Paralogic IT
TRUST IN TECHNOLOGY

SECURITY BRIEFING: DEFENDING THE RANSOMWARE THREAT

How best to defend your business and recover from an attack

A Paralogic IT White Paper

www.paralogic.co.uk sales@paralogic.co.uk 01844 293330

Introduction

Cybercrime: Fast growth, big returns!

Bank interest is practically zilch and the prospect of a property crash can never be ignored. It's tough investing for a decent return without loading your portfolio with risk. Looking for somewhere to invest to make big returns, fast? Have you considered cybercrime?!

That's a light take on the subject of cybercrime; however, for the executive it's no laughing matter and the question of IT security is likely to be the source of some discomfort in board rooms across the entire spectrum of business.

An IT security breach has the potential to leave a business between a rock and a hard place. Disrupted business operations and difficult conversations with customers might seem manageable; however, reputational damage and the fallout from an ICO investigation are matters that are well beyond the control of any firm.

In January, analysis by PwC reported in The Guardian said that approximately 55% of UK firms have fallen victim to fraud in the past two years. Cybercrime was shown to be the fastest-growing area of fraud, growing by 24%, up from 20% to 44% in little over a year.

The report also showed that more UK firms were falling victim. The global rate of companies hit by fraud was 36%, while at 55%, the UK's was nearly 20% higher.

Activists that hack - 'hacktivists' - and generally misuse digital technology in support of their causes, and hobbyist hackers - those who target high profile organisations like NASA or the US military for bragging rights - might simply be regarded as a nuisance.

However, in the midst of it all is the spectre of terrorism. From committing fraud to fund their activities, to using cyber warfare to attack infrastructure, the threat is truly cause for concern. The technology capabilities of terrorists should never be underestimated.

Malicious software – 'malware' may take many forms. From phishing scams which attempt to trick email recipients into revealing account details and passwords, to nasties such as viruses, and spyware which is intended to report back user activity and information to the servers of cybercriminals. The threat to IT security has probably never been greater.

Ransomware threat is growing

The ransomware threat has been steadily growing for a number of years. According to June 2016 figures from IT security experts Kaspersky, there was a 17.7 percent rise in ransomware attacks in the period April 2015 to March 2016 compared to the previous 12-month period, rising from 1.97 million attacks to 2.32 million.

Crypto ransomware encrypts data, leaving it inaccessible without the cryptographic key which is provided on payment of the ransom demand. Crypto ransomware attacks increased 5.5 times, rising from 131,111 in 2014/15 to 718,536 in 2015/16. Projections by the FBI suggest that ransomware is on target to extort more than $1 billion in 2016.

The risks of paying ransomware demands

It is practically impossible to overstate the risks associated with paying a ransomware demand.

- **Who are you paying?**
  These organisations could be terrorists, or criminal agencies. By paying you may be funding a range of criminal activities such as terrorism, money laundering, the narcotics trade, people trafficking and international arms dealing

- **Paying is no guarantee of data recovery**
  If there is no honour among thieves why assume criminals will honour the 'arrangement'?

- **By paying you are saying "I am an easy target"**
  Like burglars, ransomware criminals are likely to pursue the tactic of repeatedly targeting victims

It is important to be clear that no legitimate and responsible business can endorse the payment of such ransoms. The best advice to victims is not to pay and report the incident to police. However, many businesses may not be in a position to do this.

Why many choose to pay when falling victim to a ransomware attack

In response to an attack, many businesses may not be in a position to refuse to pay. This is because there is a lack of certainty when it comes to these key questions:

1. Do we have the capability to totally restore systems and data?

2. Can we tolerate disruption while systems and data are being restored?

For many the answer to question 1 should be a simple yes. However, often it isn't. When it comes to question 2 the very first thought is how long is it going to take?

These questions go to the heart of what some believe to be the First Three Rules of IT:

Backup, backup and backup!

