Focus On...

Helping you bring your organization into focus.™

March 2021 • Volume 11, Issue 03

CYBER

5 Biggest Cybersecurity Threats

How hackers utilize remote work and human error to steal corporate data

Inside This Issue

Since the beginning of the pandemic, the FBI has seen a fourfold increase in cybersecurity complaints, whereas the global losses from cybercrime exceeded $1 trillion in 2020.

World Economic Forum's "Global Risks Report 2020" states that the chances of catching and prosecuting a cybercriminal are almost nil (0.05%). Given the circumstances, business awareness and resilience is key to securing sensitive data and avoiding breaches.

Cyber threats are getting more sophisticated and intense amid the increasing levels of remote work and dependence on digital devices. Here are 5 that were the most damaging for enterprises in 2020.

1. Social engineering. In 2020, almost a third of the breaches incorporated social engineering techniques, of which 90% were phishing. Social engineering attacks include, but are not limited to, phishing emails, scareware, quid pro quo and other techniques — all of which manipulate human psychology to attain specific goals.

Cisco indicates that successful spear phishing attacks are accountable for 95% of breaches in enterprise networks. In fact, phishing attempts soared by 667% in March and 43% of workers admit having made mistakes that compromised cybersecurity.

2. Ransomware. Ransomware is a data-encrypting program that demands payment to release the infected data. The overall sum of ransom demands will have reached $1.4 billion in 2020, with an

FOCUS AUDITS™

CYBER

average sum to rectify the damage reaching up to $1.45 million. Ransomware is the third most popular type of malware used in data breaches and is employed in 22% of the cases.

3. DDoS attacks. There were 4.83 million DDoS attacks attempted in the first half of 2020 alone and each hour of service disruption may have cost businesses as much as $100k on average.

To form a botnet needed for a coordinated DDoS attack, hackers employ devices previously compromised by malware or hacking. Thus every machine can be performing criminal activity with its owner being unaware.

However, increasing traffic is not the only thing worrying cyber security experts. Criminals now employ artificial intelligence (AI) to perform DDoS attacks. The poison is the cure – AI can also be employed to look for the weak spots, especially if there is a massive amount of data involved.

This year organizations embraced remote work at unprecedented rates. The increased online traffic and dependence on digital services made them more vulnerable to cyber criminals. DDoS attacks don't cost much, thus there is an increasing supply of DDoS-for-hire services, leveraging the scale and bandwidth of public clouds.

4. Third party software. The top 30 ecommerce retailers in the US are connected to 1,131 third-party resources each and 23% of those assets have at least one critical vulnerability. If one of the applications within this ecosystem is compromised, it opens the hackers a gateway to other domains. A breach caused by a third party costs $4.29 million on average.

5. Cloud computing vulnerabilities. The global market for cloud computing is estimated to grow 17% this year, totaling $227.8 billion. While the pandemic lasts, the economy also witnessed a 50% increase in cloud use across all industries.

This trend is a perfect lure for hackers, who performed 7.5 million external attacks on cloud accounts in Q2 2020. Since the beginning of the year, the number of the attempted breaches grew by 250% compared to 2019. The criminals scan for cloud servers with no password, exploit unpatched systems and perform brute-force attacks to access the user accounts. Some try to plant ransomware or steal sensitive data, whilst others, use cloud systems for cryptojacking or coordinated DDoS attacks.

Corporate security challenges

Companies and their employees were thrust into a remote working environment rather suddenly, with many organizations' remote networking capabilities still not as shielded as their on-premise IT infrastructures. This rapid shift has left many unsecured gaps that malicious actors are constantly looking to exploit for financial gain.

The technological changes that shaped the workplace in 2020 are here to stay and so are the increasing cyber threats enterprises face. On account of that, the majority of executives say they will mainly spend their IT budgets on cyber resilience. Security teams have to develop strong policies to respond to the cybersecurity challenges, but that's only the first step. They need to effectively communicate those policies to the entire workforce and train employees to respond to them.

Source: Security Magazine, February 3, 2021
Juta Gurinaviciute

INFORMATION SECURITY

Focus Introduces Two Brand New Services

In our ongoing effort to provide you with the most valuable services, we recently added two new features to our offerings: ***Office 365 Audit*** and ***Fedline Compliance Assessment***.

Office 365 offers far reaching benefits for the modern workplace. Employees always have the most up-to-date versions with the newest features. Files can be accessed from anywhere. From a business continuity perspective, no matter what happens to equipment or facilities, Office is available. Collaboration and communication tools are additional benefits.

However, since the solution is cloud-based, it is paramount that the application be deployed and managed securely. The burden to ensure a secure environment is particularly salient for financial institutions who must meet GLBA requirements. While Microsoft shares security responsibilities, organizations are equally responsible for implementing the proper architecture and enabling the proper configuration settings.

Utilizing the Center for Internet Security 's (CIS) Microsoft 365 Foundations Benchmark as a framework, Focus Audits will audit the quality of supervision, policies and internal control procedures promulgated by the financial institution. To be clear, the purpose of this engagement is to audit the setup and use of Office 365 when comparing to an industry Best Practice Framework. This engagement does not assess the inherent security of the application.

