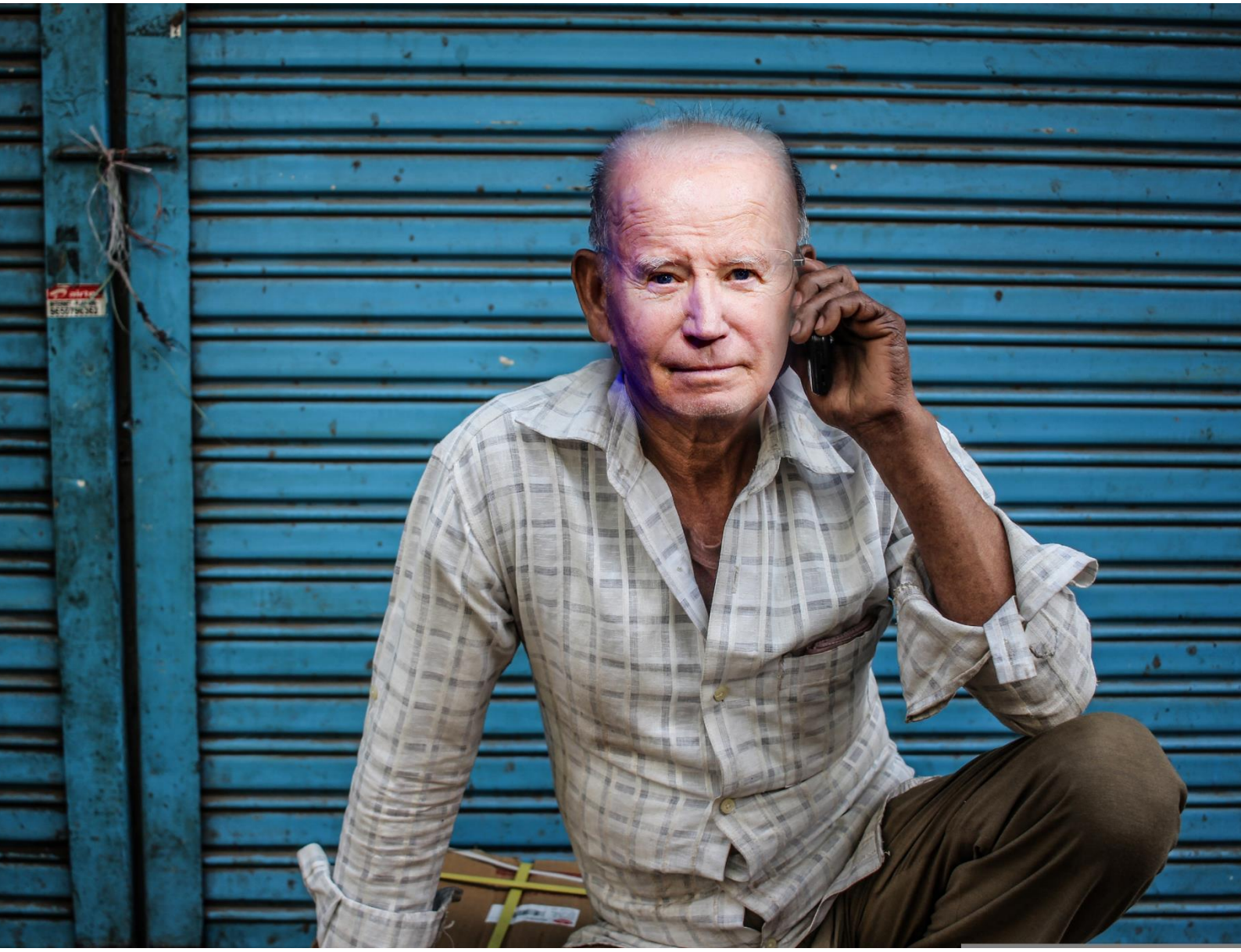
Cyberwatch Finland



WEEKLY REVIEW

WEEK 5/2024

”CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS”

