Roke

Part of the Chemring Group

An Intelligent Approach to Cyber Security

- Cyber attacks can cost a company dearly in both monetary and reputational damage
- How businesses can compete without their latest cyber counter-measures tying their hands behind their back

The impact of a cyber-attack is significant, and the combined loss of reputation, intellectual property, customers and legal damages is punishing. You just have to look at the high-profile cyber-attacks suffered by Tesco Bank (a sophisticated attack orchestrated by a criminal group in November 2016[1]) and TalkTalk[2] in October 2015, the latter of which wiped £15m off trading revenue, racked up costs of £40-£45m and lost almost 101,000 customers. These threats are emerging from a combination of increased ability amongst cyber criminals, as well as the hyper-connectivity of enterprises.

Yet organisations do not seem to be keeping up with this evolution; what's stopping your company embracing higher levels of cyber security?

For our clients the biggest factors often seem to be market confusion, budgets and security becoming a 'blocker' in day-to-day business. On the other hand, I commonly see the threat of cyber-attacks leading many organisations to lock down their systems in an attempt to achieve adequate protection, which can increase your risk.

THE DEFAULT RESPONSE - LOCK-DOWN

A computer is supposed to act as the tool for more efficient business, yet when the security mechanisms put in place to protect data start to slow users down, the human response is not a positive one. The lock-downs ultimately impact the efficiency of the business and an individual's ability to perform their role. Historically, staff become frustrated by not being able to do what they want, when they want, where they want – whether this is working with multiple complex passwords, forgetting to bring the additional token that is needed to grant system access, or not being able to work remotely. Consequently, employees often find a 'way round', resulting in unintentional security breaches. This of course opens up the organisation to cyber-attack and information leakage – the very thing the introduction of the cyber counter measures expected to avoid.

Luckily, this doesn't have to be the case. My preference is to find an individualised approach to security, which puts usability first.

WHICH SECURITY APPROACH?

With each organisation facing multiple risks based on their differing operating models it's time to take an individual approach to protecting against them. By using a business-led, threat driven approach with appropriate cyber risk defined, the result is a robust security architecture with great usability that mitigates the risk of an attack. As a first step, the chosen security strategy requires insight. You need to know what those risks are and the level of threat they pose to your organisation. This consists of the following stages:

1. Understand user needs – First and foremost, understand how the organisation needs to be able to operate to be efficient and deliver a great service to its customers.

2. Asset identification – Understand what information the business needs to protect and why.

3. Threat identification – Next we look at the threats. This requires a sharp understanding of what cyber-attacks are possible. Once the potential and emerging threats have been identified, characterise them to help establish the best method of protection.

4. Vulnerabilities – This is an in depth review of where data is vulnerable and what the consequences of an attack would be. Without understanding the effect an attack has on the business, it is hard to justify the measures needed to protect it.

5. Risk – Quantify the risks in business terms faced by an organisation to enable the appropriate risk judgements to be made.

6. Risk control - Now that the current level of exposure is understood, develop ways to control that risk using a combination of technology and process appropriate to the organisation, whilst ensuring that user needs are met.

7. Risk management – Threats will continue to evolve, as will an organisation's way of working; therefore organisations must continue to develop their processes to manage this.

Once a plan is in place, it's time to make this work in practice, and there are a number of avenues to pursue. The one aspect which all new security choices must consider as a top priority is usability, delivering productivity gains to the organisation without compromising security. So how can this balance be achieved?

SMART SECURITY

The risk of security breaches can be minimised by putting usability first, then leveraging available security to support appropriate business need. The result is a user-friendly IT system with the appropriate security in place to provide a cost effective solution for the organisation. For risk owners, it's time to endorse this alternative approach to meet the needs of end-users and remove the temptation of unauthorised workarounds and risk of business disruption. But how does this work in practice?

Through our partnership with the National Cyber Security Centre (NCSC) we are not only exploring more user friendly cyber security solutions, but also aiming to help industry take advantage of the technology and understanding already at its fingertips. Take smartphones for instance, when we saw Apple making a stand against the 'back door' option for the US Government. With the Government needing to ask for access, the effectiveness of security built into the modern smartphone becomes more apparent. And this isn't the only platform where technology offers quick and simple mitigations to the cyber threat.

Enterprises, both Government and commercial, must make use of this functionality in order to grasp the benefits that technology delivers, and remote working is a prime example of where this approach can bring significant benefits. This can strike fear into the heart of the IT department and Chief Information Security Officer (CISO) because of the potential security threats it brings. However, being able to work from home, from client premises, or on the move has become necessary for most businesses. The following present two situations that can benefit from a new, intelligent approach to Cyber Security:

- Removing the fear from mobile working – Traditionally, the approach to keeping mobile working 'safe' has been to instigate a system of complex passwords, bespoke tokens and to lock-down functionality on trusted machines. Not only does this mean increased IT costs in managing these procedures, but the potential for end-user opposition and unauthorised workarounds become significant factors. An alternative and smarter approach would be to exploit today's commodity security features. This could be as easy as selecting the options to use the security hardware already built into a laptop or tablet, or utilising the user's smartphone as a two-factor authentication token.

- Securely viewing sensitive documents on the move – In the past, employees have been forced to go to a computer that has the necessary technology to view sensitive information, or wait for a paper copy to be sent and stored appropriately. With such inflexibility, many end-users

have found ways around security measures by sending a copy to their personal mailbox, or by taking a copy on an unencrypted USB token. However, improved security architecture (such as TEE and TrustZone) is now readily available on modern smartphones. This would allow users to open and view documents quickly via encrypted email within a safe enclave on their personal smartphone. By making it quick and easy for the user to operate securely, it's possible to protect your organisation from cyber threats in a much more efficient fashion.

SUMMARY

With careful thought and help from experts in cyber security, it is possible to increase security without compromising usability. To save reputational damage, avoid associated expenses and protect the valuable data your business holds, it's time to take a step back and take a considered view of your cyber risk. Throw away the tick sheet and manage the cyber risk appropriate to your organisation. You will at the same time provide a better end-user experience while improving security and keep up with evolving cyber threats.

Read more about cyber security at Roke or contact us to find out more.

References:

1. Leyden, J. (2016). What went wrong at Tesco Bank? Available at: www.theregister.co.uk/2016/11/10/tesco_bank_breach_analysis

2. Glock, B. (2016). TalkTalk hit by record £400,000 fine over data breach. Computer Weekly. Available at: www.computerweekly.com/news/4504004 51/TalkTalk-hit-by-record-400000-fine-over-data-breach

RICHARD MORRIS

CYBER PROTECTION

Richard Morris is the Cyber Protection Lead at Roke Manor Research, CESG's only UK Conformance Test Facility for Protocol Requirements for IP Modular Encryption (PRIME) and also a highly respected CESG Commercial Product Assurance (CPA) and CESG Assured Services (CAS) test lab. Roke performs security evaluations of the products and systems used by UK Government to protect the UK from cyber-attack, and provide advice to UK Government and large enterprises regarding how to manage cyber risk, including the intentional and unintentional insider threat.

Roke Manor Research Ltd
Romsey, Hampshire, SO51 0ZN, UK
T: +44 (0)1794 833000 • F: +44 (0)1794 833433
www.roke.co.uk • info@roke.co.uk