Get these basics right to start winning the cybersecurity battle

JULY 26, 2019 CYBERSECURITY / TECHNOLOGY

Can one live long and prosper in cyberspace with goodwill only? Although Mr. Spock's famous blessing is still valid, these contemporary times call for adding another adjective to it: secure.

Regardless of the sector and industry, from the boardroom to the corridors and coffee spaces, discussions on how to remain acceptably "cyber-secured" are ubiquitous.

We all know that any organisation's most valuable assets are its clients and valuable information – data and knowledge – that allow the business to develop, innovate and grow.

Somewhere around 500 B.C, Heraclitus wrote this sentence for posterity: "No one that encounters prosperity does not also encounter danger." If, simply put, what he said means there is no good without bad, there is always the bad kid of the block trying to make some damage to your business in different ways. However, lately, the bad kids have exchanged iron for silicon, and bullets for bits, the ones that assault your information systems to infect, disrupt or hijack.

Apart from the costly technical damage and the stealing of sensitive data, a cybersecurity attack severely reduces clients' trust, and could lead to permanent business disruption. It is, therefore, an imperative to maintain acceptable security levels of any business's information assets or its partners.

Let's recall Heraclitus once more. This wise Greek also said, "There is nothing permanent except change." That's a valuable statement to bring up in the cybersecurity chess game: the cyber adversaries keep evolving their tactics and techniques, and applying

Should businesses bear in mind Heraclitus's statement, cyberattacks may be less frequent or less lethal, but it isn't the case. Most reported cyberattacks still take advantage of basic and well-known flaws inside organisations.

In this article, we outline some of the most basic practices organisations should embrace to achieve the minimum acceptable security level. We recommend your business gets the basics right, and keeps it simple but equally efficient and effective.

So your business can live long, prosper… and be secure!

Get these cybersecurity basics right

Make sure you use state-of-the-art systems

We undoubtedly had to include this tip on top of the list!

We cannot emphasise more the importance of having up-to-date systems. A majority of cyber incidents that reach global scale capitalise on known vulnerabilities. This stems from negligence or a poorly-defined patch management framework. When constraints prevent adequate patching, businesses must implement compensative controls to cover the risks.

To take a step further, businesses want to stay on the watch for publicly announced zero-day vulnerabilities and the available workarounds.

> What's a zero day vulnerability?
>
> It's a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals. It's called "zero" because the time between vulnerability discovery and the first attack is zero days.

Key action: Update and Upgrade!

Send systems you no longer use into temporary or permanent retirement

Sleeping guards never ever have a good reputation in movies, do they? Obsolete or dormant systems and applications neither. They are juicy points of entry for attackers.

Most of these systems, indeed, have limited or zero support from vendors and, consequently, do not have up-to-date security features.

In certain cases, well-intentioned employees who are responsible for ensuring that systems are up to date, tend to focus upgrades on the ones that are active in production. Sometimes inadvertently, or sometimes not sufficiently prudent, they expose the entire business infrastructure to menaces.

Think of decommissioning and disconnecting from the network systems that are no longer in use, or won't be for certain period of time (based on risk appetite).

Key action: Shut old systems down!

Because collaboration is key, you need keys to collaborate

Productivity is greatly influenced by collaboration among users, platforms and systems. The level of interconnectivity, then, is pivotal to implement that collaborative work. Nowadays, technologies that are gaining ground such as IoT or Cloud technologies call for even greater interconnection.

To enable secure collaboration, users and/or systems require that they have been granted access. But failure to appropriately provision, de-provision and monitor both user and system accounts and their authorisations poses a great opportunity for attackers to make entries and move laterally in our networks.

Adopting Identity and Access Management Systems is a step businesses are taking more and more, but when they are improperly managed, woes are considerably higher.

The adoption and strict adherence to simple information security principles such as "Least Privilege" and "Need to Know" is a necessary movement when playing the cybersecurity chess.

