Cybersecurity outlook for

2021

The right approach to building cyber resilience

ManageEngine
Log360

One single vulnerability is all an attacker needs.

-**Window Snyder,**
Chief Security Officer

Introduction

History will remember the time when the world was brought to a standstill by the COVID-19 pandemic. Considered the most disruptive global crisis in more than 100 years, the pandemic has presented an unrivaled challenge to public health, food supply chains, and the functioning of the world. Organizations and individuals worldwide have been forced to embrace new practices such as social distancing and remote working. New plans and policies are being drafted by various governments every day to stabilize their country's economy, and to minimize the effects of the disruption.

Having said that, while the world is working to strike a balance between health and economic stability, cybercriminals are exploiting the crisis. After COVID-19 was declared a pandemic by the World Health Organization on March 11, 2020, almost 88 percent of organizations worldwide, made it mandatory or encouraged their employees to work from home. In the next few months, the world became far more digitally connected than ever—and more vulnerable than ever.

Today, IT infrastructures are reflecting rapid changes with organizations adopting cloud-based and hybrid solutions to supplement or replace on-premises platforms. These decisions permanently change the way these organizations do business. This surge in online operations has also impacted remote work, and increased the risk of cyberattacks exponentially.

Despite that the past year was filled with great uncertainty for the IT sector, it stimulated a substantial learning curve, and an awakening to cybersecurity. 2020 provided invaluable lessons and insights into what we can expect, and what we should do to protect ourselves in 2021.

Let's take a look.

Dual cybersecurity mindset is the new standard

As of April 2021, employees have started returning to work in offices as the pandemic induced restrictions are slowly being relaxed. However, due to a second wave in some countries, a majority of organizations are planning to continue semi-remote telework until the later part of the year, as the end of the pandemic is still uncertain. Facebook is one of the eminent tech companies that announced it will let employees work from home permanently, while Google has allowed employees to work from home until at least July 2021.

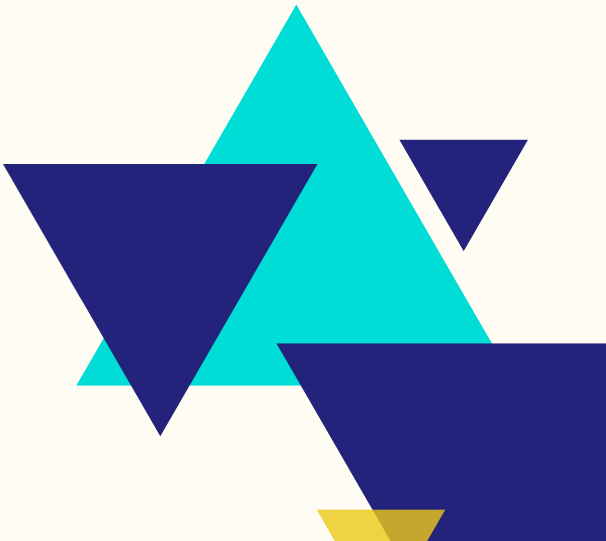
The extensive shift to remote work is not a bad thing. It has given the world an opportunity to accelerate the move towards cloud services, and paved the way for digital transformation. However, the unforeseen shift has presented a pressing challenge for information security, as remote work environments usually do not have the same safety measures in place as an office. An employee at the office works behind multiple layers of defense systems. When employees leave the office perimeter and work at home, it is easier for them to make a security mistake. This has created the need for strict additional security policies to mitigate the new risks that come with remote work.

Organizations and their cybersecurity specialists should conform to the dual cybersecurity mindset: focus on security measures for offices, as well as remote and virtual workplaces.

They have to adapt existing defenses to a new infrastructure paradigm that minimizes the exposure to the plethora of novel cyber threats and security risks that come with remote work, oftentimes where the entry points are the employees' home internet connection.

A majority of companies continue to rely on VPNs to enable their employees to work from home. Certain countries, like Canada, Austria, and the Netherlands, saw a 200 percent increase in VPN usage in March 2020. While this is a viable solution in the short term, from a security perspective, it is not sustainable for the long haul. VPNs act only as a band-aid solution to connect remote employees to their organizations. Having VPN security measures and tools in place enables organizations to focus on continuously monitoring devices and VPN connections to detect malicious activities and possible security risks.

