COVID-19
THE CYBERSECURITY IMPACT

CHARLIE WINCKLESS – Cybersecurity Solutions Director
COVID-19
THE CYBERSECURITY IMPACT

Identifying and addressing the cybersecurity risks occurring on the heels of COVID-19

Introduction ........................................................................1
Background .........................................................................2
The Eroding Perimeter .......................................................2
Malware .............................................................................3
Endpoints ............................................................................4
Solutions ............................................................................5
User Awareness Training ....................................................5
Network Controls .............................................................5
Remote Access ....................................................................6
Endpoint Security ............................................................6
Conclusion ..........................................................................6
References ..........................................................................7
INTRODUCTION

The pandemic has forced significant changes and reprioritization on organizations worldwide. It has expanded both the scope and urgency of existing threats and business challenges that organizations were already wrestling with, and the landscape is continuing to change rapidly. We are not seeing an introduction of any new cyber security threats – though existing ones have evolved and mutated. Rather, the crisis is forcing companies to ask both short- and long-term questions about their business continuity plans and emergency security readiness.

We are facing a first for many organizations: a situation where working remotely is not a valued perk, but a business and legal requirement. Many business functions have always been performed inside the corporate perimeter, now they are being forced to be performed outside of it. Moving these functions is likely a strain on all aspects of many organization’s cyber security.

From a technical perspective, users will require authentication, appropriately provisioned access rights, and data protection over the untrusted networks between the user and the application. The need for strong authentication techniques (including multi-factor authentication) is magnified as users access resources from non-traditional locations. Unless everyone has a laptop already, access may be from devices that have never left the facility before (and must still be maintained) or from personal systems that could lack many security controls and may well not be maintained to the basic standards of cyber hygiene. All of these devices will be in users’ homes, and these are likely less secure than the corporate office; physical access and privacy cannot be assumed, and the plethora of IoT devices in most homes could expose another threat vector.

Continuing to deliver on appropriate processes may also be challenging. Systems must be maintained regardless of location. This includes patching the operating systems and applications, as well as maintaining encryption systems and authentication functions such as certificates. Security monitoring and the associated responses will become even more critical in the new fluid environment populated by a mix of endpoints.

People will also be targets. Phishing, drive-by malware downloads from websites, and Business Email Compromise are endemic issues and constant security challenges. The remote and more isolated workforce may make the challenge worse – you can no longer easily ask your co-worker quickly what they think, or just ask about the financial transfer request that was emailed to you. Also adding to the problem is that organizations are being predictable; sending ‘What are we doing about COVID-19’ messages to their employees, customers, and business partners that attackers know about and can exploit as methods to engender trust. Remote users without co-workers and managers observing them may access personal email accounts and bypass corporate controls, opening another possible entry vector for malware. Last (and far from least) it is also possible that critical staff (every role is a security role) may fall ill and be unable to perform their jobs – a challenge if that individual is a single point of failure.

As above: this is all happening in an incredibly compressed timeframe. Organizations are being forced to act possibly before taking the time to think. Staff are being asked to do more, with less, and while under significant external strain and worry. The combination means that mistakes are easy to make, and these mistakes may have severe consequences – everyone has been forced to shed their traditional defenses at once, and the predators are well aware of this fact.

Finally, this is by no means an exhaustive list of the issues and problems: this white paper attempts to focus on some of the largest risks and the ones that have been materially changed by the situations created by the pandemic.
BACKGROUND

The Eroding Perimeter

The traditional corporate cybersecurity perimeter is being steadily eroded. Most organizations have some remote workers, and digital transformation and cloud adoption are driving data ‘outside the walls’. Business partners and customers all want to interact electronically and need some access to corporate assets to do so. This is not new — as far back as 2004 the Jericho Forum was formed to specifically work on defining and promoting ‘de-perimeterisation’, as they then coined it.

The perimeter (or perimeters – with organizations adopting data center and other internal perimeters) has remained a key element of most organizations’ cyber defense strategy. The firewalls and associated security controls that form this data perimeter usually maps closely to the corporate perimeter created by physical offices. It provides ‘table stake’ controls - application visibility, advanced telemetry, and the ability to stop some attacks before they reach an endpoint. More and more attacks on systems enclosed by the perimeter, however, are not stopped and must be blocked or detected by other controls.

