5 STEPS TO A PROACTIVE CYBERSECURITY PLAN

The overall lack of confidence in cybersecurity is noticeable across the whole of the digital world. Collecting our information in any way or form is either accepted or frowned on by most.

What are they going to do with it but more importantly how are they going to protect it?

The more sophisticated the systems we use the more reactive we seem to get and when it comes to cybersecurity a reactive process is not the best solution.

Care MIT
3 / 116 – 118 Wollongong Street,
Fyshwick, ACT. 2609
02 62577792

REACTIVE VS PROACTIVE SECURITY

There are only three types of responses to a cyber-attack.

Reactive - if it happens, we will do something.

The problem with this attitude is that when it does happen it is already way too late.

This is a traditional approach to cyber defence.

A rudimentary protective requirement that often includes basic firewalls and free antivirus.

It usually accompanies the attitudes of

- Too small to be a target.
- It will never happen to us, and
- We have nothing worth stealing.

It relies on the first indication of an attack or infection being the people using the devices noticing something "strange".

The biggest issue with a reactive process is the lack of visibility of not only the systems but also the threat landscape.

It is hard to get a full and comprehensive vision of what can happen, what has happened and are we being targeted.

There are several reasons why an organisation would implement a reactive security envelope.

- It has been around for a while and "that is the way we have always done it".
- It allows for choices of technology to be made that would be more beneficial for the organisation.
- It is the simplest to implement.

Proactive – let's think what could happen and plan against it.

Proactive on the other hand is based on Risk management and implementing systems and requirements to mitigate those risks.

Proactive uses threat intelligence and real time system monitoring to visualise the business environment and respond to perceived attacks and changes.

Proactive responses are not designed, as many security organisations will tell you, to stop you from doing business the way you want to do business.

All businesses, no matter the industry, are unique. The way you create revenue and deliver your products and services is different from anyone else.

Even franchises, although they are the same are still unique.

That is why proactive security is so important.

Identify the risks to your business the way you do business and then mitigate them in the way the business wants to mitigate them.

Once a risk to your business is identified it can be mitigated in one of four ways.

- You accept the risk. The impact on the business will be minimal.
- You avoid the risk. Change the way or implement policy, people or technology. Change a process to reduce the risk.
- Transfer the risk. Insurance and warranties for instance.
- Reduce the risk. Bring it down to a manageable level.

A proactive security system is based on the three data criteria of the CIA (Confidentiality, Integrity and Availability)

This also allows the organisation to define its risk appetite and apply it to all areas of the business.

Proactive is risk management and implementing contingencies.

Active – when they come, we will do something.

There is also a security stance that take a little from proactive and a little from reactive.

Most organisation are in this middle range. They have basic security system in place but have probably initiated the essential 8 business security requirements.

Those 8 are:

1. Patch operating systems
2. Patch applications
3. Implement 2 factor authentication.
4. Reduces administrator logons.
5. Hardened all systems.
6. Implemented a whitelist.
7. Reduced the use of unauthorised macros and scripting.
8. Have a tested backup.

In addition, they will have implemented a password policy, A standard business digital policy, purchased and configured a decent level 2 firewall and upgraded to end point protection.

Care MIT
3 / 116 – 118 Wollongong Street,
Fyshwick, ACT. 2609
02 62577792

HOW TO MAKE YOUR SECURITY POSTURE MORE PROACTIVE!

Reactive is OK for an occasionally situation but in today's security environment, people, even well-trained people, will burn out quickly and significantly.

Moving from reactive to proactive will take an investment in time, capability and money.

Have a unique strategy for your most common threats.

It is a common viewpoint that most organisations have already been compromised in some way or other.

With that in mind it is wise to balance prevention with the realisation of active searches.

When it comes to your organisation you have to understand the common threats associated with your environment and your requirements.

- What are your assets.
- What could be an attack against your assets.
- Have you had any attacks on these assets before.
- If these assets have been attacked what were the attack vectors and what systems did they compromise.
- Do you understand them vulnerabilities to these assets.

These questions pinpoint how cyber criminals could target your organisation as well as understanding how they have achieved an attack historically.