As organizations start preparing for a post-pandemic world, one thing is beyond doubt: the workforce expects to continue to have the flexibility to work remotely. According to a Cisco report, this key shift for employers and their labor pools requires organizations to make significant changes to move to a hybrid workplace.

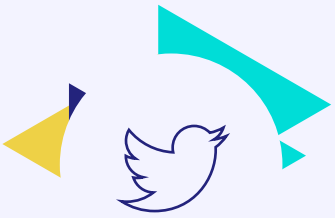


Leveraging incidents of the past

In 2020, we witnessed a drastic enhancement in the sophistication and the techniques used by hackers to infiltrate networks. Organizations, large and small have become victims, and we've seen some renowned companies, with presumably top-grade security, fall prey. Regardless of how dreadful such events are, we can always learn from the lessons of these cyberattacks, and increase our understanding of how to better protect our IT infrastructure.

Let's take a look at some of the notable cyberattacks of the past year, and how they were executed.

The Twitter breach

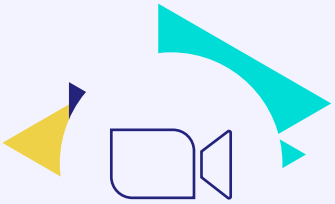


Twitter is one of the most popular social media platforms in the world; its users were astounded by a cyberattack on July 15th. The breach came to light when influential global personalities, like Barack Obama, Bill Gates, Elon Musk, and Jeff Bezos, seemed to post identical tweets encouraging their followers to contribute bitcoins via a donation link that would benefit "the community". Apart from this, the tweets also came from as many as 45 verified, but compromised, Twitter accounts, including those of renowned companies like Apple and Uber, each one having millions of followers.

- After an investigation, Twitter revealed that the attackers used social engineering techniques to target a small number of its employees.
- Executing a phone spear-phishing attack, the attackers exploited the employees' credentials to access Twitter's internal systems, and gain sensitive information on their processes.
- Using this information, the attackers targeted additional employees who had access to Twitter's account support tools.
- These privileged access tools enabled the attackers to infiltrate 130 Twitter accounts, tweet from 45, access the private messages, including photos and videos, of 36, and download the data of seven.

The implications were that the stock market value of Twitter plummeted, and cost the company's reputation heavily. Unfortunately, many followers of the compromised accounts also lost their money by falling prey to the deception.

Zoom(ing threat)



The shift to remote work took Zoom from a barely known service to one of the most recognized and widely used video and audio conferencing platforms in a short span. It experienced exponential growth with its Q2 2020 earnings, surging 355 percent year-over-year. The quick growth came with added security risks.

In April 2020, more than half a million Zoom account credentials—usernames and passwords—were available for sale on the dark web. IntSights explain that the attackers carried out the breach in four steps.

- First, they collected existing databases from multiple online crime forums and dark web markets that sold usernames and passwords which were compromised in previous data breaches.
- Then, they used an application stress testing tool, and pointed it to Zoom. Such tools are readily available on the internet.
- Step three involved a credential-stuffing attack that engaged multiple bots to impersonate normal users logging in to their Zoom accounts, but which used compromised passwords. This type of attack creates lags between attempts, and avoids accessing the same IP address to prevent being detected as a denial of service (DoS) attack. A login means that the credentials successfully masqueraded as valid.
- Finally, the credentials that were found to be valid were collated and bundled together as a new database for sale.

Essentially, this attack did not breach Zoom itself, but was carried out using a collection of recycled and stolen passwords. However, that doesn't mean the company had appropriate security measures in place. A simple cross-check audit with a password dumping site, such as "have I been pwned", could have prevented this major data breach. In addition, a number of security flaws in the application itself have led to numerous security incidents within the past year.

The Marriott cyberattack

The data breach of hospitality giant Marriott International came to light on March 31st, when it announced that the sensitive information of more than 5.2 million guests had been breached.

