Digital vulnerabilities

Introduction

Assume that you have been appointed to a task force of 5 or 6 computing professionals within your organization. You have been asked to examine the current issue outlined in the article below. Your team has not been asked to make specific recommendations to solve the problem. Rather, you have been asked to make recommendations that will help the Government decide what next steps they should take.

Prompts

1. What is/are the problem/problems here? Is there an underlying fundamental problem?
2. Who are the major stakeholders and what are their perspectives?
3. What are the major ethical, legal, and security aspects associated with the problem?
4. What are the intended and unintended consequences of existing computing solutions? Consider the consequences on individuals, organizations and society within local and global contexts.
5. What recommendations do you propose that may lead to potential solutions?

You know how to prevent malware from getting on your phone or computer: Don't click on pop-ups claiming you have won a free prize; don't click on links in emails that ask you to verify an account that you don't even have and always check whether a source is verified when downloading an app. But what about taking a WhatsApp call? Or opening a DM from TikTok? Or posting on Facebook Pages?

On Tuesday the 14th of May 2019, the *Financial Times* announced that the Israeli spy company, the NSO Group, had exploited a vulnerability in WhatsApp to remotely install surveillance malware. This vulnerability had the potential to allow an attacker to upload malicious code onto a phone by sending data that looked like a WhatsApp voice call. The target didn't even need to answer the phone for the malware to grant the attacker full access to personal information on the target's phone.

The vulnerability, identified as CVE-2019-3568, is a buffer overflow vulnerability in the WhatsApp VoIP stack which allows attackers to execute arbitrary code by sending specially crafted series of SRTCP packets. This is not uncommon and communication platforms that rely on VoIP stacks are known for having vulnerabilities. Messages and calls on WhatsApp are end-to-end encrypted which makes them invulnerable to being read by third parties while in transit. So the only way an attacker can gain access to a person's WhatsApp messages or calls is either on the sending or the receiving device.

In 2020 Microsoft released a patch for Windows 10 after a bug was discovered in Microsoft's CryptoAPI service. This is an essential part of the Window's operating system that allows developers to cryptographically validate the trustworthiness of software or data and generate authentication certificates. If the verification check isn't trustworthy, attackers can distribute malware and obtain sensitive data. Facebook too announced that it pushed a fix for a bug that doxed the account(s) that made posts or edits to Facebook Pages, denying them the anonymity that Facebook Pages had guaranteed. Another security vulnerability was found with TikTok's messaging system that allowed attackers to send users messages with malware with which they could take control of accounts, upload content and make private videos public.

Zero-day bugs, in particular ‘zero-click install’ vulnerabilities, are worth top dollars in the exploit market as they give governments, spy agencies and hackers extreme powers. NSO Group is thought to have sold spyware to Mexico and Saudi Arabia where such software has been used to keep close track of human rights activists, scientists, and journalists. Jamal Khashoggi is claimed to have been spied on by the use of NSO Group’s Pegasus spyware in the weeks before his murder. Privacy activists have criticized TikTok’s content policies and data practices and accused it of collecting data for Beijing. Jeff Bezos’ phone was allegedly hacked by the Saudi crown prince in reaction for the Washington Post’s coverage of the kingdom.

WhatsApp is the most popular instant messaging app in the world with one billion active users at any one time and 29 million messages sent every minute. Video and audio calls account for two billion minutes daily. TikTok has been downloaded more than 1.5 billion times and is on its way to becoming more popular in use than other social media. Windows 10 is installed on more than 900 million PCs around the world, making it the most used operating system. Although Facebook, Tiktok and Microsoft claim to have rectified security flaws within days of discovery, the consequences associated with these flaws are grave as it is the data of billions of people that are at risk.

A number of measures have been taken to prevent or reduce the risks associated with digital vulnerabilities. The UAE, Qatar and Oman, for example, prevent security breaches by banning VoIP voice and video communications. Encrypted modes of communication, it is argued, allow criminals to remain outside government and police radar. Facebook is expanding its bug bounty that encourages security researchers to submit security flaws for potential rewards. Such bounties have resulted in the discovery and subsequent repair of Facebook bugs. In 2018, WhatsApp paid $50 million to adopt the encryption protocol of Signal, which was thought to be the world’s most secure end-to-end encrypted messaging app. Signal’s encryption was supposed to bring a new level of privacy so that hackers, the police, government agencies and even WhatsApp itself couldn’t breach the privacy of users. The bugs, though, found their way in.

Word count: 744

FK: 13.2

References

Bergman, R., Frenkel, S., & Zhong, R. (2020, Jan. 8). Major TikTok security flaws found. *The New York Times*. Retrieved from https://www.nytimes.com/2020/01/08/technology/tiktok-security-flaws.html

Farid, S. (2019, Feb. 11). WhatsApp usage, revenue, market share and other statistics. *Digital Information World*. Retrieved from https://www.digitalinformationworld.com/2019/02/whatsapp-facts-stats.html

Goodin, D. (2019, May 14). WhatsApp vulnerability exploited to infect phones with Israeli spyware. *Arts Technica*. Retrieved from

https://arstechnica.com/information-technology/2019/05/whatsapp-vulnerability-exploited-to-infect-phones-with-israeli-spyware/

Khandelwal, S. (2019, May 14). Hackers used WhatsApp 0-day flaw to secretly install spyware on phones. *The Hacker News*. Retrieved from https://thehackernews.com/2019/05/hack-whatsapp-vulnerability.html

Newman, L. H. (2019, May 14). How hackers broke WhatsApp with just a phone call. *WIRED*. Retrieved from https://www.wired.com/story/whatsapp-hack-phone-call-voip-buffer-overflow/

Newman, L. H. (2020, Jan. 14). Windows 10 has a security flaw so severe the NSA disclosed it. Retrieved from https://www.wired.com/story/nsa-windows-10-vulnerability-disclosure/

Newman, L. H. (2020, Jan. 18). A Facebook bug exposed anonymous admins of pages. WIRED. Retrieved from https://www.wired.com/story/facebook-bug-page-admins-edit-history-doxxing/