hAPPenings

August 2018

PIONEERING PROGRAMMERS

CYBER CRIME WHAT EVERY BUSINESS SHOULD KNOW

The cost of cyber-crime on an annual basis around the world is a staggering $445 billion! The most surprising aspect about cyber-crime is that despite causing billions in damage to economies around the globe, most businesses are unware of there being such a threat until it happens to them.

Without the internet, most businesses would cease to exist. The virtual world has brought us all much closer in the actual world, but it does not come without risks. There have always been and will always be those waiting to prey on the vulnerable. In the virtual world, that is known as cyber-crime.

IT security professionals play a major role in defending businesses against online threats and cyber-crime, but it is the decision makers who are usually behind on the schedule. This results in companies not paying enough attention to the issue and ultimately lagging on taking effective measure to prevent a disaster.

In recent years, the world has seen some massive data breaches and leaks which have caused irrevocable damage to companies everywhere. Despite seeing widespread coverage, most companies are still of the view that it will never happen to them or that they do not possess any data which may be of value or considered sensitive. That is clearly living in an imaginary world where everything is perfect, right up to the point where it comes falling down.

Essential Information of Modern Cyber Crime

A simple virus infection would have been the clear definition of cyber-crime maybe a decade or so ago. Unfortunately, cyber-crime has evolved into something much darker and criminals have the ability to exploit all loopholes and weaknesses of a company's defense mechanisms.

Businesses usually fail to understand that their own employees are mostly the weakest link when it comes to penetrating a business' firewalls. Organizations invest heavily in securing their systems from external threats, but all it can take is a simple phishing email to get a vulnerable employee to click on a link which could wreak havoc.
This makes training on cyber crime and online security more essential than ever before. Especially those employees who may not have much awareness on the latest IT and online threat developments. It is integral to include material on how other companies have been breached and what needs to be done to keep everyone, especially the company safe from such attacks.

Businesses have been blackmailed, extorted and have had data held for a ransom. These are some scary scenarios, but with the proper training and security protocols in place, the risk can be minimized.

CONSEQUENCES OF BEING HACKED AND WHY PREVENTION IS SO MUCH BETTER THAN CURE

Governments around the world are tightening the rope around corporations to ensure compliance with laws relating to online safety and security of their citizens and consumers. Without these laws, it would be impossible for most consumers to shop and use services of companies online without having their information stolen regularly. These laws are how legitimate businesses have been able to grow and thrive.

Not having enough security measures and protocols in place can mean being easy prey for hackers and losing everything. Any company that is vulnerable or high at risk of being hacked cannot tell until the attack actually happens. Most companies, like individuals, consider themselves immune or invincible till it happens to them.

By being a little too lenient on something as simple and at the same time necessary as cyber security, companies risk things much bigger than just being hacked or having their data leaked. There are numerous consequences associated with being hacked. These include:

Loss of Customers

If a business cannot keep its users safe from external threats, it is correct to assume that most of them will not be return in the future. Following a major hack, companies around the world witnessed a sharp drop in profits and sales. Larger corporations may be able to take the hit for a while, but this could be disastrous for small businesses.

Legal Action and Compensation

It may not entirely be the company's fault, but it definitely will be blamed on them in the case of a cyber-attack. Especially if no precautionary measures were taken and security of online customer data was not protected by legal requirements.

Not only will customers come after such companies for compensation, governments may also slap on massive fines for not complying. Some of the biggest companies have faced fines in the range of billions of dollars by worldwide governments for failing to protect the data of their users. Better to be safe than sorry in this situation.

Reputation Damage

Money may come and go, but rebuilding a reputation is extremely difficult and near impossible for most businesses. Gaining the trust of customers is a big deal for any corporation now and being hacked can spill that down the drain in an instant.

Companies usually end up investing much more in public relations and crisis management instead of previously investing in steering away from the crisis itself. No amount of crisis management will mean complete reputational recovery. This is a dent, sometimes a massive one, which may or may not ever go away.

There is no reason to avoid investing in securing a business' interests online. It just is not worth it. You need to invest in your security before it is too late.

WHAT TO DO IF BUSINESS IS HACKED?

Stories about businesses getting hacked are now becoming less of a breaking news story because of how frequent such incidents have become. There was a time when a major hack would be the most talked about event for months on end. Now, it often seems like a regular occurrence. Instead of taking this lightly, companies need to place their cyber security priorities before everything else.

What if it is too late and a business has already been hacked? What options does it have left? What are the legal requirements that are associated with a business being hacked? The discussion is quite broad and legal repercussion should be discussed with competent legal authorities. Nevertheless, there are some basics which need to be considered in the event of a business being hacked:

Keep Clients Safe by Informing Them

If a business stored information on their customers which can be classified as personally identifiable information (PII), then they need to be informed immediately. Regardless of all data being breached or just some of it, it is advisable and necessary in many instances to send out written notices to users to inform them of what has happened, how they can stay safe and what steps the company is taking to ensure a reversal or as a remedy.

This is usually done by emails informing customers a breach has taken place, to change and secure their passwords, along with guidelines on what is now going to happen. It builds trust and maintains reputation, which doesn't happen if a company stays quiet.