- An investigation revealed that the network of an unspecified hotel chain had been hacked.
- The hackers obtained the login credentials of two Marriott employees, and accessed the entire guest details database.
- The hotel giant revealed that the breached data consisted of contact details, loyalty account information, personal details like gender and birthdays, and other personal preferences.

The cost to the company in fines for violations of the GDPR, and a massive loss of reputation, amounted to GBP 18.4 million, or more than USD 25 million.

The takeaway from past security incidents

All organizations need to be vigilant. Although we have discussed incidents of large corporations getting breached, cyberattacks can happen to any organization—big or small. If attackers can hack large organizations, it's even easier for them to attack a smaller one. Smaller organizations could go out of business quickly if they are challenged by a cyberattack.

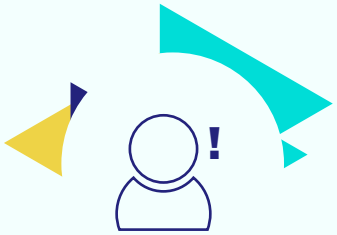
Here are some key takeaways from our analysis of cyberattacks in 2020.

Companies are considering cybersecurity as an IT issue

Approaching cybersecurity as just an IT issue is one of the biggest mistakes that organizations are making today. They are focusing on protecting personally identifiable information (PII), but failing to guard information regarding their strategies, policies, and processes. This, in turn, leads to attackers and insiders capitalizing on this information by executing social engineering and spear-phishing attacks.

Instead, organizations should rethink cybersecurity as a business priority. All employees should be educated about how a cyberattack can erode trust, and lead to other adverse consequences. Instead of relegating cybersecurity solely to the IT department, organizations should merge security practices with business operations to improve its overall security posture. In addition, necessary measures should be taken to identify indicators of compromise (IoC) from malicious insiders.

There is an uptick in human error

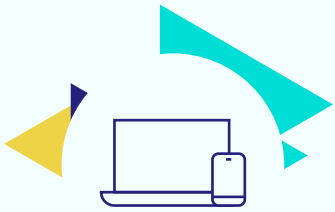


The common denominator in almost all cyberattacks that took place in 2020 was human error. From massive data breaches to email accounts getting hacked, a cyberattack is often triggered when an individual clicks on a malicious link nonchalantly.

The best way to combat human error is to educate the workforce to identify hacking techniques, and train them to prevent security blunders from happening. The infamous Twitter breach could have been prevented if the targeted individuals had recognized and avoided the social engineering attack.

Teaching the workforce to spot suspicious emails, and confirming with an administrator before sharing critical information, such as credentials, and circulating information on recent successful attacks, are some of the ways you can improve your cybersecurity posture.

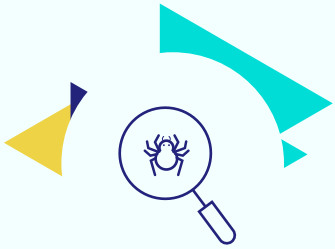
MFA is not being implemented effectively



Multi-factor authorization (MFA) is a technique to prevent hackers from gaining entry to your online services, data servers, or network using stolen credentials. Taking the Twitter breach as an example again, the incident could have been avoided if the company had insisted on a strong multi-factor authentication process to access the account support tools.

MFA adds extra layers of security beyond a simple username and password to help ensure only authorized users gain access to critical resources.

Threat hunting is rarely done

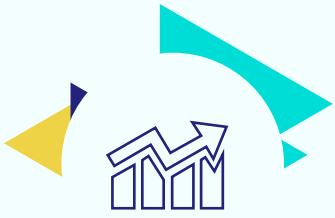


A major cybersecurity challenge for many organizations is realizing when they are under attack.

Traditional security strategies, such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and SIEM systems, offer a reactive form of security. These measures typically involve a remediation technique after a security incident has been detected. In contrast, threat hunting provides a proactive approach that involves searching for threat actors that might have already slipped through various layers of defense, and are lurking undetected in your network.