Cyberwatch Finland

KEY TAKEAWAYS

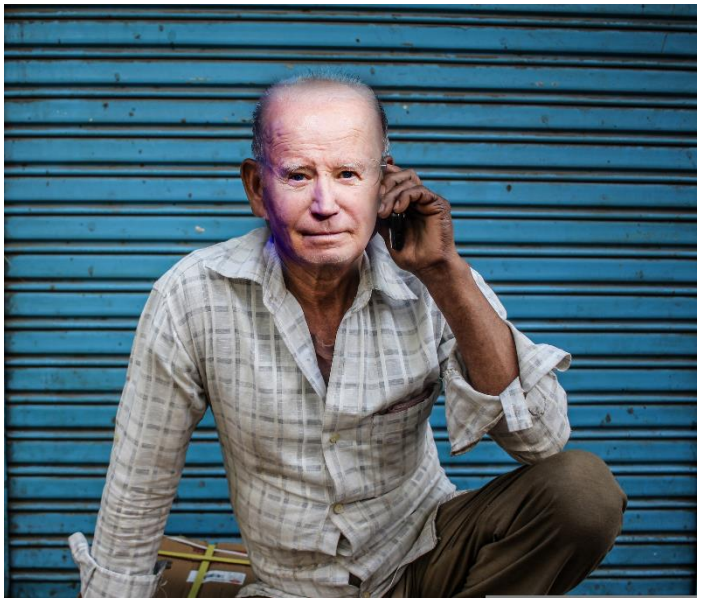
1. There is concern in the United States about disinformation about the upcoming elections, in particular about the impact of deepfakes on electoral behaviour

2. Organizations should be aware of and control all of the IT assets they manage and their open network ports.

3. Excessive supervision of employees can endanger personnel data protection and lead to sanctions against the organization.

1. DEEPFAKES AND CHINA CAUSE WORRY IN THE US PREPARING FOR ELECTIONS

U.S. security officials have raised concerns about outside interference in the upcoming presidential election this fall. Both the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) issued warnings in January. These concerns relate in particular to AI-based deepfakes, whose credibility is constantly evolving. If in the last presidential election the most ambiguity was caused by the contestation of the election results, the greatest threat in this election, according to the authorities, is the general chaos that deepfakes could cause.



Deepfake refers to a counterfeit that contains an video or sound that appears to be genuine and has been produced using machine-learning artificial intelligence. These are quite popular, and especially in TikTok and YouTube, one can find content, where politicians or celebrities are made to talk to each other about a wide variety of topics, such as video games. In the context of elections, deepfakes serve as a means of spreading mis- and disinformation and influencing the outcome of an election. Signals of the threat they pose in the United States were seen in January when, during the Democratic primaries, fake phone calls were used as a tool, in which the vote had been changed to that of President Joe Biden. This was used to conduct a phone call campaign in the state of New Hampshire, urging people not to vote at all. The impact of harassment remained unclear, but similar campaigns closer to the actual elections and spreading on social media, for example, could, at worst, affect voting behaviour.

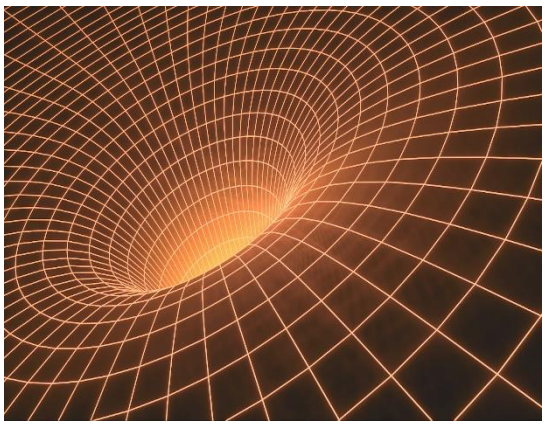
In the United States, deepfakes have also raised concerns about possible foreign interference in elections. In particular, the speeches by the authorities have highlighted concerns about China and its enormous cyber resources. Although China was not directly accused of making deepfakes, it was noted that it is an artificial intelligence superpower and the United States' most significant competitor in this field of technology. Chinese cyber influencing has recently been seen in connection with Taiwan's presidential election, for example, in the form of a large number of cyberattacks and fake news, so the threat must be taken seriously. However, focusing solely on China would leave many other players unchecked. The events that took place during the 2016 elections will certainly still be remembered. According to the report made afterward, the so-called Mueller Report, Russian special services actively seek to promote Donald Trump's election as president by, among other things, influencing social media, hacking various targets and publishing documents.

