CLOUD4C

Cybersecurity in the times of Covid19

Authors:

Imran Iraqi
Principle Technology Advisor - Cloud
Cloud4C

Madhav Singh
Associate Vice President
Cybersecurity Center of Excellence, Cloud4C

The pandemic poses unparalleled cybersecurity challenge the world over for enterprises adopting the 'Work from Home' culture. A change in approach coupled with the right security measures can help cybersecurity teams optimize their security posture.

Abstract

As Covid-19 bolsters its spread globally, online networks continue to be a breeding ground for ransomware and phishing attacks. Cyberattackers are having a field day. With more than 9000 corona-themed attacks in India in 3 months and about 19 million similar attacks in the whole of Asia around the same time, it is evident we are in for a major cybersecurity crisis. In fact, there is a sharp rise in cyberattacks including phishing, malware, ransomware and DDOS-for-ransom attacks.

The perennial security threat

Microsoft Corp Corporate Vice President (Cybersecurity Solutions Group) Ann Johnson explains, “Between February 2 and May 2, we saw 9,100 total file encounters related to COVID-19 or coronavirus. It means our detection tools actually saw malware or URL or an attachment or a phishing email that was using COVID-19 as a lure to get somebody to download malware to the system or potentially to give up their credentials via a phishing attack.” She further adds, “That is exacerbated by the fact that workforces are now largely remote and under a lot of stress. They may not have been equipped in their homes to work remotely."

Covid-19 has presented very unique challenges in the operational environment for cybersecurity leaders. Cybersecurity is not a novel concept and there are organizations that have fortified their security way before the pandemic hit us. Even then, the potential impacts of a security slack are dangerous. The threat landscape continues to evolve necessitating advanced end-to-end security measures, new authentication methods and monitoring services across multiple environments. It's time enterprises focused on the entire threat lifecycle for better planning, remediation and recovery.

As per an advisory from the U.S. Department of Homeland Security Cybersecurity and Infrastructure Agency (CISA) and the U.K.’s National Cyber Security Centre (NCSC), ‘cybercriminals are targeting individuals, businesses and organizations of all sizes with these attacks, including phishing attempts, and trying to exploit security lapses in remote meetings.’

Adjusting the focus

Cybersecurity requires awareness as well as action. It's not the sole responsibility of enterprises. Employees need to do their bit too. A lot of times, employees have a high sense of responsibility but their inability to detect threats and avoid situations provide cyberattackers the loopholes they are looking for.

Some of the immediate concerns that can lead to cybersecurity breach include:

Visual hacking – A concern as well as a nuisance, this can be avoided by being more aware of who you surround yourself with, and not taking screenshots of sensitive information or storing work-related content on unsecured devices. Especially where personal devices can be easily accessible to friends or other members in the family, it becomes important to remain vigilant at all times.

Email access through mobiles or personal devices - A lot of times, employees assume that a mail that's not marked as 'sensitive' is okay to access from their phones. Unfortunately, majority of data breach cases happen through such seemingly 'ordinary' mails.

Copying content through corporate VPN – This requires extreme caution too. Employers may do their bit by providing employees a highly secured corporate VPN. But the onus is on employees to ensure that downloads and uploads happen via the same network without resorting to unsafe public network connections.

Social engineering attacks - Very common but extremely damaging, these attacks may just be the kind of stuff enterprises need to protect themselves from. Often the weakest in the link are people, who can be manipulated and deceived. Often, social engineers impersonate to fool employees into allowing access to information. They may contact the employee as a fellow employee, IT support, manager or vendor. With prior preparation, they may forge a business card, or an ID badge or any other proof that confirms their identity. While the innocent employee may believe they have all the necessary security checks in place, these tactics can lead to major data leaks and very damaging consequences.

For effective cybersecurity, it is crucial to identify the vulnerabilities and address the challenges head on. It is important to have conversations revolving around People, Technology and Processes. Let's delve deeper into security issues at each of these levels to see how we can overcome the security hurdles.

