CHECKLIST BY SAFEDNS

Dear colleagues, we have prepared **a special security check-list** for you. Check yourselves and see **how protected you and your business are against cybercrimes.** This check-list will allow you to check such informational security domains as:

- Infrastructure safety
- Hardware and software reliability
- Confidential information protection
- Data storage and pushing

01. Notable Ransomware Cases in 2020-2021

"Virus-encoders have become a number one cyberthreat both for business and state authorities: the number of successful attacks last year went up by 150% compared to 2019, and the average ransom amount in 2020 more than doubled and comprised $170,000. The greediest extortionists were Maze, DoppelPaymer and RagnarLocker. The ransom amount they were extorting from victims varied from $1,000,000 to $2,000,000."

02. In February ISS A/S, a Danish facility management services company, became a ransomware victim. The attackers encrypted the company database, which led to hundreds of thousands of employees in 60 countries being unable to reach corporate services. The company management refused to pay. They spent about a month restoring the performance of the most part of the infrastructure and conducting an investigation. Experts estimate total loss from the incident to be about $75–114 mln.

03. In February, Redcar and Cleveland Borough Council (UK) underwent an attack. The Guardian newspaper quoted a council employee saying that for three weeks the organization had to use pen and paper to do its job. During this time the IT-infrastructure used by hundreds of thousands of citizens had to be completely rebuilt. The council managed to fully recover from the attack only by May. It is when the cost of the incident was estimated at deplorable $20 mln.

This is only a fraction of all incidents with virus-encoders. The main aim of such viruses is to get ransom from the victim. Hackers usually attack small and medium businesses without paying attention to what they do, their main goal is a ransom.

Why ransomware is dangerous

Virus-encoders flourish thanks to people's lack of attention. By opening an infected file, a user allows the encoder to start the attack himself. One more problem is that such encoders don't have virus signatures or malicious code fragments, which is why without additional skillful customization an antivirus program will mark them safe.

How to reduce probability of loss from ransomware in 2021

- Do you update your software often? ☐ ☐
- Have you changed default passwords on network appliances? ☐ ☐
- Is your network segmented? ☐ ☐
- Do you have up-to-date backups of important information? ☐ ☐
- Do you use IDS/IPS (intrusion detection/prevention systems) in your network? ☐ ☐
- Do you use email filtering? ☐ ☐
- Do you use content filtering tools? ☐ ☐
- Do you have up-to-date antivirus software? ☐ ☐

Do your employees know how to recognize suspicious emails?	☐	☐
Do you control devices connecting to your network?	☐	☐
Do you have a ransomware response plan?	☐	☐
Do you use a SIEM-system?	☐	☐
Do you use access control based on admin roles?	☐	☐
Do you encrypt important data?	☐	☐
Do you store backups in the company network?	☐	☐

Annotation

01. Install patches in order to keep your software up-to-date. A classic example of damage caused by delay in patch installation is WannaCry. In the summer of 2017 this ransomware flooded IT-networks like a tsunami. It attacked a whopping 300,000 computers belonging to individuals, businesses, government agencies worldwide. In spite of the fact that Windows Server Message Block patch preventing attacks of the same type as WannaCry had become available months before the attack took place, a huge number of companies ignored it, which led to the infrastructure being infected.

02. About a third of ransomware was spread by password-guessing, brute force, and RDP (remote desktop protocol) attacks.

03. Ransomware operators usually look for the maximum possible financial profit. Obviously, they cannot achieve it by blocking a couple of computers. In order to cause as much damage as possible they penetrate the network and look for a way to spread ransomware to the largest number of computers. To prevent such a spread or to at least make things hard for hackers you need to segment your networks, as well as to restrict and additionally protect accounts of the administrators having access to the whole infrastructure. Phishing attacks are known to be mostly aimed at developers as they have access to various systems.

04. Having reliable and up-to-date backups of all critical business information is a crucial type of protection, especially from ransomware. As a result of an unpleasant concurrence of events when hackers are able to compromise several devices, having up-to-date backups means data can be restored and work restarted promptly. Considering the importance of backup strategy, the company must know where critical business data is stored. Perhaps a financial director stores data in a spreadsheet on their desktop and the data is not mirrored in the cloud. One important detail needs to be remembered: if you don't make crucial data backups or make them without a strict schedule, a backup strategy will be of little help.

05. If you have IDS installed, you can find out about the penetration much faster and take all possible steps in order to prevent the attack.

06. The easiest way to protect your staff against hitting a malicious link in an email is to prevent it from ever getting into their mailbox. In order to achieve it you need to use content scanning tools and email filtering. Installed filters will drastically decrease the number of phishing and extortion emails.

07. A content filtering system protects a corporate network from numerous threats such as viral and phishing sites, ransomware, botnets and cryptomining attacks. It helps to prevent possible financial and reputational damages from cybercriminals.

08. Updating antivirus signatures seems like a trivial task, however, some companies, especially small ones, do not pay enough attention to this process. Many modern antivirus packages include ransomware detection functions or customizations detecting suspicious behavior typical of all extortionists, that is, file encryption. Antivirus signatures understand when external software is attempting to modify user's files and to encrypt them, and try to stop the encryption process. Some security packages even make backups for files threatened by ransomware.

09. Email is one classic way for ransomware to penetrate a company. It is because sending malware to thousands of email addresses is a cheap and easy way for ransomware operators to spread it. Even though such tactic is seemingly primitive, it is still appallingly efficient. In order to protect the company from ransomware and phishing spread via email the management should organize a workshop and teach the staff how to recognize suspicious emails.

10. Office Wi-Fi, IoT devices and remote work are only a few of a great variety of devices connecting to the company network and lacking inbuilt security functions that a corporate device needs. The more of those you have, the higher the risk that one of them, for example, a badly protected printer, will have a backdoor that cybercriminals can use to penetrate the corporate network.

11. Each company must have a performance recovery plan for an unforeseeable intervention into work processes, whether it be hardware failure or natural disasters. Response to ransomware attacks should be an inherent part of such plan. It should both address technical issues (cleaning up PCs and restoring data from backup) and encompass a broader business aspect. For example, how to explain the situation to buyers, suppliers and media, or whether the police, insurance company and regulating authorities should be involved. After a plan has been developed it is essential to make sure it is viable, because some assumptions may be wrong.

12. SIEM receives event information from different sources, such as firewalls, IPS, antivirus software, OS etc. The system filters the data and changes its format into common and analyzable. It allows to collect and centralize log storage in different systems. Then SIEM correlates events looking for interconnections and regularities. This allows to achieve high efficiency in detecting potential threats, IT-infrastructure failures, unauthorized access attempts and attacks.

13. Companies should apply minimal privilege access policy. It means that users should be granted access only to the resources necessary for their job. It is also important to understand that it is psychologically easy to focus only on basic users, but it is necessary to remember that the IT department staff represent the largest potential threat of all. RBAC (Role Based Access Control) should be used to separate administering responsibilities. It will greatly reduce the damage a single administrator may cause if they become a fraud or if their account is compromised.

14. Storage encryption may significantly decrease internal cyberthreats. If someone steals backup on a hard or tape drive, or exports a virtual machine copy, encryption can prevent the person from reading such information thus making data useless.

15. Regular backups are essential. But if such company backups are stored in the network and not autonomously, extortionist attacks may not only infect a source computer, but also backups intended to restore it.

SAFEDNS