CIONET

DISCUSSION SUMMARY

SECURITY WITHOUT BOUNDARIES: A GOVERNANCE ISSUE

This article was written by Roger Camrass, director of CIONET UK and a visiting professor of the University of Surrey, and is based on conversations during a breakfast on Cyber related topics sponsored by Okta in London this June.

Why is cybersecurity a growing concern?

Cyber-attacks are becoming an everyday occurrence as witnessed by some of the world's leading brands such as Sony, Marriott, British Airways and the NHS. With the exploding volumes of commercial data, the growing diversity of access devices and the migration to multi-cloud services, organisations are finding that traditional cyber defences are no longer effective. For example, firewalls that were designed to prevent outside-in breaches now offer little protection in a boundary-less, hyper-connected world.

Rogue states also present increasing threats. For example, Russia has become the 'superpower' of criminal cyber activity. China has stolen trillions of dollars of intellectual property from western companies. North Korea derives all its foreign income from raids on western banks.

As we enter a boundary-less world, infrastructures are morphing away from traditional service towers such as data centres and networks towards multi-layer stacks of logical components that include micro-services and multi-cloud platforms. Holding all these layers together is a new capability, Service Integration and Management (SIAM), that provides performance, commercial and security governance. Organisations are still struggling to assemble SIAM capabilities, but recognise the inevitability of such an approach. Central to SIAM is access security and identity management. This becomes a core feature of modern enterprise architectures.

Operating in a hyper-connected era

One issue raised during the breakfast was the proliferation of passwords necessary to access multiple cloud and on-premise services – sometimes as many as 15 to 20 per individual member of staff. This poses a security challenge but also makes access a time-consuming task. An alarming statistic provided by Okta suggests that 82% of internal breaches relate to stolen passwords.

There are established cloud-based techniques exploiting Multi-factor Authentication (MFA) that offer 'single sign-on' procedures. However, many of the delegates around the breakfast table raised the issue of governance – who is in-charge of secure access in a 'hyper-connected' world without boundaries?

Security today is about managing the identity of individuals who require access to corporate and public services – be they members of permanent staff; customers and consumers; or external contractors. It is also about identifying and repelling adversaries who are not entitled to any level of access. Depending on individual need, each category of user will require tailored solutions that meet their specific roles and requirements. Okta has introduced the concept of 'Identity and access management' or (IAM) that enables organisations to manage the identity of end users to reach different resources such as websites, cloud services and internal applications.

Who takes on responsibility for security management?

According to the breakfast delegates, many different parties may be involved in security management. IT is clearly a front runner here, but many such departments have lost visibility of the growing array of public cloud services that are being deployed by their business customers and end users. According to delegates there are an increasing number of functions that see security as their responsibility:

- HR who are responsible for on-boarding and retaining staff and are often involved in the personal authentication processes
- Legal who are conscious of growing regulatory and compliance issues around employee data as well as obligations to clients for secure access
- Risk officers who need to highlight and quantify the possibilities of reputational and commercial damage to their Boards
- IT who have the responsibility for developing secure enterprise architectures that are increasingly cloud based

In addition, business unit leaders see themselves as responsible for managing risks of all kinds, especially as they relate to customers and commercial partners. The challenge facing all such parties include assessing levels of risk in quantifiable terms; allocating specific responsibilities across functions; selecting security partners such as Okta; and monitoring overall security performance.

Delegates were quick to remind us that threat prevention is just another form of insurance. Companies must assess levels of risk and budget accordingly. In the case of a leading US bank, 2,000 people are employed to look after cyber threats. It is the only area of the Bank where budgets are uncapped!

Experience of cyber around the table

Given the diversity of sectors represented at the breakfast – from legal and financial to government and construction, we learnt of many new challenges. For example:

- In construction – the advent of digital twins (or databases) for buildings, from design, through build to lifecycle operations introduces potential threats, especially with the move to intelligent properties populated with IoT sensors
- In government – the adoption of Google mail and Google apps across 90% of all government staff in the UK has changed the nature of access security from something that was tightly controlled internally to that which depends largely on external partnerships
- Investment banking – the rapid development of new investment products needs to consider security of user access and customer deployment. Speed and agility in the development process needs to be balanced by such concerns

How to implement effective governance

To engage senior executives in cyber related conversations, the delegates agreed that one necessary step is to quantify potential damage due to security threats – internal and external. In this respect, cyber becomes one more critical element of the risk register. Techniques such as those offered by Okta help quantify the level of risk and its financial implications.

Once the Board is engaged in cyber conversations, the following actions will be necessary:

- Appoint a senior executive to coordinate all cyber activities through the organisation
- Understand who are your primary adversaries – both inhouse or external
- Evaluate the risks to the business – in quantitative as well as qualitative terms
- Consider the implications for enterprise architects whilst moving to cloud.

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