The FedLine Solutions Security and Resiliency Assurance Program requires that participating institutions be compliant with applicable Federal Reserve Bank policies, procedures, and security controls by December 31, 2021. Because of the evolving cyber landscape and the growing attacks on payment networks and systems, a risk-based, holistic approach has been recommended by the Federal Reserve Banks. Not only are security features embedded in the solutions themselves, but participating financial institutions must validate that endpoints used to interact with the Federal Reserve Banks are secured. Some institutions have been required to utilize an independent third party to perform a compliance assessment.

Focus Audits' documentation will identify a specific control within six areas and describe how each control is to be utilized. Recommendations to harden the security of the controls will be provided.

If you are interested in learning how these new services may be able to benefit your organization, please reach out to your Account Manager today!

COMPLIANCE

CFPB Proposes Mortgage Servicing Changes to Prevent Wave of COVID-19 Foreclosures

Millions of homeowners expected to exit forbearance in the coming months

The Consumer Financial Protection Bureau (CFPB) today proposed a set of rule changes intended to help prevent avoidable foreclosures as the emergency federal foreclosure protections expire. Due to the COVID-19 pandemic and ensuing economic crisis, millions of families nationwide have suffered the loss of income and nearly 3 million homeowners are behind on their mortgages. The CFPB's proposal seeks to ensure that both servicers and borrowers have the tools and time they need to work together to prevent avoidable foreclosures, recognizing that the expected surge of borrowers exiting forbearance in the fall will put mortgage servicers under strain.

The COVID-19 pandemic and ensuing economic crisis have contributed to widespread housing insecurity across the nation, and many families are at risk of foreclosure when federal emergency protections expire. The number of homeowners behind on their mortgage has doubled since the beginning of the pandemic—6 percent of mortgages were delinquent as of December 2020. More homeowners are behind on their mortgages than at any time since 2010, which was the peak of the Great Recession. Industry data suggest that nearly 1.7 million borrowers will exit forbearance programs in September and the following months, with many of them a year or more behind on their mortgage payments. The CFPB's proposal, if finalized, would:

Give borrowers time: Every one of the nearly 3 million borrowers behind on their mortgages should have a chance to explore ways to resume making payments and avoid foreclosure. To make sure borrowers aren't rushed into foreclosure when a potentially unprecedented number of borrowers exit forbearance at around the same time this fall, the proposed rule would provide a special pre-foreclosure review period that would generally prohibit servicers from starting foreclosure until after December 31, 2021.

Give servicers options: The proposed rule would permit servicers to offer certain streamlined loan modification options to borrowers with COVID-19-related hardships based on the evaluation of an incomplete application. Normally, with certain exceptions, Regulation X requires servicers to review a borrower for all available options at once, which can mean borrowers have to submit more documents before a servicer can make a decision. Allowing this flexibility could allow servicers to get borrowers into an affordable mortgage payment faster, with less paperwork for both the servicer and the borrower. This provision would only be available for modifications that do not increase a borrower's monthly payment and that extend the loan's term by no more than 40 years from the modification's effective date.

Keep borrowers informed of their options: The CFPB also proposes temporary changes to certain required servicer communications to make sure that, during this crisis, borrowers receive key information about their options at the appropriate time.

Source: ***Compliance Alliance, April 5, 2021***

AWARENESS

Malicious System Update App Targets Android Users With Malware

Malware Steals Data, Messages, Images; Takes Control of Phones

Android users are now facing a new malware threatening their personal information. The new Android malware poses as a System Update app that actually delivers spyware on the target devices.

New 'System Update' Android Malware
Researchers from Zimperium Labs zLabs have shared details about a new malware targeting Android users. As observed, this new malware is basically spyware that poses as a 'System Update' app to trick Android users.

Briefly, this remote access trojan (RAT) reaches a device once the victim user downloads the malicious app. Once installed, the malware then stealthily executes to take control of the device and steal data.

Regarding the data it accesses, this includes messages, database files of messenger apps, clipboard data, notifications, contacts, call logs and other device data. It also records audios and calls, takes pictures through device cameras, lists the apps installed on the device, and accesses GPS location.

It then transmits the exfiltrated data to its Firebase Command and Control (C&C) where it first registered the infected device. Whereas, at the time of device registration, it transmits certain details to the C&C such as the existence of WhatsApp on the device, battery status, internet connection, storage status, and Firebase messaging service token.

Tactics To Stay Undetected
Unlike most other Android malware, this spyware doesn't continuously exfiltrate data in bulk. Rather it activates every time a change in the data is made, for instance, the addition of a new contact or new photos. It then only steals the most recent data.

Also, in the case of videos or large image files, the malware prefers stealing the thumbnails instead. Since they are small in size, stealing thumbnails won't impact the bandwidth, thus keeping the malware hidden.

Besides, the malware also ensures not to transmit more stolen details over the mobile data connection. It waits for the device to connect to WiFi to transmit data stolen from all folders.

Moreover, the malware also hides the app icon from the menu to remain hidden. More details about this malware are available in Zimperium's blog post.

Malware Not On Google Play Store
The researchers have confirmed that this malicious System Update application doesn't exist on Google Play Store. Hence, this scam particularly threatens the Android users who frequently use third-party app stores.

Thus, to prevent oneself from becoming a victim, all users must avoid interacting with third-party app stores.

Source: LHN, Abeerah Hashim March 29, 2021

Focus Audits, LLC
11301 N. US Hwy. 301
Ste. 105
Thonotosassa, FL 33592
(813) 638-8565
www.FocusAudits.com