mnemonic

WHITEPAPER

IT OUTSOURCING CONCERNS AND MITIGATIONS

How the COVID-19 outbreak may impact your overall security posture and eight steps to reduce the risk

Introduction

Outsourcing of IT operations and development has been a hot topic for years. Outsourcing critical operations adds certain risks, but with it also comes benefits.

Common advantages include scalability, more robust disaster recovery, easier access to subject matter experts, lower costs and being able to focus resources on core business development.

However, outsourcing also introduces a more complex delivery model, security and privacy concerns, less visibility, reduced control of the overall IT infrastructure, and makes it more difficult to map IT deliverables to a company's business needs.

The pros and cons of outsourcing IT operations and development have been an ongoing discussion across most industries and organisations. The global outbreak of COVID-19 at the beginning of 2020 triggered a paradigm shift where organisations are now discovering additional risks associated with IT outsourcing.

To limit exposure and contain the spread of the virus, organisations all over the world saw their IT outsourcing partners being ordered by their governments to shut down offices, and reduce the percentage of employees permitted to work from their datacentres. For many IT outsourcing providers, their service delivery model is simply not equipped to be delivered from employees working at a home office.

As organisations scramble to determine if their well-documented SLAs are still valid, a more significant risk is if the confidentiality, integrity and availability of their data and services are being maintained and handled appropriately from their IT outsourcing partners' homebound workforce.

While this risk is not necessarily new, its impact has grown exponentially and unpredictably in March 2020. The goal of this introductory whitepaper is to highlight eight specific technologies CISOs, security teams and IT managers should consider to reduce these risks.

The list of risk mitigating recommendations below is not complete. Other technologies and approaches may make just as much sense based on what needs to be protected. However, we have selected these eight specific topics based on our vast experience assisting customers in reducing their risk exposure under similar circumstances.

Content

1 Consolidate all critical log sources into a SIEM

The ability to monitor and correlate log information from all relevant sources is key to understanding what is happening within your infrastructure, and retrospectively, what has happened. It is also essential for gaining visibility to semi-external systems that interconnect with your infrastructure, such as those an IT outsourcing partner may be using.

Organisations should review their current SIEM (Security Information and Event Management) design. As a minimum, the following should be looked into:

- If authentication logs at external entry points, such as VPNs or other interfaces with IT outsourcing partners are being collected
- If Administrator activity, including the creation of new accounts, changes to account permissions or unauthorised use of administrator and service accounts is being collected
- If Access logs for business critical systems are being collected
- If the logging verbosity on existing data points is sufficient or should be increased
- Are there defined use cases for identifying suspicious activity from IT outsourcing partners in the SIEM, and are security personnel familiar with the use cases

Collecting log data from a potentially larger set of sources may come with a cost, but will also provide organisations with more visibility and a security dashboard to prioritise incidents based on current risk.

A core requirement for the current situation is to ensure endpoint activities are logged and pulled into the centralised SIEM solution. Visibility into what is happening on the endpoints makes it possible for your organisation to understand what normal behaviour looks like and in turn, detect and act on anomalies. Major disruptors in the way people work and access resources, like in the ongoing situation, may lead to an increase in unwanted activities that should be monitored and alerted upon.

2 Strict VPN design with posture checks

VPN technology is widely used to provide remote, secure access to company networks and resources on those networks. Securing remote access has probably never been more relevant than it is right now, and for many organisations, this starts with their VPN.

One common trend with VPN technology is to introduce more advanced posture checks to verify and validate the connecting endpoint in great depth before allowing authentication. This is not a new concept, but has become more robust, more detailed and more tied into providing conditional access based on a number of different parameters (such as if processes for security solutions are running on the endpoint, if anti-virus or other solutions are updated, if the operating system is adequately patched, if specific applications like browsers are updated, or scans for unwanted applications).

It is important to address this concern when your outsourcing partner has employees working from home while still requiring access to your infrastructure to perform their tasks. A strict posture check gives some confidence in the security status of the endpoint before it accesses your network.

