PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

DGC
ACCOUNTING • TAX • ADVISORY
A DIVISION OF PKF O'CONNOR DAVIES, LLP

Cyber Roundup – August 2022

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory

As reported in one of the items below, a published software security flaw, glitch, or weakness found in software will likely be exploited by bad actors within a short time after the vulnerability is discovered and announced. It is, therefore, important for companies to have an effective program in-place on an urgent basis to combat the defect(s). The program should have the following characteristics:

- A person(s) who is responsible for understanding your environment and keeping abreast of the vulnerability publications that may impact the company.
- A dashboard or tool to allow for the successful identification of the specific assets impacted by the vulnerability(ies) that need to be updated.
- A process or tool to install the necessary updates to the impacted assets in a timely and risk-based approach.
- A dashboard or tool to validate the successful resolution of the issue.

Please contact us if you need assistance with designing and implementing such a defense program.

Key Cyber Events

The following is a rundown of trends and what's been happening recently in the cyber world. We welcome your comments, insights and questions.

- **T-Mobile and Wawa have reached settlement agreements for prior data breaches.** T-Mobile has agreed to a $500 million settlement for a 2021 breach that impacted the personal information of approximately 77 million individuals. $350 million is to be allocated to a settlement fund, while $150 million must be invested over the next two years by T-Mobile on data security and related technologies. Wawa has agreed to pay an $8 million settlement for its 2019 data breach that resulted in the theft of 34 million credit card numbers from their point of sale system.

- **In a report released by Palo Alto Networks, cyber criminals will begin to search for disclosed vulnerabilities within 15 minutes of publication**. A vulnerability is a flaw in a piece of software that can allow an individual to obtain access or manipulate the system in a way not intended.

  Tom's Takeaway: Over the years we have been consistent in promoting the need for organizations to have an effective program and process to identify and fix published software vulnerabilities in a timely manner. This Palo Alto Networks report further emphasizes the urgency.

- **Security researchers from Avast discovered a Discord server (chat application) of what appears to be teens selling different strains of malware.** The group will develop, market and upgrade the malware being promoted. Membership is based on a fee of $5 to $25. Approximately 100 individuals have signed up to the group.

- **Users of the Zelle payment app have been increasingly targeted by cyber criminals over the past year to divert funds away from unsuspecting victims.** The tactics utilized are standard social engineering tricks. The victim user will receive a phone call from what they believe to be their bank and, from there, the cyber criminals will leverage information they have on the victim from prior breaches to persuade a transfer. The Caller ID will be spoofed; as such, it will show the correct number for the bank, further adding to the legitimacy of the call. Unfortunately, fraudulent transfers that are directly authorized by the user will not be reimbursed by the bank.

Tom's Takeaway: Be it Zelle, Venmo, Paypal, or any other quick payment app, users have to be vigilant in both safeguarding access to those accounts and to whom they are transferring the money. With all of the breaches that have occurred over the past decade (and continue to occur), a lot of information about us, our habits and our finances exist for cybercriminals to leverage. One of the things we teach in cybersecurity awareness training is for individuals to always make sure to control the direction of communication. For example, a cybercriminal may be able to spoof the incoming call; however, they cannot be the recipient of the call when you call back a known good number. By taking control of the direction of the communication, more often than not, you will be able to avoid falling for a scam and speak with a legitimate entity to validate any requests.

- **Axie Infinity, an online NFT (non-fungible token – crypotocurrency) game, suffered a breach in March that resulted in the loss of $620 million.** The hack was attributed to two well-known hacking groups associated with the North Korean government. Recent reports indicate that the attack was the result of an elaborate scheme in which an engineer for Axie was targeted for a job offer on LinkedIn. The engineer took the bait and began to interact with the threat actors. To further the legitimacy of the job offer, the threat actors put the engineer through multiple interviews and eventually sent the engineer a malware-laden PDF document posing to be an offer letter. Once opened, the threat actors were able to obtain access to the internal network and transfer of the funds.

- **Oklahoma State University Health Center received an $875,000 fine from the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) for a data breach that occurred in 2018 impacting 280,000 individuals**. OCR's investigation found violations of the following key HIPAA rules:

  - Impermissible uses and disclosures of protected health information;
  - Failure to conduct an accurate and thorough risk analysis;
  - Failure to perform an evaluation;
  - Failure to implement audit controls, security incident response and reporting;
  - Failure to provide timely breach notification to affected individuals and HHS.

  Tom's Takeaway: Unfortunately, many healthcare entities may not have sufficient understanding of their compliance obligations, especially as it relates to the information security component of HIPAA. Having worked with many healthcare entities over the years, the above bulleted items are very common. One of the most important things a healthcare entity can do, as it relates to their information security, is to have a risk assessment performed correctly by a qualified third party. The risk assessment will form the basis of the entity's understanding of their systems and data as well as the implementation of control measures thereafter. If you are a healthcare entity and are in need of a comprehensive risk assessment, we can help.

- **Professional Management CO, a Colorado-based accounts receivable management company, disclosed a ransomware attack that impacted 660 of its healthcare clients.** The company claims they have not had an indication of misuse; however, highly sensitive personal information, such as Social Security and Medical Account Numbers, may have been accessed. The incident has impacted approximately 2 million individuals, making it the largest healthcare data breach of the year to date.

- **The National Institute for Standards and Technology announced their selection of the first set of Quantum resistant encryption algorithms.** While this sounds highly technical, this a major step forward in protecting our future online communications and data. In a Quantum computing world, our current data encryption protections will be bypassed with ease. Quantum computing requires Quantum protections. There is some relief to see movement in this area given the significant implications if not proactively addressed.

Contact Us

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Principal
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Nick DeLena, CISSP, CISA, CRISC, CDPSE
Partner
Cybersecurity and Privacy Advisory
ndelena@pkfod.com | 781.937.5191

Our Firm provides the information in this e-newsletter for general guidance only, and it does not constitute the provision of legal advice, tax advice, accounting services, or professional consulting of any kind.