# Report

# Risk Assessment of Cybersecurity

## Table of Contents

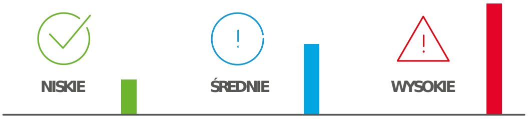
Overall Cyber Risk Assessment............................2
Detected risks.....................................................3
Security Recommendations................................4
Cyber threats and their effects...........................6

Generated on 02/09/2020.

# Overall Cyber Risk Assessment

3/5

| | |
|---|---|
| URL: | http://example.com |
| Tested on: | 02/09/2020 14:03 |
| IP of server: | 93.184.216.34 |
| Location: | United States |



| | | |
|---|---|---|
| Security risk: | ● ● ○ ○ ○ | 22 |
| Reputational risk: | ● ● ○ ○ ○ | 33 |
| Attractiveness to hackers | ● ● ● ● ● | 100 |

The use of computer systems significantly increases the vulnerability of companies to cyber threats and data breaches. Unplanned computer and IT infrastructure outages caused by e.g. malware or hacker attacks often result in losses that can lead even to to bankruptcy of the company.

The **Cyber Report** is a dedicated cyber risk assessment report. You will find the rating in it as likelihood of risk factors that may have a negative impact on your business, which is an important element in any organization's risk minimization strategy.

We present the results of safety tests on the basis of non-invasive compliance checks on the basis of publicly available information carried out by web robots.

## What does my rating mean?

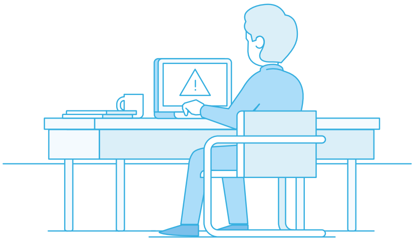
**Your website's cyber risk is relatively high. Take care of the security of your website.**

## What are the steps to take?

**We recommend passing the report on to IT specialists** to read the document on detected threats and **follow the recommendations for their elimination.**

## What does the report show?

- ✓ **Cybersecurity risk** assessed **in the range from 0 to 5.**
- ✓ **The higher the score, the worse the safety score.**
- ✓ **The final risk score has been calculated based on detected safety threats.** Details can be found later in the report.



# Detected risks

## Website security threats

● ● ○ ○ ○ **22**

The risk is based on the current misconfigured website security that could lead to potential hacks.

**Software Composition**

The risk of exploitation of vulnerabilities in website components

✓ LOW

**Traffic encryption**

The risk of taking over sensitive data

✓ LOW

**Website performance**

The risk of downtime in the operation of the application

! MEDIUM

**HTTP and CSP headers**

The risk of exploiting cross-site gaps

⚠ HIGH

**Network security**

The hacking risk posed by an inadequate level of network security

✓ LOW

**PCI DSS Compliance**

The risk of non-compliance with the main requirements of the PCI DSS

✓ LOW

**GDPR Compliance**

The risk of non-compliance with the main requirements of the GDPR

✓ LOW

**Email Security**

The risk of misconfiguring the e-mail server

✓ LOW

**Subdomains security**

The risk arising from multiple exposures

! MEDIUM

## Reputational risk

● ● ○ ○ ○ **33**

Reputation risk is mainly related to brand exposure during periods of high traffic. This means that data on the website can be changed by a third party.

**IP and Domain reputation**

The risk of blacklisting the site from major search engines

⚠ HIGH

**Current state**

Risk of malware infection

✓ LOW

**Mail server reputation**

The risk of ignoring e-mails by popular spam filters

✓ LOW

## Attractiveness to hackers

● ● ● ● ● **100**

Various aspects of your online presence that make it more attractive to hackers.

**Industry Attractiveness**

A risk factor for a specific industry

⚠ HIGH

**Hacker chattery**

Mention of a company in the Darknet, a hidden network used by hackers

⚠ HIGH

**Potential phishing**

Users who do not suspect that fraud may redirect them to a malicious copy of the official website, so they will unconsiously enter their personal data and pass it to hackers.

⚠ HIGH

**Information leaks**

Potential visibility of confidential data on the internet

⚠ HIGH

# Security Recommendations

## Tips on how to improve website security

**HTTP and CSP headers**

The listed HTTP headers must be secured with the appropriate values. It is recommended that you follow the standards of the OWASP or Firefox security headers
Misconfigurations found HTTP - 8: x-xss-protection, feature-policy, x-content-type-options, access-control-allow-origin, etc CSP - 1: Header is missing

## Attractiveness to hackers

**Industry attractiveness**

It is recommended to take or improve cybersecurity measures to protect your website from hackers

**Hacker chattery**

There is a possibility of a website hacking. It is recommended to take or improve cyber security measures to protect the site from hackers
Number of mentions in the dark web: 20

**Potential phishing**

Notify your customers and customers about 'similar' domains, about the possibility of phishing attacks
Domains containing typos:7

**Information leaks**

Ask your employees and customers to follow password security standards: set strong and long passwords, change passwords every month, etc.
Number of leaks found: 50

## Wordpress security

**Misconfiguration risks**

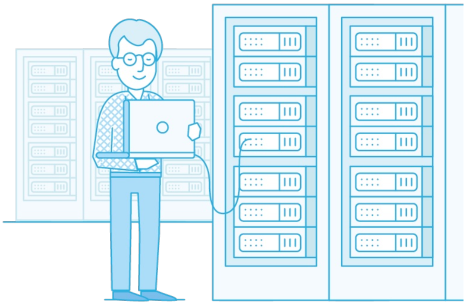
Disable xmlrpc. Also, potential XSS vulnerability is found, contact WebTotem to solve the issue.
Malicious method - RPC_Pingback_API; Classic 1.5 - PHP_SELF XSS (Latest Version: 1.6)

