CIONET

DISCUSSION SUMMARY

ADDRESSING IDENTITY MANAGEMENT IN A CLOUD-FIRST WORLD

This article was written by Roger Camrass, director of CIONET UK and a visiting professor of the University of Surrey, and is based on the conversations during a government dinner in July on 'Addressing identity management in a cloud-first world' sponsored by Zscaler.

Why is identify management an issue for government?

UK government is actively pursuing a cloud-first strategy across all departments, large and small. Government Digital Service (GDS) has promoted the use of the Internet to engage with citizens in every aspect of their lives. As cloud migration progresses, the problems of identify management and related security begin to surface as both government workers and citizens access applications based in a multi-cloud environment – well outside traditional perimeter-protected private networks.

Across the dinner table delegates described situations where a secure access mechanism becomes ever more critical in the era of cloud-first:

- Electronic patient records and associated information within the NHS
- Emergency services that include police, fire, ambulance and other departments
- Estate management that is adopting Building Information Management systems
- Railways and other public transport services that require coordination

What does a cloud-first strategy mean?

As government adopts a cloud first strategy it forfeits tight, perimeter-based control over user access and traffic movements within a private network. Instead it needs to adopt a borderless environment where applications and associated data can migrate to an eco-system of multiple clouds. Users of all kinds will be able to access a wide variety of relevant resources from mobile devices, anywhere, anytime.

A cloud-first policy implies:

- Shift of applications to multiple clouds – including software-based services such as Workday, Salesforce and Microsoft 365; and infrastructure platforms such as AWS and Azure. These are proliferating fast, often outside the control of IT
- Transformation of private networks into hybrid facilities, breaking down hub-and-spoke arrangements of the past and associated backhauling. In its place, networks take advantage of public Internet to speed up traffic flows and reduce costs

- Security transformation which heralds the end of perimeter-based arrangements, and brings a new era of software defined capabilities that are designed to secure data itself rather than private MPLS networks and on-premise data centres

In this latter respect the delegates expressed the view that they must design strategies based on 'zero trust' that no longer assumes that actors, systems or services operating from within the security perimeter should be automatically trusted, and instead must verify anyone and everything trying to connect to its systems before granting access.

What are the components of a cloud security strategy?

According to Zscaler there are at least four key components to be incorporated into a cloud-first security strategy. These are:

- Identify Management – a single point in the multi-cloud eco-system that can federate and confirm of a user's access rights to data and applications
- Cloud Policy Engine – sitting at the intersection of those multi-cloud services employed by an organisation, and thus able to oversee all security arrangements
- Security Operations Centre – equipped with the latest threat hunting tools and capabilities to ensure business continuity
- Data Privacy and Compliance – helping organisations to implement and monitor privacy and compliance policies over all internal and external services

Where are we today with respect to identify management?

As citizens we are all familiar with the diversity of applications and associated passwords that we use in daily life. Two mainstream platforms have emerged including Android and IoS to support mobile access to such applications. Neither seem to have solved the password problem, leaving us with long lists of codes that pose security challenges in areas such as financial transactions and personal data.

This situation is compounded in government as departments migrate core applications onto multiple Infrastructure-as-a-Service (IaaS) cloud platforms (e.g. AZURE, AWS and Google Cloud) as well as adopting an ever-growing number of Software as a Service (SaaS) offerings from multiple vendors. Many of the delegates complained about the number of active directories that they need to cope with – some departments exceeding 30-40. The prospect of 'single-sign-off' seems increasingly remote under such circumstances.

The strategy across government will be to enable citizens and employees to adopt a Multi-Factor Authentication (MFA) access approach that enables single sign-on to appropriate services and data sources. MFA can combine a multiplicity of factors such as location, biometrics, SMS access codes. It will be applicable to all devices and transform the user experience over time.

Taking security into the cloud

The prospects of preserving perimeter control to ever growing number of applications across government becomes increasingly remote in a cloud-first world. In addition, the wide dispersion of public and private data into a multiplicity of clouds presents greater risks to individual privacy. The delegates around the table agreed with Zscaler' s view that security itself must also migrate onto the cloud, offering:

- Single sign-on through MFA controls that understand user context
- Protection for data embedded in public clouds as required in a zero-trust world
- Software defined perimeters that can adapt to different clients and workloads

The main discussion point amongst delegates was about who decides policies and standards across government. Wholesale transformation of IT, as represented by a cloud-first strategy, will require higher levels of standardisation to deliver transparency of services to citizens. There appears to be a vacuum here that needs to be filled as migration progresses.

What to consider as next steps in the cloud journey?

There was strong consensus that security and associated identity management is a key component of any cloud-first strategy. Digital leaders in government need to answer the following questions:

- Where to locate security capabilities in a multi-cloud environment?
- How to implement a single sign-on for internal and external users
- What security standards should be enforced to ensure transparency across services

Which security partners would be appropriate in a cloud-first world?

About CIONET

CIONET is the leading community of more than 10,000 digital leaders in 20+ countries across Europe, Asia, and the Americas. Through this global presence CIONET orchestrates peer-to-peer interactions focused on the most important business and technology issues of the day. CIONET members join over a thousand international and regional live and virtual events annually, ranging from roundtables, programs for peer-to-peer exchange of expertise, community networking events, to large international gatherings. Its members testify that CIONET is an impartial and value adding platform that helps them use the wisdom of the (IT) crowd, to acquire expertise, advance their professional development, analyse and solve IT issues, and accelerate beneficial outcomes within their organisation.

cionet.com