Jenrick:IT

BE SAFE - CYBER SECURITY:

DO YOU HAVE THE BEST VULNERABILITY MANAGEMENT PROCESSES IN PLACE FOR YOUR BUSINESS?

by Janos Meszaros

I recently attended an excellent Webcast (The Truth about Vulnerability Management: Compliance Checkbox or Real Protection?) hosted by SC Magazine.

The guest speakers were Joerg Weber - Head of Attack Monitoring, Barclays, Lee Barney - Information Risk Consultant at Major UK Utility, Michelle Cobb - VP Global Marketing at Skybox.

The main message that I took from the webcast was that all organisations need to look at their current cyber security processes and to understand if they provide sufficient support for their business.

"Security should be there to assist and protect the business, but never to hold it back from its main purpose which is to operate effectively and make money."

Here are some key steps to consider:

When you look at your security processes you have to understand **exactly what it is that you are protecting** and if you are **protecting the right assets**.

"Quite often companies can waste resources protecting 98% of irrelevant information, instead of focusing on the 2% which has real importance."

Companies **also need to assess vulnerability** based on **location** and **criticality**.

It is also important to understand potential threats against your organisation and **prepare for the most common / likely / obvious ones first.**

It is worth looking at publicly available cyber security solutions created by the security community before you go out to the commercial market to commission a bespoke solution. There are number of public threat feeds available, such as Packetstormsecurity, such as **packetstormsecurity.com**

In addition, assess the tools that you are currently using to monitor threats. Ideally you need an **automated tool** which will help you to interpret and prioritise the large amount of data coming through and allow you to act on any potential threat in the shortest possible time.

It is important to keep your systems up to date, so *patching* and having an appropriate *patching cycle* are very important.

However, it is essential to find the right balance in deploying patches; a patching cycle that is too frequent can be disruptive to the business, yet neglecting patching leaves open doors for an attack.

"All the professionals agreed that critical patches need to be deployed as soon as possible, but NEVER later than 14 days from the release."

If your IT systems are outsourced it is essential to evaluate your **service providers** from a cyber security perspective.

You have to **be clear on what your expectations are** to protect your information and you have to make sure that you clearly understand the chosen service provider's cyber security procedures and the impact that will have on your business.

When an agreement is put in place (with an external provider) it is important to agree a schedule that allows you the opportunity **to review and revise the procedures and the quality of the service you are receiving**. This will ensure that your business is constantly receiving the level of support and protection you require / agree upon.

Also, you have to be realistic and appreciated that it is impossible to prepare for all eventualities or potential cyber attacks upon your business.

(Contd. On pg 2)

(contd. From page 1)

All you can do is ensure that you have the right tools, people and processes in place to deal with the worst case scenario (whatever that may actually be).

The MOST IMPORTANT aspect of any good security process is to have a quick and effective INCIDENT MANAGEMENT in place.

"Most companies have never actually tested their crisis management plan or disaster recovery plan. Only through testing will you iron out the bugs and get slick at minimising data loss / corruption / business down-time."

CLOSING NOTES:

As much as our IT systems are here to help us and make our businesses more successful, but also are liability that can be exploited.

The number of attacks against our private, commercial and public systems is increased substantially in the recent years.

Fortunately this has been recognised on a government level and the UK government recently announced that they increase the investment by 3.4% within the Intelligence Service budget (**deloitte.com**).

IN SUMMARY:

One school of thought is that these threats are making our lives more difficult, however, my personal perspective is that they also pushing us to technologically evolve; and more importantly, they are providing us with new opportunities to develop skills, careers and businesses.

LEARN MORE ABOUT JENRICK IT:

Jenrick IT are a specialist recruiter to the cyber security and defence sector.

Our specialist cyber security and defence team are experienced in sourcing and delivering SC and DV cleared contractors and permanent staff to enable companies to successfully deliver on their current projects on time and on budget.

Click here to learn more.

CONTACT JANOS MESZAROS AT JENRICK IT:

If you would like discuss and reassess the cyber security management processes for your business please contact cyber security expert Janos Meszaros:

Jenrick:IT

Janos Meszaros
Recruitment Consultant
Email: janos.meszaros@jenrick.co.uk
Mobile: (07557) 271076
http://uk.linkedin.com/in/janosmeszaros
The Clock Tower, Bridge Street, Walton on Thames, Surrey KT12 1AY
Tel: (01932) 245 500 | Fax: (01932) 245 900 | www.jenrickit.co.uk