Identifying your backup requirement

A thorough assessment of the backup requirement can only be made if you approach it from the perspective of Disaster Recovery(DR) and Business Continuity (BC).

Before you know what backup capability you need, you have to identify two key things...

Recovery Point Objective (RPO)

How far back in time do you wish to be able go?

This is often determined by how much work or change to real time data you are able to tolerate losing. Bank ATM systems, which are transacting 24/7 for example, cannot tolerate any loss of data. In a more mainstream business you might tolerate an hour, or perhaps a day, depending on the nature of your trade and the expectations of your customers.

Recovery Time Objective (RTO)

How long before you require systems and data to be available again?

This is often determined by the nature of your business. Medical systems such as those for radiology, which may be the difference between life and death, cannot afford to be unavailable for anything other than perhaps a few minutes, if at all. In less critical businesses an hour or a day may be more realistic.

Restore from backup or pay?

If you cannot answer question 1 with any certainty and have not properly examined the RTO and RPO requirements of your business raised by question 2, then you may have little alternative other than to pay a ransomware demand.

Prevention better than cure: Avoid falling victim

In many IT data loss scenarios, backup is simply the backstop and every reasonable effort should be made to avoid the need to bring it back from the brink. It follows, that like many other risks that need to be managed around business technology, the prevention of ransomware attack is better than cure.

Tools to avoid ransomware and attack by other malware

Here are some of the key tools tactics that are used to defend ransomware attack and prevent cybercrime in general. They form the basis for a layered approach to IT security which provides a degree of overlap, maximising protection.

Human factors

Pro-active IT administration

Windows and third-party application updating and patching; regular monitoring for IT security news on new and emerging threats and best practice

User awareness and training

Raise user awareness around the threats and best practice for using the web and email; consider training for existing staff and induction for new starters

Technology tools

Firewalls

Also known as security appliances, these hardware devices lockdown networks, preventing intrusion by hackers and blocking downloads of suspicious files from the Internet

Anti-virus software

Software designed to detect suspicious files and activity across networked mobile devices, computers and servers

Email scanning

Cloud security services which scan all incoming and outgoing email traffic for suspicious attachments; may provide extra value through archive and backup email services as well

Backup systems

There are a wide range of backup options to provide the RTO and RPO that are required, as determined by the needs of each business

What can we do to improve security for you?

Any Paralogic client that is concerned about the increased threat from ransomware should contact us as soon as possible. Many are aware of the issue, however, the IT security threat environment is characterised as agile. It is constantly evolving and threats continue to emerge on what some observers believe to be practically a daily basis.

This means that a constant process of reviewing the situation and adapting your approach is required. The countermeasures you may have put in place last month, last week or even yesterday, may need to be changed to reflect what is a fast moving and continually morphing threat. We are here to help our clients through providing advice and providing the right solutions.

Not a Paralogic client yet?

Security remains a cornerstone for ensuring technology returns maximum value to our clients' businesses. This document is just one example of the pro-active approach we take in helping smaller, expanding and mid-sized companies to get more out of their investment in technology.

If you're not a Paralogic client, just contact us to discover how we can help you to best defend and recover from a ransomware attack.

About Paralogic IT

Paralogic is an award winning MSP delivering IT systems and managed services to hundreds of businesses, schools and charities across the UK.

Our clients trust us to take care of all their IT needs, from strategy through to implementation and ongoing support. In return we go the extra mile to help people achieve their business goals.

References and further reading

UK businesses battling huge rise in cybercrime, report says
The Guardian
https://www.theguardian.com/technology/2016/feb/25/cybercrime-uk-businesses-battling-huge-rise-silver-fraudsters

Five-fold rise in crypto-ransomware hits 718,000 users in a year
SC Magazine - specialist website for IT Security professionals
http://www.scmagazineuk.com/five-fold-rise-in-crypto-ransomware-hits-718000-users-in-a-year/article/504744/

Cybercrime
Interpol
http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

www.paralogic.co.uk sales@paralogic.co.uk 01844 293330