LORCA NEEDS ACCELERATOR: COVID-19'S IMPACT ON SECURITY PRIORITIES

LORCA

COVID-19 has affected all industries and exposed cybersecurity gaps that already existed, making them even more problematic.

Social distancing measures have meant that the majority of employees are working from home where possible. Some organisations have had to scale or adapt their services to changes in demand, while others have experienced major disruptions in their supply chains.

These shifts have highlighted the need for businesses to increase the adaptability and resilience of their current operating models.

And this is not likely to be a temporary blip.

In the post-pandemic landscape, more employees will routinely work from home, organisations will accelerate their plans to migrate to the cloud and businesses will try to make their supply chains more resilient.

So to understand the impact this will have on security professionals, LORCA convened a group of cyber industry leaders, policymakers and innovators.

HELD UNDER THE CHATHAM HOUSE RULE, OUR DISCUSSION UNVEILED A RANGE OF INSIGHTS, CHALLENGES AND OPPORTUNITIES...

1. Organisations need solutions that enable remote workers to securely access sensitive data from legacy desktop devices

2. The pandemic has exposed weaknesses in virtual private networks (VPNs)

3. There’s a need for innovative data masking and data obfuscation solutions

4. Reliance on the cloud has grown since COVID-19, but many existing security tools are inadequate and the shared responsibility model is flawed

5. There’s a need for more advanced data management solutions for multiple cloud environments

6. Where are all the cloud security experts?

7. Vendors are being onboarded quickly but security tools don’t enable continual and agile supply chain risk management

ORGANISATIONS NEED SOLUTIONS THAT ENABLE REMOTE WORKERS TO SECURELY ACCESS SENSITIVE DATA FROM LEGACY DESKTOP SERVICES

More employees are working from home and in many cases connecting to corporate systems through legacy devices. These devices can lack patching and security tools, so an enterprise may not be able to include them within its normal monitoring and security perimeters.

One attendee described a scenario where employees needed to use legacy desktop devices to access platforms containing sensitive data through the corporate network. Although this was allowed, they were concerned that these devices – and devices with different specifications – were either unsecure or incompatible with the organisation’s platforms and applications.

The rise of Desktop as a Service (DaaS) solutions addresses these issues. DaaS creates a virtual desktop environment using the cloud, where a third-party service provider manages the desktop infrastructure.

Organisations expect many employees to continue working from home after the pandemic and are looking for solutions that give remote workers secure access to corporate systems – regardless of the operating system or device they’re using at home.

THE PANDEMIC HAS EXPOSED WEAKNESSES IN VIRTUAL PRIVATE NETWORKS (VPNs) AND HEIGHTENED THE NEED FOR ZERO-TRUST ARCHITECTURE

COVID-19 has shown some security professionals that VPNs aren’t able to support a large number of remote workers using both in-house and third-party collaboration platforms.

Threat actors have also spotted this shortcoming and are targeting remote workers accessing VPNs.

In response, some organisations are adopting VPN split tunnelling, cloud-based virtual desktop infrastructures (VDIs) or software defined perimeters (SDPs).

Others have reservations about some of these solutions and are continuing to use a single VPN – despite being aware of the limitations.

Some security professionals believe split tunnelling obscures visibility while a single VPN is a single entry point into the corporate network, for example.

As for cloud-based VDIs and DaaS, both have experienced considerable growth during the pandemic and have quickly become the most popular alternative to corporately issued devices with VPNs. Benefits include not having to issue users with physical devices, the cloud offers massively scalable infrastructure on demand and corporate information stays within the cloud environment.

However, attendees admitted that VDI and DaaS also have their limitations. Compromised personal devices could still offer attackers a route into the VDI/DaaS environment through captured credentials. This means that additional steps such as multi-factor authentication should still be used to provide robust protection.

> **the pandemic has highlighted a need for us to move to a zero-trust architecture more quickly...any innovations in that space would be welcome**

Attendees acknowledged that software defined perimeters are a more secure alternative to VPNs. But they were conflicted about adoption of these technologies. On one hand, they noted that “the pandemic has highlighted a need for us to move to a zero-trust architecture more quickly...any innovations in that space would be welcome”.

