Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

APRIL 2020

PRIVACY, DEEPFAKES CONTINUE TO BE EVOLVING CONCERNS

While cybercriminals continue to pursue ransomware and Business Email Compromise scams, it is expected that privacy, deepfake, and impersonation concerns will evolve in 2020.

Safeguarding data: Jeff Pollard of Forrester Research, Inc. explains in *Predictions 2020: This Time, Cyberattacks Get Personal* that while AI and Machine Learning (ML) are growing in value in order to improve offerings, the data that drives them may be more difficult to acquire. With the European Union's General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) in place, more customers may opt out of data-sharing agreements. At the same time, organizations are increasingly conservative with their data and reluctant to hand it over to third parties. This data shortage leads to less effective AI and ML solutions, creating a lockdown on data usage.[1]

Privacy as a human right: The focus on privacy continues to have a greater trajectory beyond the GDPR and CCPA oversight. Now that Apple has taken a stand designating privacy as a human right, organizations unwilling to adapt a strong stance on privacy may pay a price. In fact, leading in security and privacy may become a corporate differentiator. Help Net Security explains: "[Privacy] laggards may risk meeting the unseemly fate of past organizations that failed to embrace important technology paradigms such as internet, cloud, and mobile computing".[2]

Protecting against deepfakes: IT departments will ramp up investment in training and awareness around deepfakes this year.[1] Forrester anticipates that deepfake scam costs will exceed $250 million in 2020.[1] Deepfakes can also possibly impact stock prices with perceived CEOs, financial analysts, and other powerful economic figures making fake statements to move markets.[2]

Weaponizing with data from M&A activity: While laws limit data collection, M&A activity consolidates data on preferences, locations, and even medical history and conditions. To prevent data from landing in the hands of government-owned entities, companies are looking to form their own consumer data governance strategies to mitigate the risk of data misuse and even weaponization.[1]

Sleight of hand attacks disguise true intentions: Hybrid threat actors project themselves as one certain type of adversary, but are actually obfuscating their true intentions (e.g., a hacker targeting a customer database that is actually a nation state stealing intellectual property). This complicates organization threat detection and response when the true intent is unclear.[2]

[1] Pollard, Jeff. *Predictions 2020: This Time, Cyberattacks Get Personal*. Forrester Research, Inc. and/or its subsidiaries. October 30, 2019. https://go.forrester.com/blogs/predictions-2020-cybersecurity/.

[2] Help Net Security. *Cybersecurity industry predictions for 2020 and beyond*. Help Net Security. December 19, 2019. https://www.helpnetsecurity.com/2019/12/19/cybersecurity-industry-predictions-2020/.

(continued)

WHAT IS A DEEPFAKE?

A deepfake is a video that has been manipulated by weaving it with new images, audio, and video. Since 2017, when Reddit brought deepfakes into the spotlight, more and more deepfakes have been made using free, easy-to-use generative adversarial networks (GAN) machine learning technology. It is increasingly more difficult to discern between a real video and a deepfake. The presence of deepfakes can undermine the credibility of public figures and potentially be part of manipulations like fake emergency broadcasts or distribution of false election information.[1]

Deepfakes are also used as part of social engineering schemes. Hackers can now use social media for audio and video to aid in ID theft and create damaging videos and audio clips to extort money and/or data.[2] To identify discrepancies, security companies and education institutions are developing new detection technology using AI.[3]

[1] Townsend, Caleb. *Deepfake Technology: Implications for the Future*. United States Cybersecurity Magazine. https://www.uscybersecurity.net/deepfake/.

[2] Oza, Shyam. *Deepfake: The AI Endangering Your Cybersecurity*. Security Boulevard. December 6, 2019. https://securityboulevard.com/2019/12/deepfake-the-ai-endangering-your-cybersecurity/.

[3] Murphy, Hannah. *Cyber security companies race to combat 'deepfake' technology*. Financial Times. August 15, 2019. https://www.ft.com/content/63cd4010-bfce-11e9-b350-db00d509634e.

THE CASE FOR PASSWORDLESS AUTHENTICATION

The World Economic Forum released an article about passwords as part of its meeting in Davos, Switzerland in January 2020. The article discusses how password-free authentication methods can improve both the customer experience and cybersecurity.

Customer experience

Passwords are a factor in poor customer retention rates. In addition, password management is costly for organizations. With fingerprint readers and facial recognition now available, a seamless customer experience has become a consumer expectation.

Security risk

Organizations with weak password management can find themselves victims of breaches and credential stuffing attacks.

WHAT IS CREDENTIAL STUFFING?

Cybercriminals steal username and password combinations and then use them as part of large-scale automated requests to gain unauthorized access to user accounts.

Why Passwordless authentication

The World Economic Forum along with the FIDO Alliance suggest organizations transition to a password-free environment for several reasons:

- **A better user experience**: typing complex passwords is a struggle. It is easier for customers to use biometrics and authenticators for access.
- **Enhanced security**: passwordless authentication requires no transfer or storage of personal information and uses two distinct authentication factors.
- **Faster time to market**: certified solutions are now available to make it easier to implement passwordless authentication.
- **Reduced costs**: without passwords, organizations eliminate the compounded cost of employee and call center time to manage resets and lower insurance premium costs when there are no longer passwords to steal.

More information

World Economic Forum White Paper: *Passwordless Authentication The next breakthrough in secure digital transformation* – http://www3.weforum.org/docs/WEF_Passwordless_Authentication.pdf

FIDO Alliance – https://fidoalliance.org/

Source: Zwinggi, Alios and Ogée, Adrien. *4 reasons why passwords are becoming a thing of the past*, World Economic Forum. January 21, 2020. https://www.weforum.org/agenda/2020/01/4-reasons-passwords-are-becoming-a-thing-of-the-past/.

COVID-19 SECURITY RESOURCE LIBRARY

A resource library of information addressing COVID-19 security and privacy is available from the National Cyber Security Alliance (NCSA). It includes free, updated information on:

- Current scams
- Cyber threats
- Working remotely
- Disaster relief

Visit Stay Safe Online: https://staysafeonline.org/covid-19-security-resource-library/

Source: Stay Safe Online -- NCSA. *COVID-19 Security Resource Library*, 2020. https://staysafeonline.org/covid-19-security-resource-library/.

The information above is provided as a convenience, without warranties of any kind and MUFG Union Bank, N.A. disclaims all warranties, express and implied, with respect to the information. You are solely responsible for securing your systems, networks, and data. You should engage a qualified security expert to advise on your specific needs and requirements.

This *Cybersecurity News* contains news and information designed to help protect your company and employees.