Digital Transformation and the associated cloud journey have forced more cracks into many organization’s electronic walls. IaaS, PaaS, and SaaS have generated huge revenues (Gartner had estimated a total of about $280B in worldwide revenue prior to any impacts of the pandemic) and that revenue is a proxy for the volume of data and applications organizations are moving to cloud locations; locations that are inherently beyond the corporate perimeter. These applications can be accessed from anywhere, anytime, and in many cases on any device – things that traditional perimeters often try to control or even block. Each application and environment will have their own security controls – there is no limited set of chokepoints that can manage access.

The location of the data is one side of the access equation; the other is the location of the user. Teleworking places the user end of the equation beyond the perimeter, and the practice of remote working has been steadily growing. US Bureau of Labor Statistics report that it grew 115% between 2005 and 2015, that by 2019 25% of the total workforce are remote at least part of the time, and over 29% ‘had flexible schedules and the ability to work from home’.

The option to work remotely is a valuable perk to many employees - millennials, in particular, appreciate work schedule flexibility. According to a 2017 survey performed by Qualtrics and Accel Partners, over 75% of millennials would take a 3% salary cut in exchange for flexible work location and hours. Remote work adoption has not been universal – among others, Yahoo’s Marissa Mayer, famously drove employees back into the office in 2013 and IBM removed remote work as an option in 2017. Yahoo stated it was ‘to increase collaboration’, and large companies have struggled to innovate as fast as smaller-stage organizations (ironically, most of these smaller-stage organizations have telework as a given and don’t even have a policy around it). Other companies of all sizes have revoked telecommuting perks due to abuse, or due to poorly rolled out policies, but the American Psychological Association stated in October 2019 that ‘When it’s done right, telework can improve employee productivity, creativity and morale’.

Despite the potential benefits, organizations have not found ways for the remaining 70% of their employees to work remotely – until forced into it.
Malware

According to the Verizon Data Breach Investigations Report (DBIR), over 90% of the average company’s detected malware is delivered by email. It is no surprise that attackers are rapidly shifting to using COVID-19 related material as the bait to trick users into interacting with malicious content. The scale of impersonation attacks has led several to post warnings around cybersecurity threats, including the World Health Organization (and the WHO has posted guidance on this specifically) while the US Federal Cybersecurity and Infrastructure Security Agency (CISA) has posted guidance for avoiding COVID-19 cyber scams.

There are many examples of attack techniques in use in the wild. Researchers have seen active, targeted campaigns regarding the coronavirus since reporting of its spread began in earnest. By early February, IBM’s X-Force had identified a campaign using coronavirus subject matter to distribute Emotet malware in Japan. Kaspersky also reported early evidence in February of malware disguised as pdf, mp4, and docx files with claims of solutions that protect against coronavirus. By early March, Sophos reported that operators of a Trickbot spam campaign had adapted payloads in Italy to focus specifically on the outbreak.

In addition to malware over email, web-borne attacks are also appearing. Malwarebytes detected trojans being distributed from a fake site using what appeared to be the legitimate ‘outbreak map’ from the Johns Hopkins website. We are even seeing ransomware on phones. DomainTools researchers have identified a malicious Android application that purports to track COVID-19 cases but instead encrypts the phone, asking for $100 to decrypt the device. (DomainTools has released the decryption key for anyone impacted by this. It is “4865083501”)

Endpoints

Endpoints (whether servers, mobile, or user) can be a point of entry for attacks and attackers. Servers and cloud infrastructure operations will not be significantly different for the pandemic; systems must be managed and supported remotely, but those practices are well established in many organizations. The patching, updates, and maintenance of servers will be the same, just performed by remote administrators. The same logic applies to laptop and traditional remote endpoints; the structure for managing them will not be changed by the situation around COVID-19. Organizations may be challenged, however, if they have dramatically scaled up the number of remote endpoints, or if they have not had an extensive remote workforce before.

Mobile endpoints and mobile access will also not be changed dramatically (except in volume) by the pandemic. Almost by definition these devices are used outside the perimeter, and the same controls and efforts can be used during the COVID-19 crisis as before.

Non-corporate endpoints present additional issues. Basic cyber hygiene (such as patching the operating system and applications, only running trusted applications, requiring strong authentication, and configuring the system to industry-accepted security standards) may not be followed. The system may have multiple users and these users may share a single account. Standard corporate security software is unlikely to be installed, and if there is security software at all it may be misconfigured, disabled, or otherwise rendered ineffective.

All of these issues vastly elevate the risks incurred when these endpoints connect to the corporate network. In usual times, most companies will heavily restrict or completely deny access to corporate resources from non-corporate endpoints. The mandate may be in policy, technically enforced, or both – and may have to be relaxed or totally dropped if there are not enough corporate endpoints to go around.
There will be no ‘one size fits all’ solution; the needs and risk tolerances of each business will shape what is most important to that business. Understanding the risks and evaluating them is the critical first step – this allows you to move from reacting blindly to a proactive and targeted approach.

