Deloitte.

A fresh perspective

Nigeria Cyber Security Outlook 2021

January 2021

MAKING AN IMPACT THAT MATTERS since 1845

Introduction

We titled 2020 a year of shifts, and we believe for many people and businesses, it was a rollercoaster of different 'shifts' and adaptations. The pandemic has been a major backdrop to many events in the world, which undoubtedly affected cyberspace too.

The year 2020 closed with a significant shift in the magnitude of cybersecurity attacks and data breaches on SMEs, health institutions, public, private, financial and non-financial institutions in Nigeria and the world at large. The attacks targeted a lot of personal devices, cloud tools and remote working infrastructure used during this period.

As we enter the year 2021, the economic and social situation largely remain the same, although with a much positive outlook given the development of vaccines in different countries. For cybersecurity, we expect some events will happen in Nigeria given the prevailing trends in social, economic and political events around the world.

1

The Sharp rise of deep fakes

'Fake news' and misinformation have been a familiar rhetoric within the last few years. Regardless of how loosely these words might be used, this phenomenon represents a growing threat within the world at large and in the Nigerian social media space. We are in the era of easily accessible information, commoditised content creation and consumption. Different people recognise this and create content geared towards shaping social narratives and discourse. In the face of this, we also have mischievous people who, in a bid to change these narratives and social positions go on a deliberate campaign of misinformation and 'fake news' either via untrue or altered content including videos and photos. While trying to combat this rise in misinformation, a novel and more sophisticated digital threat that might prove more challenging to stop is lurking – Deep Fakes.

Deep Fakes are hyper-realistic, manipulated digital elements such as sounds, videos, and photos generated using artificial intelligence and machine learning tools and algorithms. In other words, they are unreal digital representations with the aim of looking and sounding as real as possible.

In 2021, we envisage a possible rise of deep fakes within the Nigerian cyberspace. It will become imperative to verify the legitimacy of different types of media online, especially during social, political and economic discourse. Therefore, it becomes increasingly important that the public remains cautious about content online and try to verify using different tools at disposal.

In 2021, we envisage a possible rise of deep fakes within the Nigerian cyberspace.

2

Man at Both Ends

Business Email Compromise (BEC) is not new in Nigeria. However, we will see it grow in sophistication and complexity as attackers are getting more creative and patient with their schemes and methods. This shift in technique, especially in sectors reliant on third party vendors and suppliers, takes the Man-in-the-middle attack pattern a step further by compromising both the victim organisation (customer) and a legitimate third-party/ supplier's email infrastructure. By so doing, the attacker has visibility and control over the flow of information and only needs to alter the payment details of either party. Hence, at both ends; you have an attacker manipulating the flow of information eventually resulting in payment being made into wrong accounts. We expect many more of this kind of sophisticated "Man at Both Ends" attacks launched against large organisations and SMEs in 2021.

Businesses need to ensure that appropriate email security controls such as multi-factor authentication and strong password policies are in place. Employee awareness about social engineering (the non-technical tactics hackers use to obtain sensitive information) should also be done periodically. It is important to stress that the attack's success may largely depend on the weakness in controls around payment authentication, verification and authorisation within the Organisation. Therefore, it is necessary to have strong processes and mechanisms in place and strictly adhere to them.

It is important to stress that the attack's success may largely depend on the weakness in controls around payment authentication, verification and authorisation within the Organisation.

3

More tools, more skills, more ground to play

In the last quarter of 2020, we saw some unprecedented and significant cyber-attacks against major cybersecurity and technology firms, including FireEye and SolarWinds. These attacks were attributed mainly to certain nation-state actors and Advanced Persistent Threat (APT) groups. These waves of attacks resulted in the theft of proprietary, internal and unreleased security tools as well as the breach of the SolarWinds security monitoring product through the exploitation of a backdoor written in the code. We are yet to start seeing the full effect of these attacks, and it remains imminent that some of these tools and exploits will start emerging within forums on the dark web and eventually in the 'wild'. There is certainly a lot to uncover from these attacks, and we will possibly see a lot more breaches tied to these attacks as investigations progress.

These attacks make it resounding that any organisation, irrespective of their prowess will face cybersecurity threats. Attackers are getting creative and audacious, and we expect more daring attacks on cybersecurity service/solutions providers and tech organisations.