Deepfakes are not just a concern for Americans. In November in Slovakia, the far-right Republika Party used the voice of the leader of the Progressive Party in a deepfake as part of its election campaign. During the election campaign, there was also a high-quality deepfake of the same progressive party, in which, in a “secretly” recorded debate, there was talk of buying votes. Slovakia has a so-called electoral truce, which means that news coverage of elections must stop for a certain period of time before the vote. As a result, fact-checking in these cases remained in the hands of ordinary citizens and social media.

In the fight against mis- and disinformation, fact-checking, source criticism and good media literacy play a key role. If there are shortcomings in these, and especially if the media and social debate are polarised, as is the case in the United States, deepfakes can also sink into more fertile soil.

2. OPEN NETWORK PORTS AND CYBER THREATS

Network ports are critical network components that enable communication between two different devices or servers. They act as a kind of communication channels through which requests between devices are directed to the right places. For example, a server that maintains both an organization's website and acts as an e-mail relay uses network ports to distinguish between different types of communications. When the server receives a contact request from another device, it always includes information about which port the device wants to connect to the server. Based on this, the server knows what the contact is about and can direct it to the right service. The ports are numbered according to a standard. For example, when a user wants to connect to a specific server to read the web pages it hosts, that traffic always happens through the same dedicated ports. For example, web browsing is typically done using ports 80 or 443 while ports 25, 465, and 993 are used in email transmitting.



Because of the limited number of ports, their numbering is maintained by, the Internet Assigned Numbers Authority (IANA), which is also responsible, for example for allocating IP addresses. It upkeeps a list of so-called well-known ports through which traffic is always similar (ports with numbers 0-1023). In addition, there are network port numbers registered by companies with IANA that are reserved for specific applications (ports 1024-4951). However, server administrators can also use ports whose numbers are outside of these known or reserved port numbers. In this case, we are talking about so-called private ports, through which the traffic or operations taking place can be fully determined by the administrators (port numbers 49152-65535). These ports can also be used, for example, momentarily for server maintenance, various configurations or other organization-specific solutions.

Traffic through network ports is managed by keeping them either open or closed. If the port is open, the server receives traffic through this port. For example, servers that host websites needs to have network ports 80 and 443 open continuously. However, as a rule of thumb, all ports that are not critical to the operation of the services should be closed, as unnecessary open ports can pose a significant cyber threat. Through open ports, outsiders can connect to servers, and this possibility, combined with application vulnerabilities, for example, can provide an easy and, at worst, unattended line to an organization's IT assets. Cybercriminals use network scanners that make it possible to map the target organization's outwardly visible IT assets and find out which network ports are open on which servers. This makes it possible to find out which areas in the organization's infrastructure seem most important, but also which could potentially be penetrated.

For example, if several dozen ports are open for a server, it is possible that the traffic passing through all of them is not properly monitored, or that one of them can be used, for example, to copy data from the server or penetrate other parts of the network. Ports that are left open or poorly secured are used extensively in the early stages of cyberattacks. Gates and the traffic passing through them are also protected differently. For example, port number 21, which has previously been very commonly used for data transmission, is inadequate in terms of security by today's standards. The use of it and similar ports has largely already been abandoned, but if, for example, on an old server that is still active, this port is still open, it is a significant vulnerability.

Network port management is an essential part of active information security, but in organizations where there are many networked devices and the number fluctuates, for example, due to the purchase of new equipment, maintaining an active situational awareness is challenging. Open network ports are necessary and do not in themselves pose a cyber threat, but if they are not adequately controlled, it significantly increases the chances of attackers penetrating systems. Regular network scans are essential for threat protection. Mapping open gates is not difficult, which is why criminals may also do it at regular intervals for organizations of interest. Therefore, it is important for organizations to strive to ensure that the most up-to-date situational picture of their IT assets to be protected is available to them and not to criminals.

