OCTOBER 2020 | VOL. 10

TECHNOLOGY TIMES

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY

How Person-Centered Cyber Training Supports Threat Prevention in Financial Companies

Financial services institutions must understand how to prevent cyber threats, which may require a ground-up approach.

Cyber security threats and preventive measures go hand-in-hand. Yet cybercrime continues to impose threats on the financial industry. Financial services firms are 300 times as likely as other companies to be targeted by a cyberattack," according to a report by the Boston Consulting Group. These threats can arise at any time and occur through various sources (external sources such as hackers, and internal sources such as staff members and contracted employees). Some financial companies have developed action plans with steps to take if a cyber-attack strikes, but cyber security best practices also includes establishing and initiating threat prevention methods. One example of a threat prevention method is person-centered cyber training.

Statistics show that cyber threat prevention is an immense pain point for many financial companies. In a survey of 400 security professionals in financial services, it was observed that financial institutions are better at detecting and containing cyber-attacks and less efficient at preventing them. Almost 56% of financial institutions are useful in detection, and only 31% are good at prevention.

Financial services institutions must understand how to prevent cyber threats, which may require a ground-up approach.

Financial institutions can take immediate measures to engage in threat prevention methods with person-centered training. This type of training allows an IT or cyber professional to practice and

WHAT'S NEW INSIDE KAMIND IT

October is National Cybersecurity Awareness Month! Make the most of this National holiday by taking the KAMIND IT FREE Security Assessment at: **kamind.com/cyber-security-assessement/**

Join KAMIND IT on **October 15th, 2020 for "Into The Breach** - A Cyber Defense Experience" to experience **Project Ares** first hand.

Register here: kamind.com/into-the-breach

How Person-Centered Cyber Training Supports Threat Prevention in Financial Companies

Continued from page one

hone skills by learning specific cyber lessons pertinent to the financial sector and applicable to their job role. The more upskilled the professional, the more they will be able to protect the company and company assets. A current platform that offers specific cybersecurity job role training is Project Ares.

Person-Centered Training with Project Ares

Project Ares is a browser-based learning platform designed for teaching cyber security in an engaging and hands-on applied method. This platform offers gamification and AI to train employees on the latest cyber threats and attacks. Project Ares is made up of foundational and specialized scenarios in the form of battle rooms and missions that address current cyber threats in the financial sector. The lessons within Project Ares are developed with specific job roles in mind.

For example, various scenarios are developed with the theme of a financial service, so the trainee can learn the skills needed to prepare for a cyber threat. In these specific financial missions, the trainee will learn how to **disable botnets, identify and remove suspicious malware, and protect the financial institution.**

- **Mission 1 –** Operation Goatherd "Disable Botnet" – Acting as a cyber mission force member, the trainee will access the command and control server of a group of hackers to disable a botnet network that is designed to execute a widespread financial scan triggering the collapse of a national bank.
- **Mission 4 –** Operation Arctic Cobra "Stop Malicious Processes" – The cyber trainee will analyze network traffic and stop a malicious exfiltration process.
- **Mission 5 –** Operation Wounded Bear "Protect Financial Institution" – The trainee identifies and removes malware responsible for identity theft and protects the financial network from further infections.

This individual or team-based mission training delivers collaborative skill-building experiences aligned to NIST/NICE work roles, ensuring the trainee meets specific cyber competencies. This kind of immersive, hands-on training gives learners the ability to practice various forms of threat prevention, which will benefit the company's overall security posture in the long run. The more trained cyber professionals are for their job roles, the more likely they will be able to safeguard against threats—and take proactive measures to better prevent cyber threats. If cyber professionals are prepared and well-informed

with the right knowledge and skills in their toolbox, threat prevention will be more attainable and achievable for professionals on the frontlines of defense. Professionals will be able to spot a cyber threat, but also prevent cyber threats from breaking the bank.

Discover The Immersive World of Project Ares

Project Ares is an award-winning, gamified learning and assessment platform that helps cyber professionals of all levels build new skills and stay up to speed on the latest tactics.

Discover more at www.kamind.com/project-ares

CIRCADENCE GOLD PARTNER

FBI, CISA Echo Warnings on 'Vishing' Threat

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) on Thursday issued a joint alert to warn about the growing threat from voice phishing or "vishing" attacks targeting companies. The advisory came less than 24 hours after KrebsOnSecurity published an in-depth look at a crime group offering a service that people can hire to steal VPN credentials and other sensitive data from employees working remotely during the Coronavirus pandemic.

"The COVID-19 pandemic has resulted in a mass shift to working from home, resulting in increased use of corporate virtual private networks (VPNs) and elimination of in-person verification," the alert reads. "In mid-July 2020, cybercriminals started a vishing campaign—gaining access to employee tools at multiple companies with indiscriminate targeting — with the end goal of monetizing the access."

As noted in Wednesday's story, the agencies said the phishing sites set up by the attackers tend to include hyphens, the target company's name, and certain words — such as "support," "ticket," and "employee." The perpetrators focus on social engineering new hires at the targeted company, and impersonating staff at the target company's IT helpdesk.