Key action: Manage identity and access

Adopt the no-hero mindset: cyber warfare is too dangerous to fight it alone

Just like the saying "no man is an island", no organisation is self-sufficient enough to win and thrive in the current cyber warfare.

On the contrary, every business wants to be actively involved and engaged with peers to share cybersecurity ideas, news on the field, trends and, sure thing, best practices on ways to protect, respond and recover from cyber incidents when they occur.

"Cyber" community engagement can be achieved through seminars, conferences, mutual aid agreements, subscription with response teams and so on.

Key action: Don't be shy, embrace the community!

Remember, compliance is not security. Nope.

When pursuing new projects, looking for increasing the customer base or gaining stakeholders' trust, most businesses find themselves in a race to comply with all standards and regulations out there.

Undeniably, it is fundamental to ensure your business is compliant with key information security standards and frameworks such as NIST, ISO 27001, ISF, COBIT etc.

However, be mindful that compliance is not security. Take the time to understand your business and its ecosystem, and identify your competencies, assets and potential risks. This apparently obvious but sometimes forgotten reflection time, helps businesses optimise efforts to protect and defend from the bad kids against whom is worth fighting.

Key action: Comply but stay secure!

Trends are cool but ultimately die. Your business must remain

While staying in the loop on releases from vendors and community trends, businesses want to keep an eye on day-to-day activities performed internally, and on externally exposed systems. Understand and define what normal behaviours look like, then choose a best fit (and not the best tool) to monitor the infrastructure to detect normality deviations.

Key action: Monitor your infrastructure

Think of the business ecosystem for better cybersecurity

As mentioned before, identifying core competencies and capabilities is paramount for businesses to cope with cybersecurity challenges. Precisely because of this, outsourcing some functions provides business the opportunity to focus on their core activities and improve efficiency.

When outsourcing, there is a caveat one needs to consider. More than half of all cyber incidents that businesses have reported were flaws in providers or collaborators' infrastructure. This highlights the importance of owning one's risks, and closely monitoring existing business partners' functions. Similarly, it's important to keep a close eye on what approach to monitoring outsourcees or partners have.

Key action: Monitor your business partners' infrastructure

Bear this in mind: there isn't trust by default

There is no such thing as zero risk in any environment. However, there is the zero trust concept. Businesses can adopt it to eliminate certain default trust that exists between security perimeters. Indeed, taking into account the lack of clarity in security perimeters, this concept further establishes the requirements to verify anything before access is granted, including "trusted" external parties.

Key action: Adopt Zero-Trust concept!

Sharing is caring (but only sometimes)

It only takes one security glitch to start an information leak allowing users with malicious intent or criminals to achieve their goals.

Do not leave sensitive data or information unprotected neither in the workplace nor even at home, and think twice before unveiling apparently innocuous information on social media, website or even via phone in a public space. It's quite obvious, isn't it?

Well, it isn't actually. Think of this fact: the bad boys can collate and analyse personal information we share on social media to understand our behaviours and get information about our hobbies, where we go, with whom, and when. They can create convincing lures to assault us using not only personal channels but also the professional ones.

Key action: Mind your data

When stating the obvious is good for cybersecurity

We know we haven't reinvented the wheel by listing these practices, but it's always good to recall them because our memories are fragile. You may know the saying; "A tip even from a rabbit"!

These tips are closely connected and they complement each other to achieve a common goal, securing information assets.

Just like everything else, effective information security starts from the grassroots – by this, we mean the organisational culture. Whatever you do, get the basics right and while doing so, keep it simple!

What we think

> *Keep your secrets, secret! We're used to building virtual castles to protect our environment. It is time to rethink the current applied models and move on from infrastructure protection to user and data protection.*

Koen Maris, Cyber Security Director at PwC Luxembourg

CYBERSECURITY / DATA PROTECTION

PREVIOUS POST

Six AI priorities you can’t afford to ignore

NEXT POST

Could MOOCs become a valuable tool in Upskilling?

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name*

Email*

Website

□ Save my name, email, and site URL in my browser for next time I post a comment.

Post Comment