and allocating the available budget accordingly. Once crucial components have been identified, administrators can put failover mechanisms in place.

Why is business continuity important?
At a time when downtime is unacceptable, business continuity is critical. Downtime comes from a variety of sources. Some threats, such as cyberattacks and extreme weather, seem to be getting worse. It's important to have a business continuity plan in place that considers any potential disruptions to operations.

The plan should enable the organization to keep running at least at a minimal level during a crisis. Business continuity helps the organization maintain resiliency, in responding quickly to an interruption. Strong business continuity saves money, time and company reputation. An extended outage risks financial, personal and reputational loss.

Business continuity requires an organization to take a look at itself, analyze potential areas of weakness and gather key information -- such as contact lists and technical diagrams of systems -- that can be useful outside of disaster situations. In undertaking the business continuity planning process, an organization can improve its communication, technology and resilience. Business continuity might even be a requirement for legal or compliance reasons. Especially in an era of increased regulation, it's important to understand which regulations affect a given organization.

What does business continuity include?
Business continuity is a proactive way to ensure mission-critical operations proceed during a disruption. A comprehensive plan includes contact information, steps for what to do when faced with a variety of incidents and a guide for when to use the document.

Business continuity features clear guidelines for what an organization must do to maintain operations. If the time comes for response, there should be no question about how to move forward with business processes. The company, customers and employees are all potentially at stake.

Proper business continuity includes different levels of response. Not everything is mission-critical, so it's important to lay out what is most vital to keep running, and what could stand to come back online at later times. It's crucial to be honest about recovery time objectives and recovery point objectives. The process includes the whole organization, from executive management on down. Although IT might drive the business continuity, it's essential to get buy-in from management and communicate key information to the entire organization.

One other important area of collaboration is with the security team -- although the two groups often work separately, an organization can gain a lot by sharing information across these departments. At the very least, everyone should know the basic steps for how the organization plans to respond.

Three key components of a business continuity plan
A business continuity plan has three key elements: Resilience, recovery and contingency. An organization can increase resilience by designing critical functions and infrastructures with various disaster possibilities in mind; this can include staffing rotations, data redundancy and maintaining a surplus of capacity. Ensuring resiliency against different scenarios can also help organizations maintain essential services on location and off site without interruption.

Rapid recovery to restore business functions after a disaster is crucial. Setting recovery time objectives for different systems, networks or applications can help prioritize which elements must be recovered first. Other recovery strategies include resource inventories, agreements with third parties to take on company activity and using converted spaces for mission-critical functions.

A contingency plan has procedures in place for a variety of external scenarios and can include a chain of command that distributes responsibilities within the organization. These responsibilities can include hardware replacement, leasing emergency office spaces, damage assessment and contracting third-party vendors for assistance.

Business continuity vs. disaster recovery
Like a business continuity plan, disaster recovery planning specifies an organization's planned strategies for post-failure procedures. However, a disaster recovery plan is just a subset of business continuity planning.

Disaster recovery plans are mainly data focused, concentrating on storing data in a way that can be more easily accessed following a disaster. Business continuity takes this into account, but also focuses on the risk management, oversight and planning an organization needs to stay operational during a disruption.

Business continuity development
Business continuity starts with initiating the planning project. Business impact analysis (BIA) and risk assessment are essential steps in gathering information for the plan. Conducting a BIA can reveal any possible weaknesses, as well as the consequences of a disaster on various departments. The BIA report informs an organization of the most crucial functions and systems to prioritize in a business continuity plan.

A risk assessment identifies potential hazards to an organization, such as natural disasters, cyberattacks or technology failures. Risks can affect staff, customers, building operations and company reputation. The assessment also details what or who a risk could harm, and the likeliness of the risks. The BIA and risk assessment work hand in hand. The BIA provides details on potential effects to the possible disruptions outlined in the risk assessment.

Business continuity management
It's important to designate who will manage business continuity. It could be one person, if it's a small business, or it could be a whole team for a larger organization. Business continuity management software is also an option. Software -- either on premises or cloud-based -- helps conduct BIAs, create and update plans and pinpoint areas of risk.

Business continuity is an evolving process. As such, an organization's business continuity plan shouldn't just sit on a shelf. The organization should communicate its contents to as many people as possible. Implementation of business continuity isn't just for times of crisis; the organization should have training exercises, so employees know what they'll be doing in the event of an actual disruption.

Business continuity testing is critical to its success. It's difficult to know if a plan is going to work if it hasn't been tested. A business continuity test can be as simple as a tabletop exercise, where staff discuss what will happen in an emergency. More rigorous testing includes a full emergency simulation. An organization can plan the test in advance or perform it without notice to better mimic a crisis.