Other attendees noted that adopting zero-trust architecture could be perceived as “jumping over hurdles...[which] will lead to people feeling like they will have to backdate decisions”.

There’s a clear need for zero-trust alternatives to traditional communications encryption. A small number of solutions are already on the market but innovators must consider that many organisations would be reluctant to overhaul their existing infrastructure.

THERE'S A NEED FOR INNOVATIVE DATA MASKING AND DATA OBFUSCATION SOLUTIONS

In a zero-trust environment, organisations need to enable secure collaboration and sharing with employees and vendors – even when they're working overseas.

An attendee described a situation where their organisation didn't allow vendors to access a core financial system from offshore, despite the vendor needing access to this system to perform their role.

The organisation was concerned that their most sensitive data wouldn't be secure because they didn't trust the vendors' personal devices and they didn't think that their current encryption methods and processes would provide enough assurance.

The organisation was using VPNs to encrypt data-in-transit. But VPNs have limitations. For instance, if a VPN is compromised hackers could gain access to the entire corporate network.

Other forms of encryption and data masking or data obfuscation techniques already exist on the market like character scrambling or nulling and deletion.

But existing solutions don’t provide enough assurance for offshore remote access through unknown personal devices.

> “existing solutions don’t provide enough assurance for offshore remote access through unknown personal devices”

These issues could be addressed through innovative endpoint management tools and zero-trust encryption. Innovations in other forms of data masking and data obfuscation would also be welcome.

RELIANCE ON THE CLOUD HAS GROWN SINCE COVID-19 BUT MANY EXISTING TOOLS ARE INADEQUATE

The pandemic has accelerated the move to the cloud for many organisations, but this has highlighted problems with the shared responsibility model.

This model states that cloud service providers (CSPs) are responsible for the maintenance and security of infrastructure and hardware while the customer is responsible for the security of everything that's in the cloud.

This includes encrypting data, managing the movement of data, identity access management and patching vulnerabilities. CSPs have developed a range of tools to help customers navigate their responsibilities in the cloud, such as Bring Your Own Key (BYOK) policies for encryption and out-of-band logging for incident response.

However, attendees think that many of these tools are inadequate. For example, organisations struggle to conduct forensic investigations within platform-as-a-service (PaaS) environments because existing incident response CSP tools don't allow for event capture in PaaS.

Meanwhile, some BYOK policies ensure that customers have ownership over master encryption keys but not lower-level keys. This means that if the CSP is compromised, the organisation's sensitive data can still be decrypted.

Attendees welcomed any solutions that would help them navigate the restraints of existing CSP tools.

THERE'S A NEED FOR MORE ADVANCED DATA MANAGEMENT SOLUTIONS FOR MULTIPLE CLOUD ENVIRONMENTS

Some attendees said their organisation intends to move to a multi-cloud computing environment after the pandemic.

Meanwhile, COVID-19 has resulted in a notable increase in the use of endpoints thanks in part to employees using personal devices to work from home.

Attendees believe that these factors will make tracking the movement of data in the cloud harder because data will be spread out across a wider array of services. This make it more challenging to maintain visibility and control over data – including sensitive data.

Data encryption is also a problem in multi-cloud environments. Security teams find that having to use multiple native cloud encryption tools can make configuration errors more likely while making it harder to consistently enforce encryption and key management policies.

To simplify data encryption in the cloud, enterprises are beginning to take a variable or scaled approach to encryption.

Data is categorised according to its sensitivity and an appropriate level of encryption is applied rather than encrypting all data in the same way. This reduces the likelihood of encryption errors and simplifies the enforcement of policies because there's less encrypted data.

Attendees commented that existing technologies and solutions like software-defined networking in a wide area network (SD-WAN) would provide them with greater visibility over how data is moving within the cloud environment.

