# Protecting Your E-Commerce Business. Analysis on Cyber Security Threats

**Georgiana ANDREIANU**
Faculty of Electronics, Telecommunications, and Information Technology,
University POLITEHNICA of Bucharest, Romania
georgiana.andreianu@stud.etti.upb.ro

**Abstract**

*This paper aims to gather complete information needed for a retailer running an e-commerce website, with the intention of presenting some of the most common cyber security threats, such as malware, ransomware, SQL injection, and phishing, as well as ways to prevent them from happening and ways to manage the aftermath of a full-scale attack being carried out. Some best practices will be noted as a process that should always be considered when setting up an e-commerce business, and a risk management strategy will be outlined. An analysis will be performed on a data breach with one of the biggest number of victims in the last decade, which affected the Microsoft Exchange Servers.*

**Index terms:** attack, cyber security, e-commerce, threat, vulnerability

## 1. Introduction

Over the last decade, the e-commerce industry has exponentially grown, especially during the time of Covid and the popularization of remote work. Going online to shop at your favorite store has never been easier. For the retailers, this is a true blessing, providing immense business opportunities from small scale retailers and service providers to whole large-scale industries. A high sales volume can be achieved much easier with the help of aggressive online marketing and the cost decrease of not having to rent a physical location. However, at the same time, it is a burden regarding the high risk of cyber security threats that e-commerce websites have.

With the evolution of websites and mobile applications, cyber-attacks have become more complex and more frequent in the past years. As we can see in figure 1, businesses have fallen victim to an average of 340 million attacks every year for the last seven years, according to data provided by [1]. Given the growth of online presence ever since the start of the pandemic, we can see a spike in the number of attacks since the year 2020, with the highest number of attacks being in 2021. Every e-commerce business is a hot target for cyber-crime, considering the amount of personal data and financial information that it collects. The attacks range from ones directed at the customer, such as phishing and malware to attacks that are directed more towards the server and website, such as SQL injection and Cross Site Scripting. A weakness of this kind that results in a breach can greatly affect both the customer and the business, in terms of cost of revenue and of customer trust.

For an e-commerce business to be successful, important cyber security aspects must be adhered to and respected. Defending against cyber security threats has become a job for strong electronic security, rather than exclusive human foresight and conservation. Furthermore, it is very important to have a strict protocol for risk management in the event of a breach that can affect both the customer and the business.

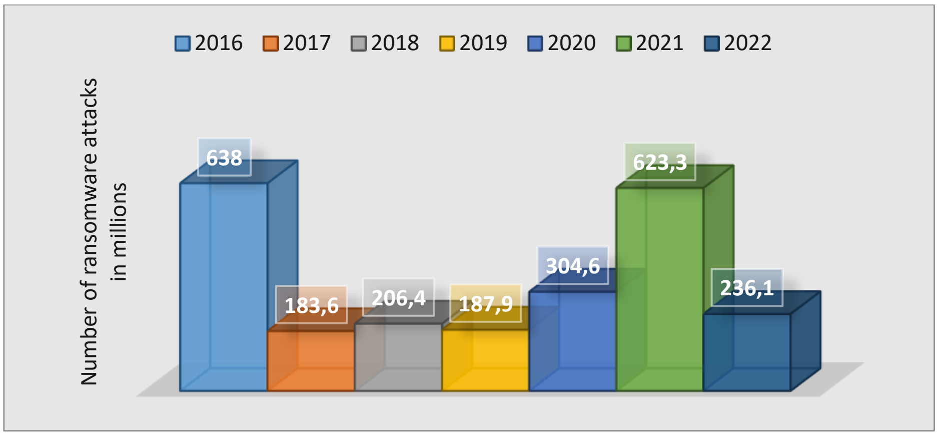

**Fig. 1.** Number of ransomware attacks in millions in the last 7 years

## 2. E-commerce Security

Electronic commerce is the business of buying, selling, or trading of goods or services using the internet as a means of communicating between the provider and the beneficiary. In other words, E-commerce is a transaction activity based on the media of information network. All business activities realized through, relying on, based on, or with the help of information network can be included in the category of electronic commerce [2].

