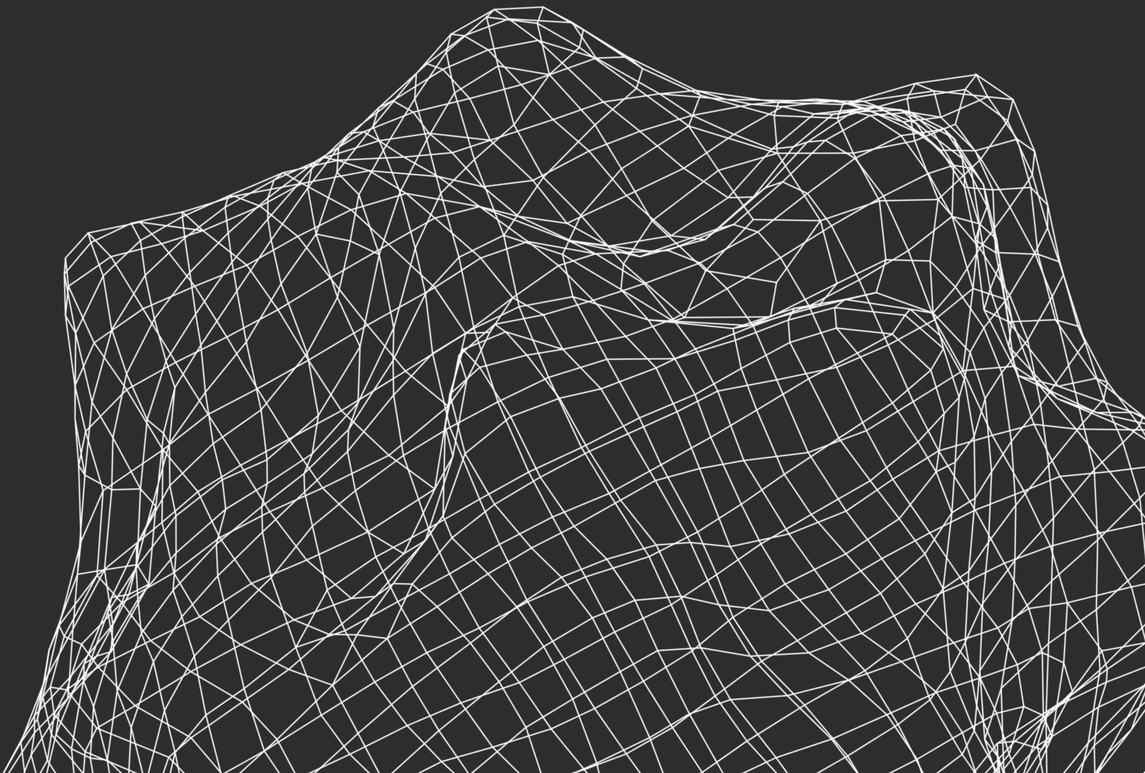
SAFEDNS

Business

Protecting Business from Ransomware



What Ransomware Is

An extortion or blackmail program is a type of malware designed to extort money. It blocks access to a computer system or prevents reading data stored in it and then demands ransom from a victim in order to restore everything to the original state.

Whether the data will be restored successfully after the ransom has been paid depends on how honest the hacker group that attacks the company is. However, there have been cases when a group simply made off with the victim's money and ransomware corrupted the information so badly that its subsequent restoration was impossible.

Cases of Major Companies Hacked

Cases of companies that suffered from hacks using ransomware have been widely talked about in the media:

Example: Colonial Pipeline fell victim of a ransomware attack in May 2021. It infected some digital systems of the pipeline blocking water supply for a few days.

or Hack Attack on NVIDIA

How to Be Protected

The most important thing is to understand that all the methods described below are not highly efficient when used individually. Protection from any kind of threats is a comprehensive set of measures that starts from educating staff and goes as far as protecting the IT infrastructure.

Ransomware operators plan such attacks thoroughly. They study the company, do research, hire specialists who look for vulnerabilities in the infrastructure etc.

1 Backup

Having up-to-date and reliable backups for all essential information is the most important item in your ransomware protection plan.