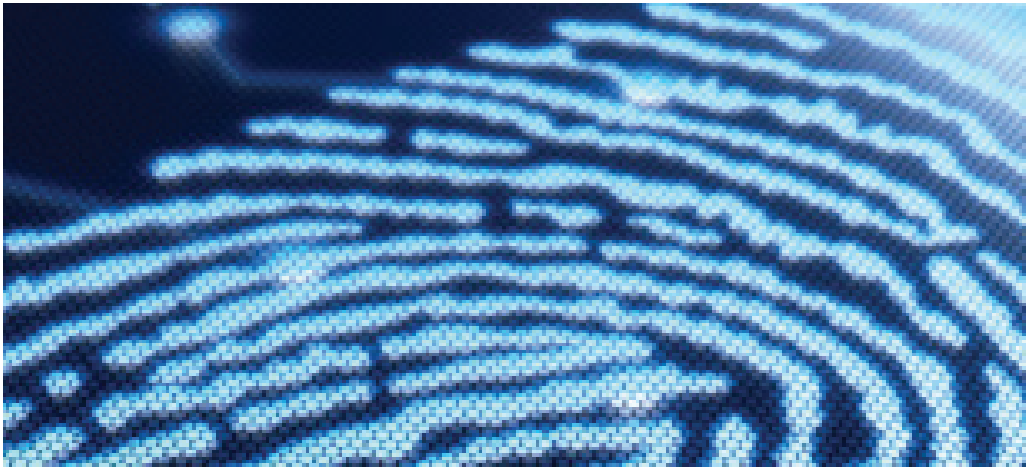
4

Signature-based antivirus will go extinct in many organisations

Defensive capabilities are moving away from rule-based and signature-based products to products driven by machine learning and artificial intelligence.

It is evident that signature-based products, especially anti-malware, are playing catch up, given the number of new malware strains and the adaptive nature of new malwares. We expect more organisations to recognize this challenge and move away from signature-based products to embrace products that offer machine learning and artificial intelligence capabilities. Many of the popular antivirus companies are now providing AI based antivirus solutions.

Many of the popular antivirus companies are now providing AI based antivirus solutions.

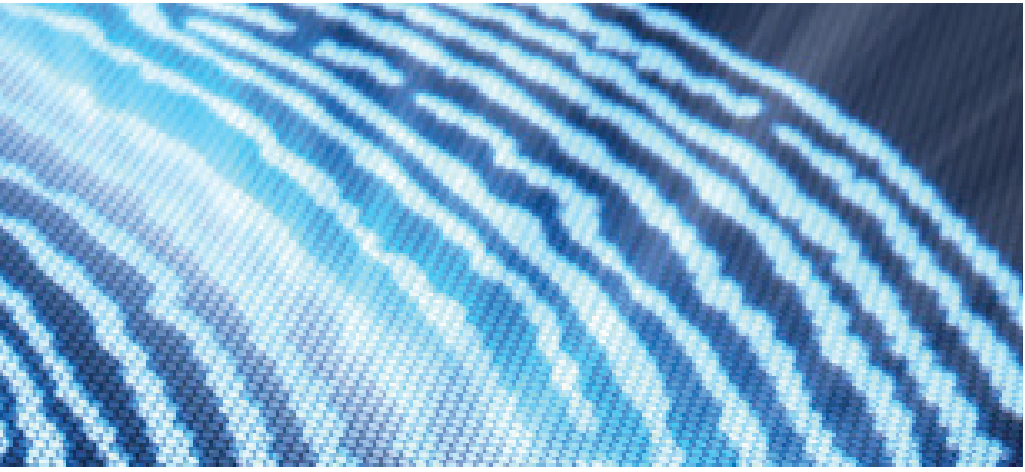


5

The spotlight will be on Nigeria

As a result of the #ENDSARS protests and the involvement of several Hacktivist groups in the protests leading to a wave of attacks on governments, private and public web infrastructure, the spotlight may now shift to Nigerian companies as attackers may feel they are seemingly easier targets. Government and public institutions are likely to face data leaks and sensitive information breaches motivated by local and foreign groups. However, on the flip side, we are likely to see international donor agencies increase financial support towards cybersecurity awareness.

Government and public institutions are likely to face data leaks and sensitive information breaches motivated by local and foreign groups.



6

The eventual death of single passwords

With many organisations still maintaining their Work From Home (WFH) directives, it becomes necessary for users to access corporate environments remotely. This brings a myriad of security challenges for organisations in terms of protecting and ensuring secure access to resources remotely.