Cyber threat hunting is important as it digs deep to find indicators of compromise (IoCs), such as unusual network patterns, malicious user and entity behavior, and unauthorized configuration changes. Prolonged and targeted cyberattacks, such as advanced persistent threats (APTs) that evade an organization's security systems, can be detected using threat hunting techniques.

Companies don't stay updated on security trends



Having access to the latest security trends and feeds enables you to secure your systems against emerging threats.

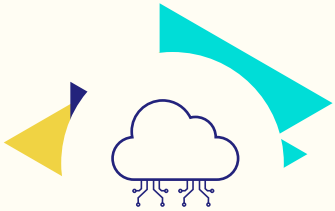
Sources like MITRE ATT&CK and InfraGard provide a knowledge base of adversary tactics and techniques gathered from actual security incidents and observations from around the world.

This information can be critical for identifying malicious IP addresses, URLs, or domain names. Armed with this information, IT administrators can create secure firewall rules, or modify existing policies to keep threats at bay.

What to expect in 2021?

Let's get to the most important question. What will cybercriminals bring to the table in 2021? Here are the top four developments we can expect in 2021.

The cloud will remain a top target



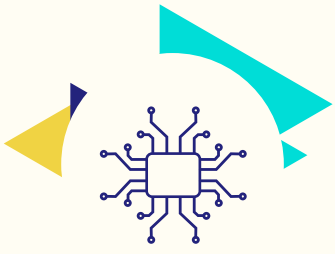
Global cloud security threats saw a huge spike in 2020. According to a report by computer security software company McAfee, global cloud-based cyberattacks increased 630 percent between January and April 2020. We can expect this trend to increase in 2021, as more organizations move their infrastructures to the cloud. Organizations that migrate to the cloud find an unparalleled level of flexibility.

But that flexibility, if not properly secured, plays to the advantage of the threat actor. Hackers constantly target opportunistic gaps in a cloud platforms' security structures. A cyberattack against an insecure cloud system will result in non-encrypted PII, hard coded passwords, and other sensitive data being exposed to the threat actor.

Beware of ransomware

We have witnessed a massive spike in ransomware attacks in 2020. In the wake of COVID-19, unprecedented amounts of ransom were demanded as well as paid. Ransomware incidents are predicted to get worse in 2021, and to evolve in terms of scale, efficacy, and impact. Most of the attacks will be targeted towards individuals, schools, hospitals, and small businesses as opposed to large corporations. This is because a lack of proper cybersecurity measures makes these entities an easy target for cybercriminals.

Weaponized AI is just around the corner

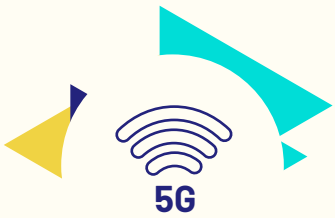


Developments in artificial intelligence (AI) have induced massive progress in innovation and automation. While AI can be used by organizations to protect themselves from cyberattacks, it can also be used by hackers to launch complex and fully automated attacks. A major reason for this is because AI research is publicly available, and it can be used by an attacker to build intelligent and self-learning exploits.

Intelligent evasion techniques, covert data exfiltration, and self-activating propagation are add-ons that AI provides to traditional malware. Hackers can also use AI to develop constantly mutating malware that can mimic legitimate programs to avoid detection.

The best methods for fighting AI-based attacks are to use AI-based defenses. Employing AI-powered security solutions is the most effective way to prepare for the paradigm shift in the threat landscape.

The implementation of 5G: Higher speeds mean faster attacks



5G is a major step towards total connectivity. It will drastically enhance the connectivity between billions of devices, the Internet of Things (IoT), and cloud-based applications. It will inspire a new generation of applications, services, and business opportunities. Greater speeds, low latency, and a dramatic expansion of bandwidth will unlock tremendous potential across several industries. On the other hand, it also means that a much greater attack surface is available for threat actors to leverage.

Battle plan for 2021

Most of the threats we've discussed can be minimized or remediated by taking the right precautions. A major concern is that many organizations and individuals don't realize the threat until it's too late.
Here are five steps you can take to protect your organization from imminent threats in 2021.