3. THERE ARE LIMITS TO EMPLOYEE CONTROL

Amazon received an administrative fine of €32 million from the French data protection authority based on the EU's General Data Protection Regulation. The reason for this was Amazon's excessive control of workers at its logistics facility in France. Too much information was collected about employees and not removed quickly enough.

Amazon's warehouse workers had equipment in place to scan all the operations they did, such as receiving, storing, sorting and reshipping packages. Amazon tracked the input provided by the scanners and made various statistics out of it. For example, the data was used to measure employee activity. If an employee did not receive an information feed for more than ten minutes, he or she may have to explain to the company the reason for the "break". The system also recorded the difference in time between 1 and 10 minutes between the scans performed by the employee. This made it possible to measure employee activity more accurately. Based on these statistics, the work was steered in such a way that, among other things, employees were transferred to other tasks. The DPA also pointed out that Amazon had retained the data it collected, and the statistical indicators obtained from it for an unnecessarily long time.

The above example was about monitoring warehouse workers, but nowadays the same thing is also talked about a lot, for example, in the IT industry and in connection with remote work in general. From a cyber security perspective, remote work creates challenges. The employer has very limited and strictly regulated possibilities to monitor employees' remote working practices. Many companies have said they have started monitoring how often hybrid employees come to the office for in-person work. Some companies even have a reward system in place to reward people for in-person work. In this way, companies bring employees under their own watchful eye and believe that the risk of abuse is reduced. The purpose, implementation and methods of technical supervision directed at employees must be discussed in co-operation negotiations before the method is introduced, whether it concerns remote or face-to-face work.

Amazon's systematic breach of employee privacy could equally be commonplace elsewhere. Differences in interpretation of the GDPR can lead to incorrect policies and even abuses. In addition, employees' poor understanding of their own rights may lead to a situation in which the employer's ethics of using methods in the supervision of employees are weighed. People are known to be the weakest link in an organisation when it comes to cybersecurity. For this reason, cyber-secure operations and following instructions should be part of the work culture. If this culture is strong and functional, even a little supervision is enough for the employer. For this reason, it is encouraged to maintain up-to-date training and instructions on cyber security operations in the organization.

REFERENCES

1. Deepfakes and China cause worry in the US preparing for elections

https://cybernews.com/news/fbi-nsa-cybersecurity-election-interference/
https://www.cnbc.com/2024/01/10/how-fbi-nsa-are-preparing-for-deepfakes-ahead-of-2024-elections.html
https://faktabaari.fi/fakta/presidenttiehdokkaiden-puheita-on-kloonattu-ja-muokattu-tekoalylla/
https://www.justice.gov/archives/sco/file/1373816/download
https://www.nbcnews.com/politics/2024-election/fake-joe-biden-robocall-tells-new-hampshire-democrats-not-vote-tuesday-rcna134984
https://www.nbcnews.com/tech/misinformation/joe-biden-new-hampshire-robocall-fake-voice-deep-ai-primary-rcna135120
https://www.politico.eu/article/china-bombards-taiwan-with-fake-news-ahead-of-election/
https://yle.fi/a/74-20056699
https://yle.fi/a/74-20071490

2. Open network ports and cyber threats

https://www.techtarget.com/searchnetworking/definition/port-number
https://riskxchange.co/1006756/open-ports/
https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/
https://www.all-about-security.de/identifying-secure-and-unsecured-ports-and-how-to-secure-them/

3. There are limits to employee control

https://www.cnil.fr/en/employee-monitoring-cnil-fined-amazon-france-logistique-eu32-million
https://tietosuoja.fi/usein-kysyttya-tyoelama
https://tyosuojelu.fi/tyosuhde/oikeudet-ja-velvollisuudet-tyossa/yksityisyyden-suoja/tekninen-valvonta
https://www.hs.fi/talous/art-2000010152480.html
Columba, Peoples, Vaughan-Williams, Nick. 2014: Critical Security Studies: An Introduction, 2nd edition. Abingdon. Routledge 2014.

Pictures: Pixabay