Once the organization completes a test, it should review how it went and update the plan accordingly. It's likely that some parts of the plan will go well but other actions might need adjusting. A regular schedule for testing is helpful, especially if the business changes its operations and staff frequently. Comprehensive business continuity undergoes continual testing, review and updating.

Source: https://searchdisasterrecovery.techtarget.com/definition/business-continuity

Meet Our Intern
Mark Myers

Meet our new intern, Mark. Mark is currently a Senior at Carrol High School, where his favorite subjects are English and Computer Science. He is active in his high school's Champions Together program and plans to attend Purdue in West Lafayette next Fall. He hopes to get his degree in Cybersecurity there.

When he is not working or going to school Mark enjoys playing video games on the computer, he built for himself, and has recently started to develop his own games as well. Mark also enjoys playing with his French Bulldog, Violet and his two Labradoodles, Maggie and Mocha.

Please join us in welcoming Mark to the PITG team and if he visits your office, feel free to say hello, we enjoy having our interns get to know our clients.

Quarter 1 2021 Leadership Team Building
Windrock Park - Tennessee

Top Technology Trend for 2021 - Internet of Things (IoT)

Many “things” are now being built with WiFi connectivity, meaning they can be connected to the Internet—and to each other. Hence, the Internet of Things, or IoT. The Internet of Things is the future, and has already enabled devices, home appliances, cars and much more to be connected to and exchange data over the Internet.

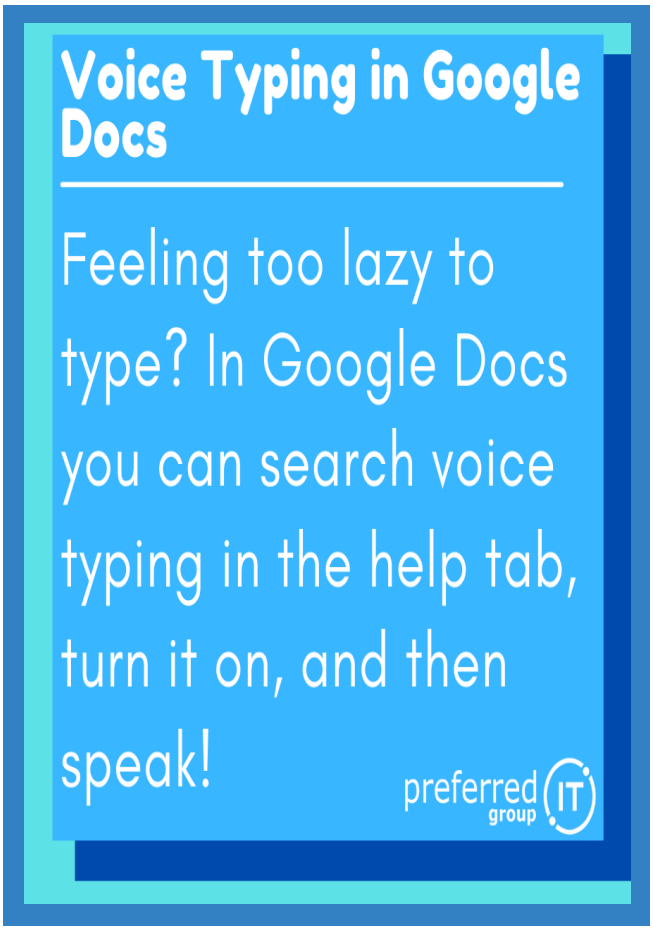
As consumers, we’re already using and benefitting from IoT. We can lock our doors remotely if we forget to when we leave for work and preheat our ovens on our way home from work, all while tracking our fitness on our Fitbits. However, businesses also have much to gain now and in the near future. The IoT can enable better safety, efficiency and decision making for businesses as data is collected and analyzed. It can enable predictive maintenance, speed up medical care, improve customer service, and offer benefits we haven’t even imagined yet.

And we’re only in the beginning stages of this new technology trend: Forecasts suggest that by 2030 around 50 billion of these IoT devices will be in use around the world, creating a massive web of interconnected devices spanning everything from smartphones to kitchen appliances. The global spending on the Internet of Things (IoT) is forecast to reach 1.1 trillion U.S. dollars in 2022. New technologies such as 5G is expected to drive market growth in the coming years.

And if you wish to step foot in this trending technology, you will have to learn about Information security, AI and machine learning fundamentals, networking, hardware interfacing, data analytics, automation, understanding of embedded systems, and must have device and design knowledge.

Source: https://www.simplilearn.com/

FUN FACT!



preferred IT group

CONTACT US

Fort Wayne
260.440.7377

Warsaw
574.306.4288

Columbia City
260.213.4266

Indianapolis
317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.