The WFH employee

Technology workers across the country are being forced to work from home, a trend that will continue well beyond the pandemic. As WFH becomes the norm, it has started exposing gaps in cybersecurity and magnifying vulnerabilities. BYOD is further aggravating the cybersecurity challenge as employees continue to plug their unsecured devices into corporate network via a VPN, further increasing the risks.

Organizations need to monitor devices, active and inactive, to apply technical controls and prevent unauthorised access to sensitive information. It is important that employees are communicated well about the perils of entertaining wrong emails and websites, and the role they play in keeping the enterprise secure. Cybersecurity awareness and understanding the basic do's and don'ts is the key here. What cybersecurity leaders actually need is a 'human firewall'.

Remote working can bring about countless challenges when employees are sent beyond their usual perimeters. In such a chaotic scenario, the network perimeter now includes but is not limited to employees' homes. Managing device sprawl and patching in a multitude of endpoints then become a herculean task for cybersecurity teams.

> “
>
> **Government, legal, insurance, banking and healthcare are all great examples of industries that are not prepared for this massive influx of remote workers,**
>
> **Sumir Karayi,**
> CEO and founder of 1E tells Threatpost
>
> ”

The Technological Barriers

It's not easy to draw parallels between home networks and enterprise networks. Despite the vulnerabilities, thousands of employees access critical data over unsecure home networks leaving backdoors open for cyberattacks. Company resources accessed via VPNs and other methods need to be monitored diligently. Often, enterprises are more prepared to respond to on-premise threats. But what about unintentional threats and those that occur at remote WFH locations especially when IT teams themselves are operating from remote locations?

Another factor that needs to be considered here is the haphazard manner in which organizations are implementing apps to ensure business continuity. Classic case in point? SaaS applications that ensure better collaboration and productivity. While using these apps, they tend to overlook major security considerations such as 2FA that come along with them.

Zoom app, for instance, garnered unprecedented popularity among users. The Computer Emergency Response Team of India (CERT-In), the national cybersecurity agency however issued an advisory stating safety measures for those using the video conferencing app. "Insecure usage of the platform (Zoom) may allow cyber criminals to access sensitive information such as meeting details and conversations," it said. Some of the safety measures suggested in the advisory for added security included keeping the Zoom software patched and up-to-date and having difficult-to-crack, unique passwords for webinars and meetings especially where sensitive information is likely to be discussed.

Trusting the Process

Covid-19 pushed virtually everyone into overdrive and even the organizations that had never considered WFH were now encouraging their employees to manage work remotely. Since this happened so suddenly, their systems lacked the necessary embedded controls. So an employee that has never managed high-risk business processes was now doing so without a VPN due to their inability to fulfil the in-person VPN-initiation requirements.

Risk mitigation in such cases requires secure remote-working tools that complement incident-response, business-continuity and disaster recovery plans. Those off the company network or VPN remain largely unprotected though a lot depends on the security stack. Proxies, web getaways, network intrusion-detection systems (IDS) or network intrusion-prevention systems (IPS) won't really give the much-needed protection in this hour of need. The absence of end-point protections of noncompany assets also necessitate added vigilance.

Another aspect that's often overlooked is security of third parties. Enterprises may get so busy securing new work-from-home protocols, that they may completely miss out on doing the same for third-party users. Care should be taken to ensure that access is limited or denied if third-party vendors or users fail to demonstrate adequate security controls.

Additionally, web-facing enterprises need to look into the effect the fast increasing consumer traffic is having on the threat environment. Cybersecurity teams need to keep their eyes open for suspected malware particularly in case of overextended web-facing technologies.

This is particularly important where online activity is very high. Securing confidentiality, integrity and availability (CIA) of network activity is of paramount importance in safeguarding consumer interests. Also, organizations that are closely associated with financial transactions should consider integrating fraud-prevention capabilities with the SOC to avoid MITM attacks and others that are equally detrimental.

