HIDDEN PROCESS
CyberSecurity Solutions

How to build an effective cybersecurity strategy?

Ensure a safe digital development of your business

I. INTRODUCTION

The entire world is taking the next steps to become fully digitalized and connected and companies are doing their best to keep up with the changes. Therefore, organizations that were typically offline are entering the IoT (Internet of Things) era, where physical and virtual worlds are connected.

**IoT technology = using the internet to connect different devices, services and automated systems and, therefore, creating a network of objects*.

It is undebatable that the IoT era brings important advantages for businesses:

- they gain a greater access to data on their products and internal system. Therefore, they can better understand how customers use their products or services and they can improve the customer experience;
- the collected data may be used to streamline the supply system, as it gives useful insights on the operation of such system;
- the businesses may identify more easily and quickly their popular items or cross selling opportunities;
- the shopping experience is improved by giving the buyer the opportunity to interact with the products in a virtual environment;

These are just a few examples on how IoT may improve an e-commerce business, as the list of the benefits is much longer and complex.

However, together with its advantages, the IoT era also brings more complex security risks and issues generated by the devices connected to each other. Although these risks are not new, they are amplified (as quantity and complexity) by the number of IoT devices. In this regard, statistics show us that in 2016 about 55% of the small and medium companies declared that they have experienced a cyber-attack within the last 12 months of activity, in 2017 it was registered a percentage of 61%, while in 2018 the percentage raised to 67%.

II. THE MOST COMMON CYBERSECURITY RISKS

To better understand the cybersecurity risks faced by e-commerce businesses and the need for cybersecurity strategies, let's dive in and see what security risks involve the most common cybersecurity attacks:

1. DDoS attacks (Disturbed Denial of Service)

DDoS is a technical attack that implies overwhelming a server with traffic from multiple sources (a group of internet connected devices which have been infected to allow remote use maliciously send

requests, packets or data) with the consequence that the server reaches its saturation and start denying the legitimate connections. Therefore, the server slows down or even completely shuts down.

Sales are not possible while the website is offline, therefore, the immediate effect of the DDoS attacks is losing the profit that might have otherwise been realized (usually the losses are much higher during holidays, when the demand is also higher). When the customers have so much options on the internet, it is highly unlikely that they will wait until your website is back online. Also, it should not be overlooked that the DDoS attacks are usually used as diversion for a more malicious attack.

2. Phishing attacks

These are social engineering attacks that seek to steal user data, including login credentials and credit card details by masquerading as a trustworthy entity.

There are several different types of phishing attacks used by cybercriminals to convince the users to perform some type of actions. The most common phishing attack involves sending authentic looking emails about the need to verify the account information, undesirable account changes and more other scams with the goal that the user will click on a link or will access a bogus website where the sensitive information shall be collected.

For the online retail, we would like to draw your attention especially on two types of phishing attacks:

- content injection phishing: implies that the hacker replaces part of the content of a legitimate website (by exploiting a vulnerability) with false content designed to mislead or misdirect the user into giving up sensitive information;
- spear phishing: a targeted form of phishing when the emails are highly customized for specific persons within an organization (CEO, executives, contractors etc.) with the goal to steal data or to install malware on the recipient's computer, to gain access to the target's network and, therefore, capturing credit card information of the customers.

Just a click on a malicious link is enough to cause a security breach.

3. Malware

Malware is any malicious software (program, file, code) especially designed to be harmful to systems.

There are a lot of types of malware, each of them with different functions: viruses, trojan, spyware, worms, ransomware, adware, botnets etc. Despite their diversity, all malware seeks to take control over the device and to interfere with the normal activity. Although they cannot harm the hardware, they usually have the capability to provide remote access for the attacker, to send spam from the infected device, to steal sensitive data or to investigate your computer activity without your knowledge or your permission. As you can see, malware use spam and phishing emails to infect devices.

In the e-commerce world, ransomware requires a special attention. Ransomware is typically a malware that lock down a computer or encrypts the files, threatening to erase everything unless a payment is made (usually the payments are made in bitcoin or other cryptocurrency as it grants anonymity). There are two types of ransomware in circulation:

- encrypting ransomware: it is designed to encrypt the system files and after the payment is made provided the victim with a key which can decrypt the content;
- locker ransomware: it locks the victim out of the operative system, without encrypting the files. The victim has to pay a ransom to gain back the access.

Usually the code behind ransomware is not very advanced (ransomware is based on spam e-mail and social engineering) and it is easy to obtain through online criminal marpketplaces, while defending against it is very difficult.

The ransomware gained a lot of popularity in the last years due to cryptocurrency payment methods. In 2019, the global damage made by ransomware is expected to exceed $ 11.5 billion.

The e-commerce websites are a very tempting target for the cyber criminals because they manage a lot of sensitive data (personal information, credit card details etc.). All the attacks described above as well as many others represent a permanent possibility and threat for the online retail as any software and any e-commerce platform have vulnerabilities that are known or shall be known by the cyber criminals.

4. Man in the middle attack (MITM)

A MITM describes an attack where the attacker places himself between two devices (a web browser and a web server) and intercept the communication.

Depending on the target or the goal, there are many techniques used for MITM attacks. Regarding online retail, SSL hijacking requires a special attention.

SSL hijacking is a web attack based on the principle of computer sessions (the time period the communication between two systems take place). To understand how SSL hijacking is working you have to be aware that when you connect to a website, the computer and the web server go over series of steps: (1) the computer connect to an unsecure server (HTTP); (2) the unsecure server is automatically to the secure version (HTTPS); (3) the computer connects to the HTTPS server; (4) the HTTPS server provides a certificate, proofing positive identification of the website.