Presidio has identified solutions that are widely applicable in this situation, though which ones are most relevant and in what order will vary widely between organizations and even departments. If these are not in place today, a phased approach, tied to business risks and needs will be necessary; it is simply impossible to implement everything at once.

**User Awareness Training**

A little education can go a very long way to helping users make smarter decisions. By focusing on cyber hygiene, the use of COVID-19 as bait in malware attacks, and by making employees feel as safe as possible, an organization can provide itself with a first line of cyber defense. Helping employees understand the ‘why’ of decisions that are made for security purposes can also encourage employees to see extra controls as reasonable.

**Network Controls**

Even while employees are working away from the office, network controls can be effective. Email security is largely independent of location, and an advanced email gateway can mitigate many threats. Fraud detection, advanced malware blocking, URL re-writing, and advanced spam filtering will bolster the effectiveness of your user awareness training.

Another network protocol that can be leveraged for security regardless of the user location is DNS. By embedding security functions into DNS responses, access to malicious sites can be dynamically blocked as they are identified, effectively allowing the rapid leverage of a provider’s threat intelligence. Further, attacks using Domain Generation Algorithms (DGA) may be detected and also possibly blocked.

Both of these first two options can be applied regardless of the ownership of the endpoint, though users may be unwilling or unable to easily switch their DNS settings on personal systems.

A more comprehensive option is to use a Secure Access Service Edge (SASE) solution, with traffic being tunneled to a cloud-hosted security gateway. This means that more controls can be enforced on the endpoint, even when it is not in a corporate location. Depending on the scope and scale, this can even include Firewall-as-a-Service, effectively creating a perimeter for the deperimeterized user.

**Remote Access**

SASE can also be an element of a remote access strategy, offloading multiple tunnels to a cloud location and having fewer tunnels back to corporate gateways. Moving the load of establishing and managing all the remote access gains efficiencies of scale.

Regardless of the method used to terminate traffic, there are both security and non-security constraints to remote access. There must be sufficient bandwidth available at the corporate...
end to service the aggregate traffic (and at the user's end of the link for their individual needs), and sufficient encryption capability to protect it. If remote access tunnels are terminated on existing on-premise platforms, licensing may be an issue. For untrusted endpoints, virtual desktops may be needed for critical applications or users – although these approaches can present both scaling and operational challenges if used en masse.

Organizations will have to develop their own unique strategy and deploy the right compensating controls where less-than-ideal security is a business requirement. Tools and processes like User and Endpoint Behavior Analytics (UEBA), careful filtering, and a fanatical adherence to least-privilege should be adopted as required.

**Endpoint Security**

Endpoint security is the first and last line of technical defense. It bolsters and supports all the other elements we have discussed; if malware gets past email or DNS filters, endpoint security provides another opportunity to catch it. If malware is delivered by another method (like a user accessing personal email on a corporate system), endpoint security provides a means to catch that too. It may also provide advanced telemetry on what is happening on the endpoint and assist in monitoring and in detecting attacks.

Ensuring that endpoint security is in place and effective dramatically increases the ability to securely operate outside the firewall.

**CONCLUSION**

The most important thing to do is to take care of our teams right now – and that means making sure we help keep them informed so they can make smart decisions. This extends to user training and general communications. Adding some technical controls to allow them to work effectively will let the business continue, albeit in modified form.

Finally – plan and be proactive. Don’t just react unless it’s absolutely required; we can all benefit from some basic analysis. Much is changing, so as you look at what you plan, it will be worth running these changes in a (virtual) tabletop setting to try and identify problems early – especially as functions move which have never been performed outside the corporate perimeter.

Done well, it is even likely that the steps taken to address this current crisis will enable better operations in the future and may be the gateway to a longer-term remote workforce, with all of the benefits that can bring.

References

5. The future of remote work https://www.apa.org/monitor/2019/10/cover-remote-work
6. Coronavirus “safety measures” email is a phishing scam https://nakedsecurity.sophos.com/2020/02/05/coronavirus-safety-measures-email-is-a-phishing-scam/
7. Beware of Criminals pretending to be WHO https://www.who.int/about/communications/cyber-security
10. Coronavirus used to spread malware online https://usa.kaspersky.com/blog/coronavirus-used-to-spread-malware-online/20213/