Raising awareness among remote workers

Cybercriminals are reinventing ways to exploit cybersecurity vulnerabilities of enterprises. Training the employees to embrace cybersecurity and adopting a mindset of responsible working can significantly help enterprises in fortifying their efforts to combat cyberattacks. Employees should prohibit friends and families from accessing work devices and avoid using personal email for work. While it is the responsibility of enterprises to up their security measures, it is individual responsibility that can eventually help them win the war against cybercrime.

The game changers

With borderless teams transcending cities, countries and continents, it becomes imperative to protect data that travels along with them. Thankfully, there are a bunch of solutions enterprises may want to consider to address the many challenges pertaining to remote working.

We've handpicked a few.

Desktop-as-a-Service

A bird's eye view is just what is needed to monitor the corporate and critical systems employees access from home. This unique solution employs hi-tech dashboards that offer invaluable insights pertaining to:

- ↗ Users' SSL VPN Logins , both successful and failed anomalies
- ↗ Reputation score of the user home network by checking IP Reputation with Threatintel feeds
- ↗ Logins from non-business locations
- ↗ Logins at abnormal times and days
- ↗ Logins from blacklisted countries
- ↗ Same user logging in from different locations
- ↗ Users who are facing connectivity issues
- ↗ Data residing at a centrally controlled location instead of an uncontrolled user location

Endpoint Detection and Response or EDR-as-a-Service

The evolution of malware has always been a cause of concern for cybersecurity leaders. Ransomware attacks too are becoming highly sophisticated. All in all, there are several vulnerabilities that need to be taken care of.

EDR-as-a-Service helps:

- ↗ Spot attacks and zero-day exploits
- ↗ Investigate forensic evidence to uncover scope of breach
- ↗ Search and explore endpoints via rapid access to 6 months of historical data
- ↗ Assess the impact of threats on environment interactive reports
- ↗ Detailed inspection of suspicious files
- ↗ Auto response to mitigate issue without or less human intervention

Privileged Access Management or PAM-as-a-Service

The most overwhelming aspect of security threats is that they come from insiders. Insiders that are malicious or negligent or disgruntled. Often, they take advantage of the access they have to unsecured privileged accounts. The fact that insiders are expected to do routine work makes it very difficult for cybersecurity teams to track their daily activity.

The access to privileged accounts may give them the power to read, modify or delete sensitive data, use passwords and grant access to other unauthorized users. Whether intentional or unintentional, insider threats can disrupt the wellbeing of the whole enterprise.

PAM-as-a-Service helps:

- Control and monitor privileged user access
- Protect passwords of assets using password vaulting that prevents credential leak
- Implement host level restriction to monitor and prevent abusive insider threats
- Manage credentials used by applications, container platforms, automation tools and other non-human identities
- Tackle human and non-human access to CI/CD consoles
- Leverage native application attributes and role-based access controls to authenticate applications and containers.
- Accelerate PAM implementation/deployment through containerization

The Zero Trust model is all set to become mainstream

The recent pandemic has urged cybersecurity leaders to revisit old approaches to enterprise security. The stakes are higher now that employees are working remotely. The 'here to stay' WFH culture has now necessitated a zero trust approach that puts users at the center of an enterprise's security efforts.

So rather than trusting anything inside or outside of an enterprise's perimeters, anything and everything trying to access its systems should be questioned, checked and duly verified. It boils down to a simple philosophy - trust no one. An extremely aggressive method, zero trust seems to be the perfect solution in a highly integrated world.

Conclusion

Times are changing. The need for robust cybersecurity is felt more than ever before. While employees continue to play an active part in fortifying enterprise security, Cloud4C presents solutions that are time-tested and backed by sound research.

Allow us to assess your security architecture. We'd be happy to help you with solutions that will ensure total security and complete peace of mind.