Re-enforce digital security

Develop the integrated security to reduce risks

KPMG Smart Government
Catalyse digital progress

Executive Summary

People and data are no longer confined to physical, specific places. We're working in more agile ways using remote systems to store personally identifiable information. In this modern world without perimeters, cybersecurity becomes a more complex issue.

Lack of perimeters leaves cyber vulnerabilities

The recent ransomware attack on one of the UK Government's widely used outsourcer by Black Basta has shown the devastation that can be caused without the right security measures in place. This attack is currently estimated to cost the outsourcer £15-£20M and that figure will continue to rise. It's not just the attack on the outsourcer though, it's the impact this will cause on people's personal lives with the data that will be exposed and made public.

Protecting data, networks, workloads, and user identities as users interact in cloud, mobile, on premise, and remote environments is no small feat. Zero-trust is a powerful framework to bolster government cybersecurity and equip government department leadership to manage risk in a more efficient and effective way. Had this been in place Black Basta would not have been able to achieve the level of intrusion witnessed.

It's time to rethink cybersecurity for digital, no-boundary environments

A zero-trust framework shifts any cybersecurity defence focus from network-based, static perimeters to protect users, assets, and resources. Government organisations are simply not keeping up with modern security demands — The WannaCry ransomware attack on the NHS in 2017 costed the UK economy over £10 million in one day.

The most important detail? Zero-trust helps governments maintain public trust.

Four components of our zero-trust framework:

- Strong identity management with authentication and user rights to help ensure access only to authorised people
- A mobile device/workload management strategy that includes application programming, interface security, frequent security updates and a workforce device inventory
- A software-defined perimeter service
- Data security measures encompassing a wide range of technologies and software, including data loss prevention tools and processes, file integrity monitoring, and encryption

[1] "Will Rishi Sunak reassess UK cybersecurity policies?" Open Access Government, November 21, 2022

[2] Black Basta ransomware attack to cost Capita over £15m" ComputerWeekly.com, 10th May 2023

Zero-trust is a multi-step process you may have already started.

With so many systems, processes, data and people to secure, complete threat mitigation is a fine art and a science. Creating a digital experience for customers that is secure means investing in a multi-step, ongoing zerotrust framework.You might be on the journey towards strong security, but there will always be new risks to consider.

- **Establish strong data governance.** Understand cybersecurity risks, seek resources to address vulnerabilities, and make risk-based decisions regarding resource allocation.
- **Protect the most critical data.** Assign each data breach category a rating of high, medium, or low importance, with the overall data set receiving the highest rating in any category.
- **Deploy a multi-cloud strategy.** Use more than one cloud service provider to flexibly align services and capabilities to meet needs.
- **Assign cloud gatekeepers.** Organisations can use cloud access security brokers as cloud gatekeepers to oversee information and threat protection from malicious attackers, even beyond the government customer's network perimeter.
- **Establish accountability.** It is important to not only implement effective, efficient network controls, but also monitor their use and maintain their effectiveness.
- **Foster a cybersecurity mindset.** Cascade responsibility so all personnel understand the importance of data protection and their specific roles.

Breaking down the numbers in the UK

Almost

50,000

UK government ministers and civil servants were vulnerable to cyber-attacks until March 2020[1].

£10 million,

in one day was the cost of the WannaCry ransomware attack on the NHS in 2017 to the UK economy.

85.5 percent

of respondents among 300 UK public sector organisations surveyed in 2020, said they would "prefer a multi-cloud vendor.

[1] "Global number of cyber security incidents in 2020. sorted by victim industry and organisation size," Statista, 2021.

[2] "IOTW: Almost 50,000 UK government ministers vulnerable to cyber attacks", Olivia Powell, Cyber security hub, 2023.

[3] "Will Rishi Sunak reassess UK cybersecurity policies?" Open Access Government, November 21, 2022.

[4] "State of Cloud Adoption survey 2020" UK Cloud. 2020.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/uk

CREATE | CRT145789B | May 2023

Document Classification: KPMG Public