# Security Recommendations

## Concerns about potential attacks

⚠ **Domains containing typos,** which may impersonate the official website and allow the theft of customer data and decrease in the company's turnover

| FOUND 7 DOMAINS | IP SERVERS |
|---|---|
| eample.com | 69.172.201.153 |
| exmple.com | 67.210.233.131 |
| examle.com | 104.200.23.95, 104.200.22.130 |
| exaple.com | 54.72.11.253 |
| exampe.com | 72.52.179.174 |
| xample.com | 209.126.123.13 |
| exampl.com | 45.33.23.183, 96.126.123.244, 45.56.79.23, 45.33.2.79, 198.58.118.167, 45.79.19.196 |



# General Wordpress Security Recommendations

## Tips on how to improve Wordpress security

Update WordPress core
The best way to keep WordPress core secure is to enable automatic updates. This way, you don't have to check for updates every time.

Disable WordPress API
There are some issues with the REST API, most notably the fact that the REST API can actually bypass the WordPress authentication system, including two-factor authentication. It is recommended to completely disable the WordPress API, this can be done using the plugin - Disable REST API.

Add two-factor Authentication
Add two-factor authentication using Two Factor or Google Authenticator. WordPress doesn't offer two-factor authentication by default. When you connect to the back-end management interface, all you need is a username or email address and a strong password.

Move the WordPress login URL
Another way to make your WordPress site more secure is to change your login page. Everyone knows that to enter a website, just add / wp-admin to the end of the URL.

Remove redundant WordPress themes/plugins
Remove any unused WordPress themes and plugins. Please note that unused or inactive themes and plugins pose a serious threat to your WordPress website. Hence, it is imperative that all plugins and themes that are not in use are removed immediately.

Enable reCAPTCHA
Enable reCAPTCHA on forms to prevent spam. “One of the quickest and easiest WordPress security tips for online forms is to enable reCATPCHA for them.

Update plugins and themes
Updating your WordPress plugins is very similar to updating the WordPress core. Most often vulnerabilities are found in outdated versions of plugins, they must be manually updated in the appropriate WordPress dashboard.

Disable XML-RPC
XML-RPC is a special WordPress feature that enables remote access and posting. This functionality can be a security issue as it creates another way for an attacker to gain access to your site. If you do not need this function, you should disable XML-RPC, this is done using the Disable XML-RPC plugin.

Install WordPress backup solution
Backups are the first defense against any attack on WordPress sites. This can be easily done with plugins like VaultPress or UpdraftPlus.

Add contributor or editor account
Publish content using a contributor or editor account instead of an administrator account.

Use vulnerability scanners
Implement a web application vulnerability scanner. Web application vulnerability scanners look for weak spots in your web applications so they can be fixed before hackers can exploit them.

# Cyber threats and their effects

### Malicious software (malware)

Malware is a variety of malicious programs that attempt to infect your computer or mobile device. Hackers use them for various purposes - stealing personal information, passwords and money, and blocking access to devices.

**Particularly troublesome include:**

- computer viruses - malicious programs or codes that infect programs and files by copying themselves,
- ransomware - a ransomware program. When run on the device, it encrypts the data and prompts you to pay for data recovery. However, even paying the ransom does not guarantee data return. Some ransomware can also encrypt network drives and cloud data.

**Example:** A store employee entered an infected website from which he downloaded the file and opened it. The next day, warehouse orders and cash registers started malfunctioning, and a network failure stopped sales. Some files have been encrypted by ransomware.

### Phishing

It consists in impersonating others in order to steal data from the victim, most often access information, e.g. login and password to company systems, or to persuade them to take certain actions. Scammers often send an email that pretends to be a message from an authentic institution or person and trick you into opening an infected file or website.

**Example:** An employee received a message allegedly from the IT department asking him to log into the new e-mail access page. Not paying attention to the content of the message, he clicked on the link and entered his data. As a result, the hacker gained access to the employee's mailbox, which contained confidential customer data. The hacker threatened to sell this data online and demanded a ransom.

### Access blocking attack (DoS and DDoS attack)

Massive attack on a computer system or network service, which consists in sending a large number of orders (attempts to connect to the system, operations). Its purpose is to block the operation of the company's system by seizing all free resources.

The access blocking attack comes from a single source or from multiple sources, such as zombie devices previously infected with malware and controlled by the hacker.

**Example:** Hackers launched a DDoS attack on the florist's servers. Within a minute, they sent out a million requests to view a website where flowers are being ordered. As a result of the attack, the florist was unable to sell for a week, which resulted in a significant loss of her income.

### Data breach, e.g. theft, data leakage, loss of documents

This is, for example, a situation where an employee accidentally sends an e-mail with a visible full list of recipient addresses, medical records of clinic patients are lost, a dishonest employee steals the financial data of your company's clients or hackers steal customer data from your database.

**Example:** A dishonest employee stole over 700 personal data of customers, including names, addresses and contact details, PESEL numbers. It turned out that the data was transferred to a new employer. Since this is an event that results in a breach of the GDPR, the notification had to be forwarded to the President of the Data Protection Office and the data subjects concerned.

### What could be the consequences of cyber incidents?

- Lock, failure or shutdown of computers and other company devices.
- Slowdown or blockage of the company's computer network.
- Theft and sale of sensitive enterprise data.
- Data encryption and ransom demand for recovery.
- Gaining access by third parties to classified company documents.
- Loss of customer, employee and contractor data.
- Business interruption (business downtime) and associated loss of income.
- Damage to the company's reputation.