Fortalice

FIRST HORIZON AND IBERIABANK CLIENTS

For those that could attend today's event, it was excellent to be with you, even if virtually. For those that could not join us, not to worry; here are the details.

My goal is to share best practices for the most pressing topics given where we stand in the COVID-19 pandemic crisis.

Thanks, Theresa Payton

Discussion

1. Top 3 security risks to your business and how to mitigate them
2. Triple Threat for 2021 + 2 bonus predictions
3. Spotting and Stopping Manipulation Campaigns
4. Q&A

The Top 3 Security Threats:

Based upon our work with clients here are the top 3 threat hunting findings and attacks we have seen to date in this heavy work from home environment.

Caveat: Security changes are going to be hard for your users so consider frequent video webinars to roll out and demo the changes.

1. Automated account take over -- For collaboration tools such as Slack, automated account take over attacks are well underway. Attackers comb data breach dumps of passwords and corporate email accounts and reuse those.
   Mitigating control: *Search password dumps for your corporate email accounts and enforce 1:1 password changes by notifying the user. Consider a more frequent password reset policy during COVID-19.*

2. Business Email Compromise -- Socially engineering your work-at-home staff into changing wire instructions, sending money to the wrong place, presenting staff with fake purchase orders, and impersonating the CEO or someone that has authorization to request funds transferred.
   Mitigating control: *Domain name design; credentials; template protocol; text each other a code*

3. Security and Privacy Issues -- Almost all of the major video conference tools have had to deal with issues at some point. Google Hangouts, Zoom, RingCentral, WebEx, and Microsoft Teams have addressed various vulnerabilities that would allow an attacker to eavesdrop on a meeting or find recorded files stored on public cloud instances. Make sure you are very familiar with their security guides.
   Mitigating control: *Set security policy at the corporate level, train everyone in your company regarding the policy and how the settings impact the user experience via webinar. If you don't,*

you run the risk of employees deciding corporate policy "gets in the way" -- or they'll just use the other person's platform -- so they don't have to deal with complexities.

Mitigating control: *When employees leave your corporate instance of collaboration tools, they may not realize how unprotected they are. For example, Slack and Microsoft Teams collaboration tools are often open across industry-sharing, peer groups. These open forums have had challenges with malware being delivered through links and attachments.*

2021 Cybercrime Predictions

- COVID-19 innovations lead to innovation in cyber crimes
- 5G will accelerate cyber crimes
- Misinformation campaign hits global elections (Again!)
- AI Poisoning will be a "thing"
- Ransomware goes all in on cloud

How to Spot and Stop Manipulation Campaigns

- Read the book - wink! Available in hard cover, ebook, and audio formats at https://www.amazon.com/Manipulated-Inside-Cyberwar-Elections-Distort/dp/1538133504

- Have a digital disaster playbook for all of the 2021 predictions I mentioned

- Check trusted vetted news organizations by going to their site directly (3 – local, national, outside your country)

- Go to organizations such as factcheck.org or snopes.com

- Ask employees before clicking on links or opening attachments to think twice. If they still need to take action, this free tool can do a quick scan looking for danger -- https://www.virustotal.com/gui/

Free resource released by DHS' CISA: COVID-19 Exploited by Malicious Cyber Actors https://www.us-cert.gov/ncas/alerts/aa20-099a

FBI update on BEC scams: https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic

If you do suspect or want to report any type of COVID-19 fraud, the FBI has a special unit assigned to COVID-19. The Fraud Coordinator is Senior Litigation Counsel Shaun Sweeney at USAPAW.COVID19@usdoj.gov or 412-644-3500.

Fortalice

Draft Employee Etiquette Work From Home Policy For Your Staff

Dear Employee,

We hope this finds you doing well and staying healthy. As you conduct company business during COVID-19, please follow this work from home policy and guidelines:

Workspace

- Check your location and how it looks to the viewer on the video conference.
- Make sure the viewer cannot see sensitive information such as a whiteboard behind you with notes from a previous meeting.
- Be sure to remove from view all confidential or sensitive material.
- Be careful of messages and pop-ups if you are sharing your screen.
- Who else is around? This is not just about the people located in the same space as you.
- Are there voice-activated assistants around such as Google Home, Alexa, Echo Dot or even a smart TV as they could accidentally listen and/or record? If yes, consider unplugging them during work calls.