In terms of engineering, e-commerce is a large system consisting of platform operators, providers, network consumers, suppliers, manufacturers, distributors, retailers, and many other groups collectively working together. Since e-commerce success as an industry depends on a system of entities, its security should also be based on the security of the whole system. The aim is to create a dynamic balance between all the components.

Cyber security protects computer systems from information disclosure, misdirection, damage, or theft of electronic data, software, or hardware [3]. In e-commerce, the main goal is to have a secure electronic behavior related to e-commerce activity. Even though businesses continuously invest in technologies to prepare against cyber threats, hackers are developing more and more complex ways to gain access to business systems and data, using cyber-attacks of different approaches and complexities, which will be reviewed in the following subchapters.

### 2.1. Phishing

Phishing is a type of social engineering and refers to methods used by attackers to trick victims - typically via email, text, or phone - into providing private information like passwords, account numbers, social security numbers, and more [4]. An attacker may try to send an email which seems to come from a reputable source, asking for information. This is an attempt at gathering personal and financial information about a person and using it in a malicious way. Websites are prone to becoming a casualty of this cyber security threat, with about 70% of the companies worldwide falling victims to phishing in 2020 [5].

### 2.2. Malware and Ransomware

Malware, or malicious software, is the most common cause of cyber-attacks. This software is programmed to handle control on your computer, and anything on it or entered into it, over to the cyber criminals without you even knowing it [6]. Malware is designed specifically for damaging, interrupting and obtaining unauthorized access to a system, while locking you out of your computer and denying you access to all important data.

Ransomware is a specific type of malware where the attacker holds access to sensitive files until the victim pays for them to be released. Both malware and ransomware are great threats to a business, as it can cause inconveniences for the retailers, the employees, and the customers, all while having expensive costs for removing.

### 2.3. SQL Injection

Another important aspect of security is protecting databases. They can be put at risk by attacks such as SQL Injection, a method of cyber-attack where attackers insert malicious SQL commands into the forms or input fields of a web application to access or modify database information without authorization. This type of attack can have serious consequences, such as exposing sensitive data, losing, or altering data and even taking control of the system.

There are a wide range of vulnerabilities, attacks and SQL injection techniques that occur in different situations. Some common examples include obtaining hidden data, where a SQL query can be modified to return additional results; subverting application logic, where a query can be changed to interfere with application logic; database examination, where information about the version and structure of the database can be extracted.

### 2.4. Cross Site Scripting

Cross Site Scripting, or XSS, implicates inserting a malicious code, most commonly JavaScript, into a webpage. Basically, an attacker injects malicious executable scripts into the code of a trusted application or website by sending a malicious link to a user, who then accesses that link. An attacker can use XSS to send that malicious script to an unsuspecting user. The end user's browser has no way of knowing that the script is not to be trusted and will execute it. Because it believes the script comes from a trusted source, the malicious script can access any cookies, session tokens or other sensitive information kept by the browser and used with that site. These scripts can even rewrite the content of the HTML page. In this instance of a threat, the website itself is not in any danger, but the customers are at risk of being exposed to phishing, malware and other kinds of cyber security risks.

### 2.5. E-skimming

E-skimming is a method of stealing credit card information and personal data from payment processors on e-commerce sites. In this attack, hackers gain access to checkout pages and capture payment information as customers type it in real time [7]. The collected information is sent to an Internet-connected server with a domain that is controlled by the attacker, who will either sell the payment data or use it to make fraudulent purchases. E-skimming can result from XSS, phishing, brute force attacks or third-party compromise.

### 2.6. Brute Force Attacks

A brute force attack is a password-based attack where the cyber-criminal uses cracking tools to try all possible combinations of passwords to uncover valid passwords [8]. The aim of this attack is to duplicate a valid password for the online store’s administrator and gain otherwise unauthorized access. Another password-based attack is a dictionary attack, which aims for the same result, but instead of using scripts, the attacker manually tries all possible combinations of letters and numbers to guess the password. Given the time and labor required for the latter, a brute force attack is the more common approach.