Another emerging option is what is called zero trust network access. This approach provides specific access to a specific application or service at a specific time. Such technologies support secure access from both managed and unmanaged devices. The concept is becoming a tactical way to allow access from external consultants and contractors by providing them with just the minimum of access they need to perform their job. For instance, that could be access to SSH into a specific server to perform a task at a specific time. The access will at all times require a full posture check as well as an authorised authentication via a supported federation partner. Zero trust network access could ease the pain for allowing access from the IT outsourcing partner's employees working from home.

3 Optimise privileged access management

Providing privileged access is a constant concern for larger enterprises. While most organisations aim to comply to the principle of least privileged access, it is hard to maintain in practice. The concept of least privileged access means that only specific and minimum entitlements required to perform a task should be granted. Access should be based on a need to know basis. Excessive access causes high risk exposure and in an outsourcing setup, this becomes even more critical.

To address such concerns in a structured way, Privileged Access Management tools (PAM) has emerged as an almost mandatory platform for large organisations today. PAM is used by organisations to centrally manage and govern access to all critical resources within an organisation. The focus is not just on least privilege and minimum permissions, but PAM also limits the access to the specific time it takes to complete a task or a batch job.

When outsourcing IT services, the use of PAM tools improves security as it ensures that all accounts, be it personal, built-in, admin accounts, root, shared accounts and so on are only used for the intended purpose and when it is required. Privileged accounts are also a concern when it comes to software, but for this whitepaper we will focus on the human element.

With the events of March 2020, managing access has never been more important. The extended use of remote workers was likely never in scope for most signed outsourcing agreements and associated SLAs prior to this date. However, the new situation requires rethinking of how a PAM tool can be used to ensure even more controlled and secured access.

Another option worth mentioning is to record privileged remote sessions for environments that require the highest level of security. These can be made available in both text format and in video format. All keystrokes typed can also be recorded for audit purposes.

Privileged access management must be a continuous focus area to ensure inappropriate access is removed, ensure all shared accounts and service accounts are documented, and monitoring and reporting on who is actually using the access they have been provided.

A PAM tool also helps streamline the process of protecting secure workspace alternatives for remote users by ensuring that the right permissions are set for access via VDI solutions (Virtual Desktop Solutions) like those offered by Citrix, VMware and others, or straight RDP sessions (Remote Desktop Protocol). Ensuring the least privilege access is enforced on RDP sessions becomes more manageable when relying on a PAM tool.

Another related topic that is equally important is to protect and manage SSH keys to reduce the risk of unauthorised access to critical systems. Secure Shell, SSH, has been widely used for more than 20 years and due to the necessity of command line access to critical systems, strong security measures must be implemented to ensure the risk exposure is minimised accordingly.

In the current situation, implementing or improving an existing PAM program is essential to ensure contractors and outsourcing partners will be granted exactly the minimum permissions required to perform the specific tasks that are in scope.

Additionally, cloud transformation has required organisations to extend Privileged Access Management to cloud environments as well. This in itself is an extensive topic that will not be covered in more detail in this whitepaper. However, it is important to stress the need for implementing a PAM solution that covers all relevant access management aspects to ensure least privilege becomes the default operation model, regardless of what should be accessed and by who.

4 Endpoint Detection and Response

Security teams are increasingly aware of the risk posed by advanced threat actors bypassing existing security controls and threat prevention tools via phishing, social engineering and exploitation of unpatched vulnerabilities in servers, laptops and desktops.

For many organisations, the global outbreak of COVID-19 has resulted in a significant increase in employees working remotely. While some workers are familiar and adjusted to working from home, for many it is a new experience. IT teams globally had to quickly scale up and roll out remote solutions, and may have bypassed their established procurement and implementation processes, such as risk assessments, security reviews, and planning to integrate the service into existing security architecture.

While this is challenging at best to facilitate for your own employees, it becomes even more demanding when your IT outsourcing partners are in the same situation. What kind of controls and security measures are they putting in place to ensure that all access to their customers' environment are handled in a secure way? This raises a red flag for many organisations. One way to push for more visibility, alerting and enforcement capabilities is to introduce, or extend the use of, a specific technology called Endpoint Detection and Response (EDR).