Many studies have shown that about 80% of data breaches were caused by compromised, weak, and reused passwords. Evidently, using passwords alone has its weaknesses. As long as they are meant to be remembered, they are predictable. While we do envisage that passwords as we know it may die off completely in the nearest future, 2021 will see many organisations enforcing different types of multi-factor authentication mechanisms for all of their users irrespective of their privileges. There will also be increased adoption of the zero trust architecture to combat remote working threats. This trend started a few years ago, and more adoption will be seen in 2021.

Many studies have shown that about 80% of data breaches were caused by compromised, weak, and reused passwords.

7

Phishing attacks will still reign; they will be bigger, better and bolder

In 2020, Google reported about 46,000 phishing websites created every week, representing a 20% rise in the number of phishing websites created in 2019. It is no doubt that the pandemic motivated and presented fraud opportunities to many malicious persons. As we move into 2021, with the pandemic entering its second wave in several countries and vaccines' increasingly available, we expect this phishing schemes to get more daring and take advantage of the social and economic conditions.

...we expect these phishing schemes to get more daring and take advantage of the social and economic conditions.

8

Back to the drawing board

Businesses will have to rebuild their security strategy and architecture to accommodate the new normal (i.e. remote working). Before now, several organisations' security architecture was built around having users in a controlled physical environment using tools that have been configured by the Organisation. However, this architecture will have to change given that a majority of the workforce are working from "unsecure" remote locations and using devices that may be below the security standards of the organisation.

We will also see organisations build strategies geared explicitly towards circumstances like pandemics and how businesses can sustain their operations without compromise during times like this. We will see more Business continuity plans with strategies to cope for unusual circumstances, remote working plans that are security intensive among other plans and strategies.

Businesses will have to rebuild their security strategy and architecture to accommodate the new normal.

9

Cybersecurity will become imperative for business survival

Just a couple of years ago, only large organisations had good cybersecurity programs as they felt they were visible to attackers. Many SMEs were not paying attention to security because of probable sentiments that they had little to no attack surface and visibility. However, recent times have shown us that this is not the case as SMEs are continuously being attacked. Several SMEs also have minimal capacity to detect, prevent or respond to these attacks appropriately. This trend is unlikely to stop as attackers now see many SMEs as easier targets due to their unwillingness to invest in security. In 2021, we will see a lot more SMEs improving their cybersecurity programs and increasing their security budgets to enhance cyber resilience and protection.

We also expect to see an upsurge in the number of security professionals in 2021, and they will be moved from the background to being trusted allies from planning to execution. We may even see organisations having security professionals as part of their board and executives.

In 2021, we will see a lot more SMEs improving their cybersecurity programs and increasing their security budget to enhance cyber resilience and protection.

There will be more regulations around Cybersecurity and Data Privacy/protection.

Over the past two years, many businesses in Nigeria have implemented the Nigerian Data Privacy Regulation (NDPR). As the number of attacks increases and data leak and breaches occur, we are likely to see more stringent cybersecurity regulations and enforcement around security safeguards in place by businesses, especially those within data-sensitive sectors.

In 2020, we saw a lot of discourse around the Social Media bill. The Government explored different avenues to regulate social media majorly due to misinformation concerns, especially during the #EndSARS protests. While this came with much resistance, we expect more discourse around social media regulations and perhaps some semblance of a government regulation to address the different concerns.

In 2020, we saw a lot of discourse around the Social Media bill.

Conclusion

2021 will prove to be a very interesting year in the economy, health, business and cybersecurity will not be left out. Last year showed us that security will always be a major concern irrespective of seemingly tough times as attackers are always looking for an avenue to exploit security weaknesses and profit off them. An introspection into the lessons and events in the past will help us develop foresight and adequately prepare as we progress in the New Year.

Businesses need to focus on beefing up their cybersecurity programs, implementing initiatives to continuously monitor internal people and system activities, proactively managing vulnerabilities and risks, test incidence response and business continuity plans and assume a position of being already breached. Most times, all it takes is just one successful entry by the attackers; hence businesses cannot afford to be lax about their security. We wish you a secure 2021.

Tope Aladenusi
Leader, Cyber Risk Services
Deloitte West Africa
Email: taladenusi@deloitte.com.ng

Deloitte.