The joint FBI/CISA alert (PDF) says the vishing gang also compiles dossiers on employees at the specific companies using mass scraping of public profiles on social media platforms, recruiter and marketing tools, publicly available background check services, and open-source research.

"Actors first began using unattributed Voice over Internet Protocol (VoIP) numbers to call targeted employees on their personal cellphones, and later began incorporating spoofed numbers of other offices and employees in the victim company. The actors used social engineering techniques and, in some cases, posed as members of the victim company's IT help desk, using their knowledge of the employee's personally identifiable information—including name, position, duration at company, and home address—to gain the trust of the targeted employee."

The actors then convinced the targeted employee that a new VPN link would be sent and required their login, including any 2FA [2-factor authentication] or OTP [one-time passwords]. The actor logged the information provided by the employee and used it in real-time to gain access to corporate tools using the employee's account." The alert notes that in some cases the unsuspecting employees approved the 2FA or OTP prompt, either accidentally or believing it was the result of the earlier access granted to the help desk impersonator. In other cases, the attackers were able to intercept the one-time codes by targeting the employee with SIM swapping, which involves social engineering people at mobile phone companies into giving them control of the target's phone number.

The agencies said crooks use the vished VPN credentials to mine the victim company databases for their customers' personal information to leverage in other attacks."

The actors then used the employee access to conduct further research on victims, and/or to fraudulently obtain funds using varying methods dependent on the platform being accessed," the alert reads. "The monetizing method varied depending on the company but was highly aggressive with a tight timeline between the initial breach and the disruptive cashout scheme."

The advisory includes a number of suggestions that companies can implement to help mitigate the threat from these vishing attacks, including:

- Restrict VPN connections to managed devices only, using mechanisms like hardware checks or installed certificates, so user input alone is not enough to access the corporate VPN.• Restrict VPN access hours, where applicable, to mitigate access outside of allowed times.
- Employ domain monitoring to track the creation of, or changes to, corporate, brand-name domains.
- Actively scan and monitor web applications for unauthorized access, modification, and anomalous activities.
- Employ the principle of least privilege and implement software restriction policies or other controls; monitor authorized user accesses and usage.
- Consider using a formalized authentication process for employee-to-employee communications made over the public telephone network where a second factor is used to authenticate the phone call before sensitive information can be discussed.
- Improve 2FA and OTP messaging to reduce confusion about employee authentication attempts.
- Verify web links do not have misspellings or contain the wrong domain.
- Evaluate your settings: sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

krebsonsecurity.com - August 20th, 2020

KAMIND IT
5200 Meadows Road
STE #150
Lake Oswego, OR 97035

Prsrt Std
U.S. Postage
PAID
Permit No. 2358
Portland, OR

RETURN SERVICE REQUESTED
Jackson Biehn
KAMIND IT Inc.
5200 Meadows Rd
Lake Oswego OR 97035-3202
S1 P1

Do These Things To Protect Your Business From Getting Hacked

1. Train Employees. Your team needs to know how to identify and handle today's IT security threats. Cybercriminals often rely on your employees' lack of training to break into your network. Ongoing training gives employees tools and resources to overcome this and many other IT security challenges. Make training a top priority!

2. Hold Employees (And Yourself) Accountable. Training and company guidelines don't mean much without accountability. When you set rules, follow them, just as you follow industry and government rules and regulations when operating your business. Be willing to hold anyone who does not accountable.

3. Have A Disaster Recovery Plan. Things happen. When you store sensitive data, you need to have a plan in place to recover and restore that data should anything happen. This doesn't just include data loss from malicious attacks but other types of disasters, including hardware failure, fire and flood. How is your data being backed up and saved? Who do you notify in the event of a breach? Who do your employees call in the event of disaster? **SmallBiz Technology, Dec. 26, 2019**

4 Tips To Get Projects Done On Time With A Small Team

1. Give Them The Tools And Resources They Need
We all need tools to get things done – project management software, content creation tools, messaging apps, virtual private network access and more. Have a conversation about what each team member needs to maximize productivity and work closely with them to meet that need.

2. Set Aside Time For Proper Research
Don't jump headfirst into a project without jumping into research first. Information is a powerful tool to get things done efficiently and effectively.

3. Assign Accordingly
Before the team goes to work, make sure assignments or responsibilities are delegated properly and check in with everyone on a regular basis to make sure things are going smoothly (or to see if they need help).

4. Plan And Plan Again
Plan out the project before you set to work. Give yourself and your team a map to follow as you work through the project. As with any project, expect obstacles along the way and be willing to update your map accordingly. **Small Business Trends, July 4, 2020**

This monthly publication is provided courtesy of **Matt Katzer, CEO of KAMIND IT** & Amazon Best-Selling Author of ***"Securing Office 365 - Masterminding MDM and Compliance In The Cloud"***

KAMIND IT's Mission: "KAMIND IT Assists Organizations to Utilize Technology to Drive Innovation"