When outsourcing partners have people working remotely while still accessing your infrastructure, EDR provides the best tool to understand exactly what is happening on each endpoint, as well as making it possible for organisations to perform threat hunting by rapidly polling statuses from tens or hundreds of thousands endpoints. This is regardless of where they are located. As long as they are connected to the Internet and have the EDR agent installed, threats can be prevented, detected, and contained immediately.

Threat hunting, investigations, and content development should be performed by specialised security personnel. These actions can be initiated by for instance externally alerted incidents (e.g. from authorities) or ad-hoc requests. Indicator sweeping can be performed based on indicators collected and received from partners and collaborating organisations.

Here are some examples of common use cases for EDR, which will be highly relevant to organisations outsourcing their services:

- Monitor processes, registry changes, file activity and network activity
- Detect unwanted software that is being installed
- Hunt for indicators of compromise (IOC) like file hashes, processes and registry settings
- Isolate endpoints from the network in severe situations
- Kill applications or processes that represent security risks

5 Cloud security posture management

As many organisations embark on cloud journeys it is vital to ensure that all cloud-based solutions meet the same security, change management and reporting requirements as if they stayed on-premise.

If not managed the right way, cloud environments can cause challenges. Potentially critical risks can for instance be introduced if something becomes misconfigured. There are far too many public examples detailing how a simple misconfiguration resulted in enormous amounts of confidential data being exposed publicly on the Internet.

Cloud security posture management is a technology that helps customers visualise, monitor, alert and report on configuration status and configuration changes in cloud environments like AWS, Google Cloud and Azure. The ability to detect misconfigurations and enforce security best practices in these environments is extremely important.

It has also become more common to use such technologies to perform compliance assessments and report on status versus a wide range of global standards and frameworks. The ability to visualise a test score for a given assessment is a very powerful way to optimise the configuration. It is also important to take into account that the same tool will be used in multi-cloud environments where all or a combination of AWS, Google Cloud and Azure are in use.

An IT outsourcing relationship where users potentially perform configuration changes in your IaaS environments from home might add even more risk. Cloud security posture management will alert on misconfigurations or unexpected changes introduced by outsourcing partners, so you can quickly remediate, either automatically or manually, to remove the risk introduced.

6 Cloud Access Security Broker

Cloud Access Security Broker (CASB) is emerging as a key technology to provide visibility into core SaaS applications like Office365, Salesforce, ServiceNow, Docusign, Slack and similar. CASB enables organisations to get full visibility into what is happening within their core SaaS business applications and alert on any risks that are discovered.

There are different ways to implement a CASB service, but for the purpose of this whitepaper, the important aspect is how to integrate the services transparently in a well-documented way using APIs. The purpose of APIs is to present a set of protocols and routines to facilitate integration with other systems. All mature SaaS applications have support for APIs to let anyone integrate and communicate with the service.

As integrations with SaaS applications happen on the backend via API integrations, no traffic redirect is required. Still, all important actions happening within the SaaS application itself can be monitored and alerted upon. One example is the ability to monitor file uploads, downloads and sharing within Office 365. Actions like file copy, file deletion, and new admins added are examples of other activities that should be monitored.

In an outsourcing agreement, it is even more important to monitor such activities to ensure your organisation has full visibility into what your outsourcing partner's employees are doing when working remotely. All the monitored activities can be pulled into a centralised SIEM solution to ensure that these data points become an integral part of the overall picture. Mature CASB solutions provide built-in detection mechanisms to alert on threshold-based metrics like how many external recipients someone can share data with from Office 365. Detecting uncommon behaviour like bulk deletion, bulk copy, move or rename operations is also of great interest and should be alerted upon. Repetitious downloads, uploads as well as uncommon activity time and login activity times are other examples of the insight that can be provided by implementing a CASB solution.

The leading CASB solutions can also run discover tasks to reveal if your SaaS applications, like Office 365, contain any sensitive data as classified by Azure IP, Titus, Boldon James or by metadata produced and added to files by core business applications. From a compliance perspective, it can be very helpful to be able to present reports stating that no sensitive files reside in the SaaS.