If in an unfortunate course of events hackers manage to gain access to and encrypt data on some devices in your network, having up-to-date backup will help you to restore the business or infrastructure work in a short time.

It is important that backups of the information that is of critical importance to your business are stored on a device that does not have access into the company network. It will come in handy if attackers succeed in corrupting most or all of your IT infrastructure.

2 Educating Staff

- Ransomware operators use email to deliver malware to the company infrastructure very often. Regarding costs, this way is very cheap, too. Anything can arrive by email, from a letter with a regular link to a malicious website to a letter with an infected Word or PDF attachment. The most important thing is to explain to the staff that they need to be cautious of any suspicious or unusual emails (and it doesn’t matter whether they arrive in their corporate or personal mailbox).
- It is also worth explaining the employees why downloading software from suspicious resources or inserting a flash drive found at the office door into a computer USB port is a bad idea.

The main thing to remember is that the **easiest** rules that **everyone seems to understand** are for some reason given the least attention.

3 Passwords

About a third of all ransomware is distributed by brute force attacks on companies’ unprotected services. With this attack method, hackers try to gain access to servers and other devices using as many password combination variations as possible. In most cases those attacks are conducted in hope that sooner or later they will manage to guess the password and penetrate the organization perimeter.

A mistake many companies often make is that they do not change default passwords on network devices (for example, username: admin and password: admin) or choose password combinations that are easy to guess (qwerty1234, password, pass123 etc.). This goes to show that brute force attacks are still relevant.

Ideally, there should be a unique password everywhere starting from admin panels of network devices to regular employees’ personal accounts. Complex passwords must consist of at least 12 characters, not contain full words, and have numbers and special characters.

For example: _+=@5T@a#BFkN2pc

4 Complicating Network Infrastructure

Obviously, hacker groups look for the biggest financial gain, and it is clear that if they compromise one or two computers in the network, they will not get it. In order to achieve more they look for ways to spread malware to cover most of the infrastructure. Segmenting your network will help you to make their job way more difficult.

It is also a good idea to restrict and additionally protect administrator accounts with access to all or the majority of your infrastructure.

5 Control of Connections to Corporate Network

Computers and servers are not the only devices you need to worry about. Office Wi-Fi, IoT devices and remote work scenarios are also at risk. At the moment there is a great number of devices that are connected to the company network and do not have inbuilt security systems. For example, a printer or another network device will have a backdoor through which cyber criminals can penetrate the company network. Extra attention needs to be given to such devices – they need to be protected in all possible ways.

Another potentially dangerous device is a personal laptop or the one given by the company that an employee takes home and then connects to the corporate network from it. For example, let’s consider a situation where an employee has brought their personal laptop to the workplace and connects it to the corporate network. Software from unknown sources is installed on it. The consequences may vary – from harmless to infecting all the company devices.

6 Antivirus

Updating antivirus software may seem like a trivial thing, but there still are companies, small ones as a rule, that do not pay due attention to it. At the moment a lot of antivirus software can detect ransomware in the system and warn about it. Some can even identify attempts to encrypt files and backup such data.

7 Up-to-Date Software

Patching is a tedious and time-consuming procedure which, however, is of vital importance for avoiding security breaches of your company infrastructure. Many companies avoid this procedure and fall victims of blackmailers as a result.

It is important to understand that ransomware operators monitor new vulnerabilities no less than IT security specialists (they are simply on opposite sides of the trench).

When a new vulnerability appears, for example, Log4j*, hacker groups start exploiting it in order to attack as many companies as possible before they update their software to a new version in which this new vulnerability has been patched.

Monitoring IT security news is also of no little importance in order to find out about new zero-day vulnerabilities**, their elimination or protection methods until a new patch is released.

* Log4j vulnerability is also known as Log4Shell or CVE-2021-44228. It is a critical software breach that allows offenders to run an unauthorized remote code just by sending a command to log a certain line. ** Zero-day vulnerability is a software vulnerability that was discovered by cybercriminals before software developers. There are no patches for zero-day vulnerabilities yet, which makes attacks more highly likely.

Contacts

🌐 www.safedns.com

☎ USA +1 (800) 820-2530

All +1 (571) 421-2990

✉ sales@safedns.com