Top Tips for Using Cloud Services Securely in the COVID-19 Era

Reliance on cloud services has become a critical lifeline for organisations. Many are increasing their cloud workloads, while others are fast-forwarding their move to the cloud.

The effects of COVID-19 on the use of cloud services include:
- intense pressure on service availability from the Cloud Service Providers (CSPs)
- uncontrolled use of unapproved cloud services while working at home
- extreme reliance on secure connectivity to the cloud.

ISF Members can find more detailed guidance in the ISF report, Using Cloud Services Securely.

The Executive Summary for this report is available here.

DEPLOY YOUR CLOUD STRATEGY AS A BUSINESS ENABLER
Accelerate your move to the cloud to benefit from the greater elasticity and scalability it provides. Whether you are pursuing a cloud-first or all-in cloud strategy, now is the time to maximise cloud computing to enhance business operations. CSPs have so far shown robust levels of resilience whilst responding confidently to the increased global demand for cloud services.

RESTRICT THE USE OF UNAPPROVED CLOUD SERVICES
Limit the ability for users to access unauthorised cloud services (e.g. document storage, PDF converters and other file transfer solutions). Perform regular network traffic audits, constantly review the firewall rulesets and provide guidance to employees on approved cloud resources.

FAST TRACK ON-BOARDING OF NEW CLOUD SERVICES
Align with your procurement process to enable swift on-boarding of new cloud services while ensuring the minimum necessary cloud controls can be deployed. Pay particular attention to network connections, access management and data protection.

CONNECT SECURELY TO CLOUD SERVICES
At a minimum, use HTTPS to connect directly to non-critical cloud services. Secure VPN or WAN connectivity should be used for the most important cloud services. With the current spike in VPN usage, verify that the strongest encryption solutions have been deployed, vet all VPN solutions, keep them up-to-date and regularly patched.

MONITOR THE AVAILABILITY OF CLOUD SERVICES
Frequently check the service availability status of major CSPs in regions where critical cloud services are hosted. For smaller CSPs, it may be necessary to engage directly with service delivery representatives to obtain regular updates.

LEVERAGE EXISTING CLOUD SECURITY PRODUCTS
Take advantage of products and services designed specifically for managing security in the cloud environment. Cloud Access Security Brokers (CASBs) can quickly identify unauthorised cloud services and stop the exfiltration of sensitive data from cloud applications. Cloud Security Posture Management (CSPMs) can detect misconfiguration issues such as sensitive information being openly accessible to the general public.

FIND OUT MORE
Discover more useful resources at www.securityforum.org/covid-19/