If you have not or do not understand where attacks may have come from these are a number of examples of attacks against your organisation.

- Brute force.
- Denial of service.
- Malicious software.
- Email fishing attacks.
- Ransom where.
- Social engineering attacks.
- Attacks against databased components including websites.

Proactive is not just tick the box of a compliance audit or a component of the security envelope.

There are thousands of products in the marketplace designed to protect one facet of your organisation.

Care should always be taken to implement a protective strategy around a specific risk to ensure that money is not wasted, time is not expended, and capabilities are not compromised.

When it comes to implementing security technology the following questions should be asked.

- Do you have the right training and knowledge transfer in place to ensure the technology is going to work to the level it is designed to do?
- Is technology being added to address the strategic component.
- Does it have a measurable return on investment?
- Can it be integrated into all existing and proposed systems?
- Is it cost-effective?

The most important component of the technology for security is to ensure that it meets the requirements of the organisation and if possible a proof of concept should be adapted to achieve the required protected requirements.

Understanding what your business does.

Your business is unique.

It already has a large number of policies, processes, procedures, standards, plans in place to ensure that anybody within the organisation has a clear understanding of the organisations requirements.

This allows the organisation to function in its uniqueness.

A training program should be initiated to ensure that present and future staff understand their requirements to protect the business.

- Aligning security with the business uniqueness is important.
- Business security is everybody's requirement.
- Train your staff including management and give them the right tools and authority to succeed.
- Game If I and challenge your staff and ensure that results can be measured.
- Create an open loop that allows for a constant improvement process.

Everybody in your organisation should understand the organisation's mission and the security requirements within that organisation.

Security awareness, policies and procedures are essential for a improved business security environment.

Set clear roles responsibilities and expectations.

There should be clear roles and responsibilities within the security team as it is essential efficient and effective incident response.

By assigning responsibilities and implementing expectations there is a clear alignment within the organisation and the teams and any projects implemented.

Be aware of what the criminals can do.

If you think like cyber criminal then you will implement contingencies and plans around those ideas.

This allows your security team and insight into how the organisation should be protecting itself from a cyber event.

Invest in security requirements.

As part of the security envelope vulnerability scanning and risk analysis should be paramount.

Regular irregular vulnerability scanning of systems, networks and smart devices gives in-depth visibility to how the cyber criminal could target your organisation.

The utilisation of pen testing should only be initiated when everything else has been implement.

It is no use doing a penetration test without implementing the regular security requirements to may be able to see what the pen test is actually targeting to ensure that not only are vulnerabilities addressed but also that if a targeted attack happens your internal security team will understand what is required to stop it from happening.

Incident response.

An incident response or breach plan needs to be implemented if the system indicates a breach.

If you are doing pen testing then a incident response report should be raised by the defenders to show that they had an understanding of what was going on.

This should be done regularly either as tabletop exercises or full-blown business requirements.

If you have not got a tested backup are an idiot.

In the event where everything else has failed you need to be able to get back to business as normal as fast as possible.

To achieve this, you need to have a backup of all critical data, asset requirements and systems as necessary.

Implement the 3 2 1 rule when it comes to backups.

Three copies of all critical data, into different locations, and one of those locations has to be off-site and out of band.

Implement a process of visibility.

When purchasing new security technology is essential that not only integrates with historical systems but also integrates with systems already in place.

This allows for visibility and interoperation requirements within the organisation, referred to as a single pane of glass view.

This list is not a defined requirement for proactive security it is a very good start and points the organisation in the right direction.

Some of these requirements can be automated to improve functionality.

WANT HELP IN IMPLEMENTING A PROACTIVE BUSINESS SECURITY SYSTEM?

If you are concerned about how to make your business more resilient using a flexable proactive system.

Our system is 6 areas that are tailored to integrate together into a security solution that is noy a silver arrow approach.

Want to know more information just click on this link and book an appointment with one of our professional security people

https://letsmeet.io/rogersmith/the-ebook-series-6-books-mat

Care MIT
3 / 116 – 118 Wollongong Street,
Fyshwick, ACT. 2609
02 62577792