## 3. Best Practices for Implementing Cyber-Security

Authentication and authorization are essential parts of basic security processes and are vital concepts that e-commerce business administrators should use to protect users' systems, information, and personal data. Although the two terms seem similar, they have different and necessary roles that, when combined, determine the security of the entire platform.

Authentication verifies the identity of a user or service. This is necessary to protect and secure access to the website, its data and all its content. For example, when we need to access a website or online service, we usually need to enter our username and password. Then, behind the scenes, it compares the username and password we entered with a record it has in its database. If the information entered matches, the system assumes we are a valid user and we are granted access.

Once the user's identity has been verified through authentication, it is up to the authorizer to determine the user's access rights. In other words, authorisation is the security process that determines the level of access a user or service has. As an example, we can think of ourselves as being employed in the marketing department of a company that uses an internal web application to store and process data. After successfully logging in, the content on the page must be specific to the department we belong to, without having access to the information of the accounting or human resources department, for example, for which we are not authorised.

In order to ensure these two processes, some simple, but at the same time crucial aspects of web application security must be ensured and checked. Authentication can be put at risk by attacks such as brute force attacks. Because of this, strict policies have been put in place and are being followed by more and more companies, such as fixed forms for passwords that can be used (a password must contain a minimum of 8 characters, a capital letter, a digit, and a special character).

Also, a good practice for maintaining authentication is to formulate the alert that appears when a wrong email or password is entered in such a way that it is not disclosed whether the email or username used exists in the system, so as not to provide an opportunity to gather information about web application users. If multiple unsuccessful login attempts have been made to an account, it should be automatically locked for a period of several minutes to provide protection against brute force attacks.

Another best practice that is progressively being adopted with web application development is the integration of two-factor authentication, called 2FA for short, which requires two different authentication methods. Using this method, a user is granted access to a website only after demonstrating two or more pieces of confirmation to an authentication mechanism: knowledge, such as knowing the account username and password; possession, such as an access card to an office building; and inherence, such as a fingerprint.

To ensure effective authorisation, it must be verified that each user has access only to data specific to the group to which they belong. Authorisation can be bypassed by simple actions such as adding a group- or user-specific extension in the access link to a web application (e.g., www.cybercon.ro/admin). If that page opens and the information is visible, this is considered a security vulnerability.

To ensure customer trust it is crucial to offer total transparency over personal data policies and ways of enforcing them. With the expanding demand for personal data handling by every website, customers are getting increasingly distrustful over how their information is stored and shared. Demonstrating transparency by giving details on the privacy policy that is used reassures customers that their information will be safeguarded and will lay a good base for customer trust and loyalty.

Cyber security threats such as phishing, malware and ransomware are often directed towards customers or employees, so a good way of protecting against this sort of attacks is having regular trainings with the employees about the dangers and effects, both on the company, and especially on the individual.

## 4. Risk Management

Cybersecurity risk management is an ongoing process of identifying, analyzing, evaluating, and addressing your organization’s cybersecurity threats [9]. The job of risk management involves everyone in the organization. For this, key actions must be considered, such as: developing robust policies and tools to assess merchant risk; mitigation of IT risks, possibly through training programs, as mentioned before, or new policies; identification of internal weaknesses such as lack of 2FA; testing of the overall security process; documentation of merchant risk management and security; identifying emergent risks, like new regulations with business impact.

Generally, the strategy for managing risks involves following a four-step process which helps organizations have a better grasp and control over cyber security threats. The process commences with identifying the risks and assessing them based on potential impact and the possibility of attackers exploiting present vulnerabilities. After the analysis is completed, risks are prioritized based on each company's preferred mitigation strategy. The final step is monitoring risks, which concentrates on controlling the response, even in a constantly changing environment. This process can help e-commerce businesses to develop and adopt a cyber-security risk management plan.

