HOXHUNT

Cybersecurity in a hybrid work environment

Table of Contents

Introduction

The past year has fundamentally changed the way we work today and how we will work in the future. Before 2020, companies that offered the possibility of remote work to their employees were considered forward-thinking. They understood that all employees do not need to be in the same location to be productive and drive the company forward.

When COVID-19 became a reality, employees had to start working remotely almost immediately to maintain business continuity. It was an enormous change both for the companies and people that have never worked fully or partly remotely. Everybody became familiar with collaboration tools like messaging applications, video conferencing, or file-sharing overnight.

We will never return full-time to the office

Now experts estimate that even once the global pandemic is over, we will never return to work solely from the office. PWC estimated that 83% of employees would want to work once a week from home, and 55% will want to continue working fully remotely.

Moving completely to remote work has been a challenge for IT leaders and security teams for the past year. The storm is not yet gone. The hybrid environment will continue to be a cybersecurity risk in the years to come. While employees will most likely thrive in this environment by being more productive and maximizing their work-life balance, attackers will try to take advantage of this vulnerability.

We will take a look at what hybrid work means for security operations, the risks, and how you can enhance your security using technology and training.

What does hybrid work mean for IT leaders & security teams?

According to a recent report from Tessian, half of the organizations surveyed were hit by a security incident while employees were working remotely in 2020. In their survey, 75% of the respondents stated that they believe that remote work will remain significant, and a hybrid workforce will continue to have many unique cybersecurity challenges that IT leaders and security teams must prepare to resolve.

Phishing, ransomware, and social engineering continue to be dangerous

One of the primary findings of the report was the increase of phishing and ransomware attacks that were targeting employees. Email-based threats have been a top priority for CISOs to tackle for years, and at Hoxhunt, we have seen an increasing interest in preparing people to face social engineering attacks.

The hazards of BYOD, home network, and public WiFi

Another issue is that employees could be using their personal devices for work, their family members could have access to their work devices, or their home network is more vulnerable to threats and attacks than the one at the office. This means they could be downloading unsafe applications or malware, or they would access data from unsafe devices.

In addition to working from home, more than ever, security leaders need to consider that people may be doing work through public WiFi.

“

75% believes that remote work will remain significant.

Improving cybersecurity while maintaining productivity

Of course, while employee well-being and productivity are vital for an organization, security operations need to come up with a plan that identifies the risks of the hybrid work environment to prepare multiple layers of security solutions that defend the company’s network, data, cash, and intellectual property.

To mitigate the most likely threats, IT leaders can identify how to update both their technical defenses and security awareness training to minimize the risk of a breach, but also to maximize the benefits of the changing work environment for the employees. While 34% of leaders are afraid that maintaining security during hybrid work will put pressure on their teams, with good planning, the right technology, and adequate training, you can remove the stress from your teams and employees.

“

A hybrid work environment could increase the opportunities for attackers to launch a successful attack.

The risks of hybrid work

The hybrid environment could increase the opportunities for attackers to launch an attack.

- The home network may not be secure enough, and people may use the factory settings.

- People may use their own devices, even if not a computer, and they may connect their printers to the device. According to Hacker Noon, printers are a major attack vector, and hacking unsecured printers is easy.

- Smart devices could also be hacked to listen to what the victim is saying, for example, in online meetings.

- Not updating the devices can result in vulnerabilities that attackers could easily utilize.

- Downloading free applications could be problematic.

- Family members could have access to the employees' devices, which could result in errors and, consequently, in a successful malware attack.

- Incidents that could occur in an office work environment, like clicking on a phishing email link, can happen in the home office too. It's even easier to fall victim to them when there are no people around to ask for help from when the employee is second-guessing the email.

- Attacks starting from a home network could enter the company's network rather easily. This could be a starting point for a distributed denial-of-service (DDoS) attack.

- Not using a VPN could mean that someone attacking the network could monitor the employee's computer easily.

- Insider threat continues to be a major concern and a potential risk to data security. Employees have unprecedented access to data, and without supervision, it could be easy to capture or compromise data by accident or for new employment or financial gains.

- People are more mobile, which means that they may be working using public WiFis.

“

Both technology and training will play an important role in your defenses.

Phishing and email-based threats remain the top attack vectors

Attackers tend to utilize unfortunate events for their own gain. This hasn’t been different during the global pandemic. The pandemic has been the perfect opportunity to prey on people’s fear, curiosity, anxiety, or vulnerability. Moving to remote offices has been a unique situation that we have never experienced before, and it instantly has an effect on people; many felt stressed, overwhelmed, or even isolated.

It's no wonder that phishing scams have been on the rise. Not long after the pandemic has started to take over the world, reports showed a 667% increase in phishing emails. Even the FBI has issued a warning regarding the alarming increase of scams.

As Tessian stated, between March and July 2020, 68% of the survey respondents admitted that they clicked a link or downloaded an attachment. Of all incidents, 49% started with a phishing attack. It's no wonder that organizations consider phishing as one of the top priorities that they need to tackle.