Follow Industry and GDPR Regulations

As of May 2018, businesses are required according to the new General Data Protection Regulations (GDPR) laws to inform relevant supervisory authorities within 72 hours.

This is applicable to companies who have stored information of customers residing in the European Union. If a business fails to report the breach, it may result in a 2% fine of the company turnover or 10 million euros.

That is for GDPR compliancy. Every industry has its own regulations according to the laws of the country it is doing business in as well. It is mandatory to follow those laws and regulations, otherwise a business may be stuck in legal troubles for years to come.

Contingency Plans and Cybersecurity Experts

A cyber security expert, or team of experts, depending on a business' size, need to be called in to assess the situation and the damage done. They will also be able to tell if the network is currently under attack or not and how far hackers have penetrated the system.

They will also be the best ones to advice when contingency plans should come into play, otherwise data backed up and recovered may also fall pray to an active threat

It is always better to stay prepared and practice various scenarios that may occur. This will keep business running smoothly and people aware of what to do and when to do it in the case of there ever being a hacking.

Pioneering Newsbytes

Chrome, Firefox Working on Improving Memory Allocation for Browsers, Memory Demanding Websites

Laptops, tablets and other mobile devices are packed with an increasing amount of RAM and storage memory. Despite the better specs, speeds are slowing down on popular internet browsers such as Google's Chrome and Mozilla's Firefox. This is primarily seen as the browsers themselves becoming memory hogs in order to become an all-in-one system, along with websites too demanding more and more resource allocation.

Luckily, both Google and Mozilla have begun working on this issue and are introducing fixes to ensure that their browsers don't slow down modern devices.
It looks like the race to become the fastest loading browser is on, once again.

HOW TO STAY SECURE IN VOLATILE TIMES

Businesses are more prone to cyber attacks, hacking and online threats now more than ever before. The drastic rise in companies losing it all due to loopholes in their online security has resulted in large scale failures and permanent damage to reputation. Data protection is key for businesses who are looking to make it big and survive in today's tough corporate atmosphere and with the right tools in place, it is completely possible.

The problem is not limited to viruses and malware attacks anymore. Cyber criminals now prefer blackmailing and threatening companies by holding their data for a ransom. A number of companies recently faced that exact same issue and despite paying the hefty ransoms, they still weren't able to get their sensitive data back.

Crime in in the online world is real and just as threatening as in the 'real' world. Cyber criminals are often impossible to track and this can lead to an increase in problems for any business in question.

The good news is that it is possible to stay secure in today's volatile times. Companies do not have to make budget cuts to compensate for the added layers of security since playing it smart and knowing what to do will bring about the same results.

Here are some security tips for businesses who are looking to stay secure and keep their data safe:

Updated Hardware and Software

Using outdated software and even hardware is a big no-no in cyber crime 101. This is just wishing for cyber criminals to attack. If a company is using hardware and software which is now history and hasn't seen an attack happen yet, security experts almost guarantee that it will happen in the very near future. There is just no way to rule out the possibility of it. Luck only lasts so long before it gives out.

Modern hardware and the latest software is a must to keep a business safe from any threats which may arise inside or from the outside.

Backup and Recovery

Even the most secure networks and systems around the world have fallen prey to cyber crime. No matter how much a company invests in its online security, there is never a 100% guarantee. Which is why having regular backups done is essential to making sure that lost data can be recovered at any given moment when needed.

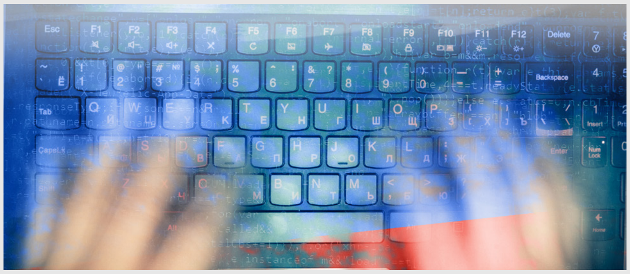
Empower Employees

Uninformed employees are the biggest threat to any organization. Invest in their training, give them the knowledge and tools to empower them to tackle threats online and keep everyone around them safe as well. This is of high importance because the office is wherever an employee goes with an internet connection and access to company networks.

An office is no longer limited to a walled structure and neither should security precautions be.

Pioneering Newsbytes

Russians Deep on American Infrastructure, Old Bluetooth Flaw Exposes Devices and LifeLock Shocks by Exposing Millions



This past month has been extraordinary for tech security as it marked a year since the terrible Equifax data breach which impacted nearly 150 million Americans. That doesn't mean security is tighter than ever. It is believed that Russian hackers are integrated so far deep into the US infrastructure that they are able to cause large-scale blackouts in an instant. Not only that, but a decade-old Bluetooth loophole has left countless devices exposed and no one knew until now. The most ironic development was that LifeLock, a company focusing on keeping identities safe online, had a flaw in their own system which exposed millions of customer email addresses. A flaw, which the company says is now fixed.

PIONEERING
PROGRAMMERS

www.devs4msps.com
www.pioneeringprogrammers.com

1059 S Sherman Street
#140 Richardson, Texas, TX 75081

info@devs4msps.com

☎ 972-895-3100