Software approaches that should be used to protect against cyber-crime involve using cyber-security tools such as firewalls, encryption software, digital certificates, digital signatures, public key infrastructure and a strong password policy. Data plays an important role in any e-commerce business, so the best path to ensure data integrity is to use hashing and perform regular data back-ups, which will establish data availability and integrity in the event of a breach.

Organizations should follow the appropriate standards and frameworks for certifying a safe and secure online shopping experience. Some of the most important ones that also offer best practices and requirements for cyber risk management are ISO/IEC 27001:2022 and NIST Cybersecurity Framework Version 1.1.

**Table 1.** Cyber risk management according to standards and regulations [10][11]

| Standard | Risk management strategy |
|---|---|
| **ISO/IEC 27001:2022** | Establishing and maintaining information security risk criteria |
| | Ensuring that repeated risk assessments produce consistent, valid and comparable results |
| | Identifying risks associated with the loss of confidentiality, integrity and availability for information withing the scope of the information security management system |
| | Identifying the owners of those risks |
| | Analyzing and evaluating information security risks according to the criteria established earlier |
| **NIST Cybersecurity Framework Version 1.1** | Identifying and documenting asset vulnerabilities |
| | Tuning into the latest cyber threat intelligence from information-sharing forums |
| | Identifying and documenting threats, both internal and external |
| | Identifying the potential business impacts and likelihood of risk events, utilize threats, vulnerabilities, likelihood, and impacts to determine risk |
| | Identifying and prioritizing risk responses |

## 5. Effects of a Full-Scale Cyber-Attack

In January 2021, an attack with one of the largest number of victims happened on the Microsoft Exchange Servers, one of the largest email servers in the world, affecting over 60.000 businesses, companies, and organizations worldwide. The attackers took advantage of four security vulnerabilities that were not known to the provider, called zero-day vulnerabilities, which can be seen in figure 2, explained by Microsoft in [12]. Thus, they were able to gain unauthorized access to user emails, passwords, and administrator privileges to small businesses and even US governments.