In case of an SSL hijacking, the HTTP server is not redirected to the HTTPS version, but the attacker uses another computer and secure the server to intercept all the information passing between the server and the user's computer (including passwords, credit card details and other sensitive data).

III. BUILDING AN EFFECTIVE CYBERSECURITY STRATEGY

With the Internet in the middle of your business' development, there is no better way to secure your digital transformation than having a corresponding cybersecurity strategy

An effective cybersecurity strategy shall be tailored to your particular business and risk profile. Moreover, a security strategy that is aligned with your business strategy shall be able not only to protect your assets, reputation and customers but, ultimately, shall improve your business.

Basically, a cybersecurity strategy should have more steps:

1. **Identify all your sensitive data**

It may seem surprising, but there are very few companies knowing where all their sensitive data is located. You could say that is quite difficult to protect some unknown assets that you do not know where to find, right? Well, many companies invest large amounts of money in standard security solutions, without knowing exactly what their sensitive data is and what security solutions are effective for them.

Therefore, the first step in building your security strategy should always concern (i) what your sensitive data is and (ii) where your sensitive data is located. A security specialist will help you inventorying your data and choosing the proper solutions to protect different types of data and the processes around them (an application that use a certain type of data will also need proper security measures).

2. **Asses the current level of cybersecurity awareness**

Knowing exactly what sensitive data you manage and where it is located leads you to the next step where you can better understand what is the role of your employees in the management and use of the sensitive data and what may be their impact on the organization's security level. Understanding your assets will help you (i) establishing and implementing best practices and (ii) educate and train your employees on these best practices to reduce and prevent breaches that target insiders, such as phishing.

With regard to potential insider threats, a special attention should be also pay to acquiring and installing devices. Using a product that offers secure boot ensures that no one has tampered with the code between manufacturing and deployment. In the unlikely event that someone alters the device firmware with malware, the device simply won't start up, because overall signed firmware hash and the hashes in the firmware are altered.

A strong security strategy should be reflected in all aspects of your business

3. Perform a classification of your data

Not all data is equally valuable. A classification of the data according to its importance for the organization and its impact on the security level is essential for a correct allocation of resources to the most important data that needs protection.

All the efforts for identifying the location of your data shall be worthless if you will use your resource to equally protect your assets. The reality is that for some assets less protection measures shall be necessary than for others. Therefore, an equal allocation of your resources shall not offer you sufficiently strong protection measures, leaving some of your assets exposed to vulnerabilities.

Moreover, within the complexity of the IoT world, we can only accept that security vulnerabilities cannot be reduce to zero. The security specialist will help you find the most efficient way to allocate your resources.

Instead, you may establish a level of acceptable risks to be your target. In this way, you will not waste your resources on vulnerabilities without a considerable level of risk and you should be able to track your evolution in securing your business.

4. Understand the real risk exposure

The heart of a cybersecurity strategy is an efficient combination between penetration tests and vulnerability assessments. The vulnerability assessment shall identify, analyze and prioritize your website/ecommerce platform existing vulnerabilities. A vulnerability assessment may be seen as a risk management process because it evaluates the existing cybersecurity level. In addition, the penetration tests simulate cyber-attacks to identify and exploit the hidden vulnerabilities and to provide complete information about vulnerabilities and their risks.

As every business has a different approach, there is no such thing as standard penetration test or automated assessment. A good penetration tester shall assess your business' specific functioning and shall design an appropriate penetration test, in accordance with the identified characteristics (by the vulnerability assessment).

The results of the performed tests and assessments should be accessible for both technical and nontechnical teams

---

In order to be able to scratch from zero your cybersecurity strategy is essential that the information provided by your security specialist to be accessible and understandable not only for your IT team, but also for your management team so they can understand the risk exposure, the impact of the employees actions, the specific risks raised by your business and to be able to implement and supervise security best practices.

5. **Routine = safety**

Cybersecurity is closely linked to the dynamic of your online business. Any change or growth in your business' activity shall be reflected in your cybersecurity status. Unexpected increase of visitors/buyers, marketing campaigns, changes/additions in the website's functions, software updates, changes within your team, development of new technologies, publishing new vulnerabilities found by hackers, all of them may generate new threats and vulnerabilities for your online business.

Such a dynamic character may be only controlled by a well-developed routine. Therefore, running routine penetration tests shall help you increase the visibility over your security weaknesses and test the effectiveness of already implemented security measures.

6. **Reaction plan**

Cybersecurity is not anymore a problem of "if", but a problem of "when". Therefore, an incident response plan will help you to identify, minimize and reduce the costs of a cyber-attack. A security breach brings high-pressure situations, so a prior plan which indicate the members of the incident response team, whom they have to communicate (other members of the organization, legal counsels, press etc.) and quick steps to be taken when the incident occurs, will make the situation easier for everybody and the incident shall be eradicated faster.

A cybersecurity incident response plan should contain some essential chapters:

a. Scope, terminology, security characteristics of the business: prioritize of security issues, the most sensitive assets, the most probably security incidents (found out by a vulnerability assessment);
b. roles and responsibilities of every member of the team: coordinator, incident response handler, insider threats, users, etc.;
c. incident response phases: preparation, detection, containment, investigation, remediation, recovery;
d. full documentation regarding the incident - within several weeks after the incident, a fully analyze of the attack is required to assess the successful and effectiveness of the incident response plan. Based on the conclusions, the plan may be adjusted for future situations.

Building an effective cybersecurity strategy is not only about having a proactive approach, but, in the today IoT era, is the best solution for a sustainable growth of an online business.

If you need any assistance in building the proper cybersecurity strategy for your online business or any help regarding cybersecurity, do not hesitate to contact us at 004 0754 558 977 or email us at contact@hidden-process.com.