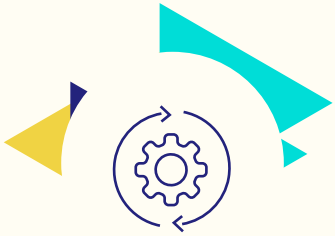
Secure your organization's cloud

Ensuring your organization's cloud is secure is the need for the hour in 2021.

- Optimize identity and access management (IAM), and privileged access management (PAM) strategies to enforce least privileged access policies to sensitive data.
- Adopt customer-controlled keys to encrypt data; this is crucial for mitigating data breaches.
- Reevaluate your cloud framework, and look for security vulnerabilities in it. Devise a clear plan on how to identify, isolate, and correct configuration errors in the cloud environment.
- Take additional precautions: implement MFA, use strong encryption techniques, employ efficient anti-malware solutions, and other strategies.

If implemented properly, all of the above strategies will minimize the risk of cloud threats to your operations.

Automate security at every stage



Cybersecurity automation includes continuous monitoring, auditing, alerting, and response. Use security solutions, including security automation and orchestration (SOAR), robotic process automation (RPA), and security information and event management (SIEM), to help you automate security efficiently.

Automation combined with AI is an effective layer of defense against cyberattacks, and crucial for relieving overburdened IT security teams. By implementing security automation in an organization's network, the cybersecurity teams can focus on activities that are more critical. It also minimizes the risk of human error.

Reevaluate your IT infrastructure regularly

To ensure cyber resilience, it is important for companies to reevaluate their entire IT infrastructure on a regular basis, and look for hidden security bugs and loopholes. A thorough analysis of your IT framework, including devices, applications, networking tools, policies, workflows, and databases, will provide insights into security risks, points of weakness, and help you understand which assets require other actions, such as maintenance, upgrades, etc.

Deploy a unified log monitoring system

Log monitoring enables you to identify malicious actors in your system. Given the large amount of log data generated by various components of an IT system, it is impractical to review all of these logs manually each day. Using a unified log monitoring system allows you to track your entire infrastructure using rules to automate the review of logs from different sources, and highlight events that might represent problems or threats.

A log monitoring solution with built-in AI and machine learning capabilities will increase your opportunities to detect anomalies and mitigate cyber threats.

Stay updated on security trends

From a security perspective, it is vital to stay abreast of the current global threat landscape. Staying informed about the latest security threats helps you adapt to trends and implement effective defense strategies. It will also help educate users about the new types of malware, attacks, and scam techniques.

Security alerts and advisories help you keep your organization's network secure. A simple update or product patch can prevent a massive data breach. Attending cybersecurity events is also a great way to stay updated on the current cyberattack trends and learn how you can mitigate them.

Conclusion

This past year was one of the most challenging in history. The global pandemic has forced organizations to pause and reprioritize. Cybercrime is fast-growing, and is not expected to be tamed anytime soon.

With no end to the global pandemic in sight, it is safe to assume that a significant portion of the labor force will continue to work from home. As hackers prey on the susceptibility of individuals new to working remotely, organizations should explore solutions that optimize and improve their processes as they address new cybersecurity challenges.

It is crucial to understand the hackers' level of sophistication and determination. Organizations should consider cyber threats as a massive impediment to their business and cybercrime should be considered as seriously as any other crime.

Cybersecurity teams should try to understand the motivation of threat actors. This will help you improve your strategies for combating cyberattacks. For example, a malicious insider's motivation could be financial gain or revenge against the organization by disrupting operations. In such a case, the indicators of compromise (IoC) to look out for would be unusual outbound network traffic and privilege misuse. Similarly, the IoCs for cybercriminals motivated to steal PII include an increase in database read volume and geographical anomalies.

Further, the development of cybersecurity knowledge and expertise is crucial to improve preparedness and resilience. Planning for and implementing the strategic techniques described in this report will help you fight cybercrime effectively.

About the author

Samson Santharaj is a computer science engineer on ManageEngine's product marketing team. He is skilled in IT security and compliance management. He regularly writes articles and e-books on key IT security topics and provides strategic cybersecurity guidance to security professionals and organizations around the world. Check out his blogs here.