When focusing on the API integrations, CASB solutions are easy to implement and they can provide significant value straight from the initial activation phase as these services come with pre-built dashboards and policies that can be used to enable monitoring and alerting based on the examples listed above.

7 Insider threat technology to detect misuse

Your IT outsourcing partner's activities while working remotely could potentially cause issues if sensitive data is handled incorrectly, or if unwanted activities take place on the endpoints. A way to monitor this is by introducing an endpoint technology on critical endpoint machines that monitors, alerts and potentially blocks authorised access misuse.

This kind of technology has proven very capable in establishing a security baseline on endpoints, as it uncovers risky user activities based on knowledge about past activities. The technology identifies anomalous behaviour on endpoints and triggers required actions based on that.

After identifying unwanted behaviour, it can record what is happening on specific endpoints and alerts a centralised management solution. The recording will reveal all the activities the user was performing before, during and after an incident was registered. It can potentially even allow a SIEM solution to consume the findings and orchestrate what should happen next, like potentially isolating the machine, stop services and processes, disable unwanted software, take the machine offline, and so on.

Introducing this kind of technology can be of great help to make sure there will be produced evidence when unwanted activities are detected. Some examples of relevant use cases:

- Monitor and alert on unwanted removable media activities
- Monitor and alert on local print spooler jobs containing sensitive data or specific file types
- Monitor copy/paste activities between applications
- Monitor on what applications are being installed
- Monitor and alert on privilege escalation attempts
- Monitor and alert on what certificates have been added
- Monitor and block exfiltration attempts related to cloud service uploads
- Monitor unusual command line behaviour

8 Data loss prevention on endpoints

Last but not least, information security. By deploying a data loss prevention (DLP) agent on endpoints used by your outsourcing partner's employees working remotely, you will add new and necessary capabilities.

Data loss prevention has become something close to a de-facto standard for the global Fortune 1000 organisations. It ensures that you can monitor how sensitive data is being used on endpoints, if any sensitive data is stored locally, or if sensitive data is moved to cloud services, removable media, local printers, or home storage systems.

Monitoring what is commonly called "data-in-use" adds full visibility into all activities happening on the endpoints and triggers responses based on any defined information security policies.

Below are three real-world examples of endpoint data loss prevention in action:

Example 1: a user downloads a Word document that contains data defined as sensitive in its metadata. If the file is stored locally and later on uploaded to the user's private OneDrive account, this can be blocked in real-time to prevent the data breach.

Example 2: a contractor has a number of files stored locally that should not under any circumstances be stored on remote computers. It can be specific file types like CAD/CAM or files that are classified using metadata, watermarks, etc. The data loss prevention system can detect that the files are stored locally during a scheduled data discover task. Sets of external machines are scanned to look for locally stored files that violate given information security policies. If any files are detected, these can automatically be pulled into a safe central quarantine location to remove the risk from the endpoint.

Example 3: a contractor working for one of your outsourcing partners inserts a USB key to copy files onto an unknown device. The USB key will not be accepted as it is not listed as an approved device based on serial number, vendor ID, product ID or other attributes.

About mnemonic

mnemonic helps businesses manage their security risks, protect their data and defend against cyber threats. Our expert team of security consultants, product specialists, threat researchers, incident responders and ethical hackers, combined with our Argus security platform ensures we stay ahead of advanced cyberattacks and protect our customers from evolving threats.

Acknowledged by Gartner as a notable vendor in delivering Managed Detection and Response (MDR) services, threat intelligence and advanced targeted attack detection, we are among the largest IT security service providers in Europe, the preferred security partner of the region's top companies and a trusted source of threat intelligence to Europol and other law enforcement agencies globally.

With intelligence-driven managed security services, 200+ security experts and partnerships with leading security vendors, mnemonic enables businesses to stay secure and compliant while reducing costs.

Contact us

mnemonic
Henrik Ibsens gate 100
0255 Oslo
Norway

contact@mnemonic.no

Oslo | Stavanger | Stockholm | London | Palo Alto