Fortalice

TIPS:

For those that could attend today's event, it was excellent to be with you. 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

- Top 3 security and how to mitigate them
- Triple Threat Cybercrime Predictions for 2021-2022
- Spotting and Stopping Manipulation Campaigns

The Top 3: Security Threats

Besides ransomware, there are other cybersecurity threats lurking. Focusing on the Top 3 Threats will also assist you with your ransomware detection and resiliency strategy.
Caveat: security changes are challenging to customer interactions and organizational activities so consider how-to-guides and video webinars to rollout and demo the changes.

1. Automated account take over -- For remote access platforms and accounts with privileged access, such as bank accounts or administration accounts, 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.
2. Business Email Compromise -- Socially engineering your 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 videoconference 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 on your company regarding the policy.

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.

Advice to Follow Back at the Office

- Design for the Human
- Model futuristic scenarios & practice playbooks
- Segment To Save It
    - Prevent Business Email Compromise / Wire Transfer Fraud by implementing a domain name that's not your public facing domain name, create credentials only used for money movement, talk to your bank about options, create a wire transfer template, consider each person has a code name not easily guessed
- Identity / Access Controls
- Books on internet safety, privacy, and manipulation campaigns:
    - Protecting Your Internet Identity: Are You Naked Online?
    - Privacy in the Age of Big Data
    - NEW BOOK -- Manipulated: Inside the Cyber War to Distort the Truth

Fortalice

2021 Cybercrime Predictions

- COVID19 Innovations Lead to Innovation in Cyber Crimes
- 5G will accelerate cybercrimes
- Misinformation Campaign Hits Global Elections (Again!)
- AI Poisoning will be a "thing"
- Ransomware goes all in on cloud

2022 Cybercrime Predictions

- XR will be hacked!
- Mini-Black Swan Banking Event
- AI Drives Misinformation Campaigns Without Human Intervention

How to Spot and Stop Manipulation Campaigns

- Read the book Manipulated - 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 & 2022 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/

Fortalice

Resources:

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

Ransomware Victim Organization No More Ransom: https://www.nomoreransom.org/en/index.html

Europol Ransomware Assistance: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/no-more-ransom-do-you-need-help-unlocking-your-digital-life

Avast's Free Decryption tools: https://www.avast.com/en-us/ransomware-decryption-tools

Trend Micro Decryption Tools: https://success.trendmicro.com/solution/1114221-downloading-and-using-the-trend-micro-ransomware-file-decryptor

Have a Question?

www.FortaliceSolutions.com

Email: Watchmen@FortaliceSolutions.com

Call: (877) 487-8160