But a core feature of SD-WAN is that it sets up a one-to-one encrypted channel between the user and the network. This encryption capability is agnostic about the type of data being encrypted and the zero-trust model isn't able to deal with a variable approach to encryption in the cloud in a nuanced way.

> "the zero-trust model isn't able to deal with a variable approach to encryption in the cloud in a nuanced way"

Many attendees see a need for data management innovations within the cloud. These solutions should allow organisations to track the movement of data across multiple cloud environments and networks (such as 5G, for example) while accounting for variable encryption.

They also think there's a gap in the market for technology that acts as a single reporting system for all their cloud environments.

WHERE ARE ALL THE CYBERSECURITY EXPERTS?

Some enterprises are currently managing over 10 different cloud environments. But securely migrating to a multi-cloud model and establishing a centralised cloud policy can be very difficult across such a complex architecture because each cloud provider operates differently. Each CSP has their own cloud tools, and some CSPs have more than one tool for the same task.

Attendees thought that a lack of knowledge was the greatest barrier to successfully managing the complexity of these environments. Not all security teams have an in-depth knowledge of how each provider works and they're not always able to integrate their knowledge into a unified view that provides actionable insights.

With more organisations migrating to a multi-cloud model because of the pandemic, there's more demand for cybersecurity professionals with in-depth knowledge of how to migrate to – and navigate – multi-cloud environments.

VENDORS ARE BEING ONBOARDED QUICKLY BUT SECURITY TOOLS DON'T ENABLE CONTINUAL AND AGILE SUPPLY CHAIN MANAGEMENT

There's been a surge in pandemic-related cyber attacks since the lockdown began and successful ransomware attacks on supply chains have sometimes been the result of vendors having poor basic cyber hygiene.

At the same time, other organisations have managed disruptions in their supply chain by sourcing and onboarding new suppliers – sometimes overnight – without completing cyber risk assurance assessments.

Attendees mentioned that these situations highlighted the importance of being able to assess a vendor's cyber health continually and not just when they're onboarded.

They also noted that initial risk assessments are often based on a vendor's own self-report, which could be biased and unreliable.

Some organisations with a more mature approach to supply chain risk assessment use external services that provide unbiased, daily updates of a vendor's cyber health.

But attendees argued that these solutions weren’t suited to agile supply chain management because they lack features that support quick decision-making when onboarding a new supplier. For instance, an unbiased, up-to-date risk assessment doesn’t tell the organisation whether that supplier’s cybersecurity posture fits with their current risk appetite.

This means organisations have to spend time on and assign resources to interpreting assessments and manually comparing scores across potential suppliers.

> “there’s a clear need for data-driven, unbiased risk assessment platforms”

There’s a clear need for data-driven, unbiased risk assessment platforms. Innovators in this space should be ensuring that solutions allow organisations to quickly assess, onboard and monitor new suppliers while providing actionable, real-time insights that support agile supply chain management.

CONCLUSION: ENABLING AGILITY

The pandemic has highlighted the importance of operational resiliency, scalability and adaptability.

For instance, BYOD policies allow staff to work from anywhere while cloud computing enables businesses to scale workloads according to demand and risk management solutions are facilitating the secure onboarding of suppliers.

But organisations that didn’t already have technology-enabled operating models or security practices in place that would allow for this agility have ended up taking risks they wouldn’t normally have the stomach for.

So if agility is the new normal, security by design and default must be as well.

The pandemic has also placed a spotlight on the need for zero-trust technologies and solutions, while businesses that are migrating to a multi-cloud infrastructure require more cloud experts as well as solutions that support a shared responsibility model.

There’s an opportunity for cyber startups to act as enabler for businesses to thrive in a post-pandemic world that rewards the agile and the brave.

CONNECT WITH US

lorca.co.uk
info@lorca.co.uk

Twitter: @LORCACyber
LinkedIn: LORCA Cyber

FIND US

Plexal, The Press Centre Here
East, 14 East Bay Lane
Queen Elizabeth Olympic Park
London, E20 3BS