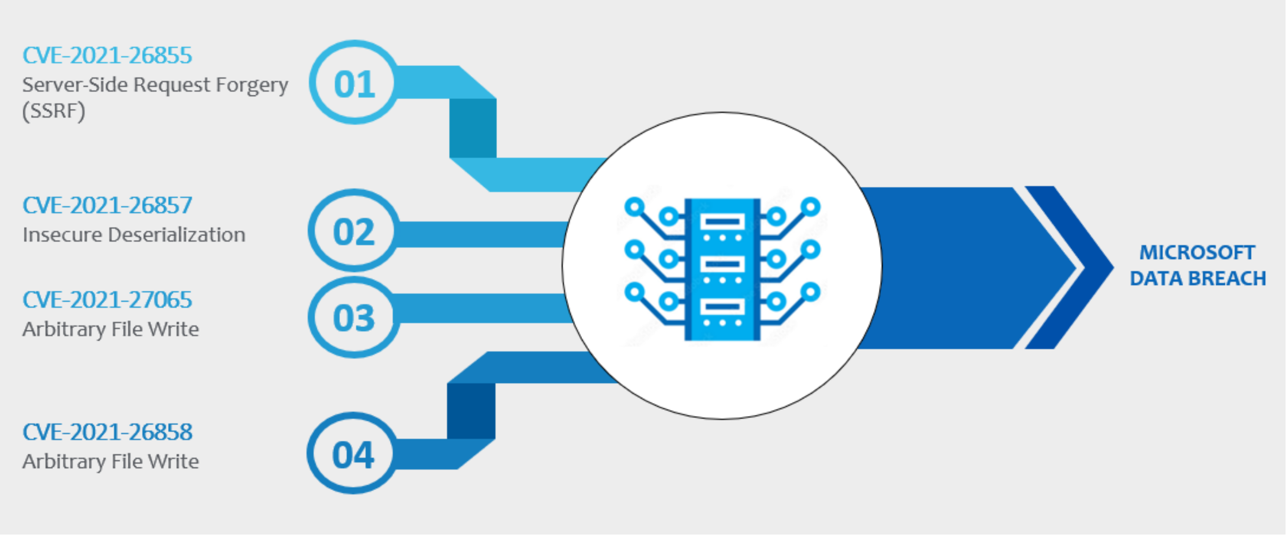

**Fig. 2.** Zero-day vulnerabilities exploited in the 2021 Microsoft data breach

The first of the zero-day vulnerabilities allowed attackers to connect to a server by creating session IDs and access tokens, to then authenticate as a standard user without actually owning those privileges. Afterward, a second vulnerability was exploited which gave administrator rights to the falsely authenticated user, when the last two unknown security weaknesses allowed attackers to upload code to the server in any location, using the administrator privileges.

The operation required three months in which the cyber-criminals carefully searched for coding errors which would allow them to gain control of the vulnerable systems. They then broke into each company's email server with only a connection to the internet and a locally managed system. The next step was to install malware, a web shell that provided a backdoor to the compromised servers, to access other systems and fundamentally take over the whole server.

The cyber-criminals used the web shell to run commands remotely and gather information such as passwords and email addresses, which was possible because Microsoft Exchanges doesn't use encryption to store them in memory. They also added users, added additional backdoors to other vulnerable systems and installed ransomware.

Since the hackers were able to access organizations' systems, the requests appeared to be coming from the MES, so Microsoft could not detect the malicious code and approved it. Eventually, they discovered the vulnerabilities and patched them. Microsoft released a total of 24 security updates for MES 2013, 2016, and 2019. Table 2 shows a timeline of the revisions performed on the servers.

**Table 2.** Microsoft Released Security Updates Timeline [13]

| Version | Date released | Details |
|---|---|---|
| 1.1 | 2 March 2021 | CVSS scores were updated for the affected products |
| 1.0 | 2 March 2021 | Information was published |
| 2.0 | 8 March 2021 | Security updates for CVE-2021-27065, CVE-2021-26855, CVE-2021-26857, and CVE-2021-26858 for several Cumulative Updates that are out of support, including Exchange Server 2019 CU 6, CU 5, and CU 4 and Exchange Server 2016 CU 16, CU 15, and CU14 |
| 3.0 | 10 March 2021 | Security updates for CVE-2021-27065, CVE-2021-26855, CVE-2021-26857, and CVE-2021-26858 for several Cumulative Updates that are out of support, including Exchange Server 2019 CU 3; and Exchange Server 2016 CU 17, CU 13, CU12; and Exchange Server 2013 CU 22, CU 21 |
| 4.0 | 11 March 2021 | Final set of security updates for CVE-2021-27065, CVE-2021-26855, CVE-2021-26857, and CVE-2021-26858 for several Cumulative Updates that are out of support, including Exchange Server 2019, CU1 and CU2; and Exchange Server 2016 CU 8, CU 9, CU10, and CU11 |

| Version | Date released | Details |
|---|---|---|
| 5.0 | 16 March 2021 | Security update for CVE-2021-27065, CVE-2021-26855, CVE-2021-26857, and CVE-2021-26858 for Microsoft Exchange Server 2013 Service Pack 1 |

Even if Microsoft released security updates for the vulnerabilities, the companies and organizations that were using the servers were still susceptible to attacks until they upgraded their systems as well, otherwise hackers would have still been able to exploit the CVEs. This would not have been necessary if the systems used a cloud-native infrastructure, because Microsoft could provide automated security by pushing the patch and immediately fix the issues.

As we've seen, no entity is completely safe against cyber-security threats and there is no definite template to keep hackers away, but it may be worth to consider using solutions that engage security into your development pipeline from the first release, rather than struggling to push patches after data has already been breached.

## 6. Conclusions

E-commerce is a flourishing industry, and it is set to only develop more over time. To establish a successful business, one needs to take into consideration all of the threats, vulnerabilities and risks, which is a harder job than ever seeing the on-going evolution of technology today.