Examples of Email Threats

Phishing	Phishing is a type of social engineering where the attacker attempts to obtain sensitive data by impersonating a trusted entity.
Spear phishing	Spear phishing is a highly-targeted form of phishing attackers use to send personalized emails to well-researched targets (often to executives or people with access to money).
Malware	Malware can be harmful files or software, most typically delivered as an attachment or through a malicious link.
Ransomware	Ransomware is often delivered through emails. Ransomware encrypts the victim's data and systems and demands a fee to get the access back.
Spyware	Spyware infects the victim's systems to gather sensitive information.
Credential theft	Attackers are trying to harvest credentials, for example, by spoofing a trusted online website to get the victims to give away their login credentials.
Business email compromise	Attackers send an email message that appears to come from a trusted source, for example, they could be asking someone to conduct a wire transfer as soon as possible.

Bringing security to the hybrid work environment

To start, policies, service level agreements (SLAs), and data processing agreements (DPAs) should be updated to reflect the challenges of the hybrid work environments.

When you are reviewing the policies, make sure that you concentrate on the paragraphs that consider work-from-home rules. Don't only focus on the users' security behavior, but plan if a breach would happen how will you ensure business continuity by responding to the incident and mitigating it.

When you update your policies and create new processes, communication is key. You can't expect people to review the security policies by themselves. You actively need to communicate it to make sure that it sticks. You may want to collaborate on this with someone from your internal communication team to make sure that you reach your employees. This is the first step to preventing attacks in hybrid work environments. In your communication plan, you also need to leave space for technology and training.

Both technology and training will play an essential role in defending your organization from a breach.

Technology defenses for hybrid work environments

On the technology side, you can use a lot of tools to improve your security position. We've listed some of the essential measures that you can implement to keep your users safe.

1. Email filtering and scanning

Email filtering solutions can filter both inbound and outbound email traffic and scan messages to classify them as phishing, spam, malware, adult, bulk, virus, impostor, suspicious links, and more.

2. VPN

With a virtual private network (VPN) setup, users have privacy, anonymity, and security when they are using their home network or private WiFi.

3. Multifactor authentication

Multifactor authentication (MFA) is an electronic authentication method that allows users access to accounts only after they have provided two or more pieces of evidence that they own these accounts.

4. Endpoint protection

With endpoint protection, you can defend computer networks that are remotely connected to your main network.

5. Encryption

By setting up encryption on computers, you can protect the data stored on the devices as the encryption will turn them into an unreadable format.

6. Anti-virus

With anti-virus software, you can detect and remove known malware and prevent an attack. It’s important to note that new attacks are emerging and anti-virus software may not catch those.

7. Password manager

A password manager is a digital vault that securely stores passwords or login information. With it, users can create strong passwords, and they can automatically use it when they access applications.

8. Backups and securing critical data and resources

Make sure that all vital data are secure and that you have backups in case an incident happens.

9. Access governance

With centralized access governance, you can safely and easily manage who has access to your company’s resources.

10. Safe collaboration tools for virtual workspaces

Provide your employees with safe collaboration tools, like Teams, Slack, Dropbox. These methods are safer than sending sensitive documents and information to your coworkers via email. These tools also enable people to collaborate in real time.

11. Insider threat detection software

Insider threat detection software can send real-time alerts of suspicious behavior to isolate outliers quickly and minimize risks.

Training can add a layer of security in the form of a human firewall

As a cybersecurity provider, we cannot emphasize enough how important it is to train your employees frequently with realistic simulations. We saw new threat vectors and phishing emails constantly emerging, especially at the beginning of the pandemic: attackers were utilizing COVID-19 as their primary theme, preying on people's fear and anxiety.

Cybersecurity awareness training will be more important than before. You can't ignore the basics, especially when you have new people joining your company that may have never received any education before or they come from a completely different security culture. At the same time, you need to emphasize the need to change people's cyber behavior. It's important to teach people the habit of being careful when using their emails and report potential threats. You can achieve alertness and contribution through frequent, up-to-date, and personalized training.

When people start reporting threats, make sure that the processes are clear for employees on what to do so that you can start mitigation work as soon as possible. The process should be simple and positive so that employees dare to come forward.

When the training is engaging for people, they don't mind participating because it's also deeply integrated into their workflow without disrupting their productivity; it's easier to build cooperation with them to support your defense work. Security awareness training needs to resonate with people, so it wouldn't be just another burden for them.

As 58% of all IT leaders are planning to introduce more training, the emphasis will go toward finding training providers that can truly capture people's interest and give them lessons on how they can protect their employers' assets and take these skills to their personal lives as well.

Security should not hinder people’s productivity

Accommodating the new hybrid work environment hasn’t been easy for most people, but as the survey results show, people have learned to enjoy its benefits and want to continue working from home. This is a fact security teams cannot ignore, and they need to update their playbooks to reflect on the unique challenges of remote work.

While at the moment, it may seem like a burden to create plans, buy new technologies, and take your training to the next level, in the long-term, it will pay off. A majority of people clearly enjoy the freedom that remote work brings to their lives, and it can improve their productivity, which is beneficial for any company.

Focus on improving people’s security behavior step by step. Forming a habit takes time, but it’s the most beneficial for your defenses. At the same time, people will learn to be safer also in their private lives.

HOXHUNT

www.hoxhunt.com