This paper is a starting point in studying the cyber-security of the e-commerce industry. An analysis of cyber-security threats for e-commerce businesses was conducted, revealing the most common vulnerabilities and attacks that pose a risk for the business. The results were documented and explained for every person that may be interested in developing a successful and safe shopping experience for customers. For this purpose, best practices were underlined, and a risk management strategy was proposed.

The most common cyber threats include phishing, malware and ransomware, SQL injection, XSS, e-skimming. The best approach for protecting an e-commerce business is to set and apply a set of best practices which consist of using encryption software, firewalls, 2-factor authentication, password policy, transparency about data policy, tools to ensure data integrity and availability, and using cloud infrastructure to provide automated security. Important factors to consider for a safe environment for customers are authentication and authorization, which set the basis for effective cyber-security.

Future developments should contain exploring vulnerabilities represented by the vendor's implemented software, such as PHP version, databases, web servers or other such components. Other vulnerabilities might be represented by physical attacks or employee error (accidentally sharing sensitive business information).

In light of the constant evolution of software technology and cybersecurity, cyber criminals are becoming progressively more able to tackle complex web applications, with the use of hacking tools and online available documentation. Thus, vendors, retailers, providers, merchandisers, and any person aspiring to become a part of the e-commerce industry must be prepared for the most common cyber threats and have a well-established risk management strategy.

## References

[1]. M. Mclean, 2023 Must-Know Cyber Attack Statistics and Trends, 2023, Available online at: https://www.embroker.com/blog/cyber-attack-statistics/. Accessed on 14.03.2023.

[2]. R. Zhang, L. Fang, X. He, C. Wei, E-commerce and E-commerce Security, in The Whole Process of E-commerce Security Management System: Design and Implementation, Singapore, 2023, pp 1-4.

[3]. Schatz, D., Bashroush, R., and Wall, J. (2017). Towards a more representative definition of cyber security. J. Digit. Forensics Secure. Law 12, 1558–7215.

[4]. BigCommerce, „What You Need to Know About Securing Your Ecommerce Site Against Cyber Threats", 2020 [Online]. Available online at: https://www.bigcommerce.com/articles/ecommerce/ecommerce-website-security/. Accessed on 05.03.2023.

[5]. Galov, N. (2022). 17+ sinister social engineering statistics for 2022. Available online at: https://webtribunal.net/blog/social-engineering-statistics/#gref. Accessed on 10.03.2023.

[6]. CH. Sireesha, V. Sowjanya, Dr K. Venkataramana, „Cyber security in E-commerce" in International Journal of Scientific & Engineering Research, 2017, pp 187-193.

[7]. Adobe Experience Cloud Blog, "Ecommerce security - what it means, common threats, and modern best practices". Available online at: https://business.adobe.com/blog/basics/learn-about-ecommerce-security#:~:text=Ecommerce%20security%20is%20a%20set, need%20to%20defend%20against%20cyberattacks. Accessed on 10.03.2023.

[8]. M. Abomhara, G. M. Køien, „Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks" in Journal of Cyber Security, 2015, pp 65-88.

[9]. Hyperproof, "Cybersecurity Risk Management: Frameworks, Plans, & Best Practices", 2023. Available online at: https://hyperproof.io/resource/cybersecurity-risk-management -process/#:~:text=and%20manage%20risk.-,What%20is%20Cybersecurity%20Risk%20 Management%3F,has%20a%20role%20to%20play. Accessed on 13.03.2023.

[10]. Information security, cybersecurity and privacy protection — Information security management systems - Requirements, International Standard ISO/IEC 27001; Geneva, 2022. Available online at http://www.itref.ir/uploads/editor/2ef522.pdf. Accessed on 13.03.2023.

[11]. Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, 2016. Available online at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Accessed on 13.03.2023.

[12]. Microsoft, Security Update Guide, 2023, Available online at: https://msrc.microsoft.com/update-guide/vulnerability. Accessed on 15.03.2023.

[13]. Microsoft, Microsoft Exchange Server Remote Code Execution Vulnerability, 2021. Available online at: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855. Accessed on 15.03.2023.