10th anniversary EUROPEAN CYBER SECURITY MONTH

Prevention Response for Ransomware Attacks

choose to be safe online

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

In this document, you will find a protocol to
prevent and respond to ransomware attacks
and have your company prepared for these cyber threats.

Prevention

Prevent a **ransomware attack**.

1. Software appliances

Double-check to make sure that all users log in and work from under a VPN.

Make sure that you have a firewall installed and actively working.

Your organization must be using the latest generation and updated endpoint protection measures. They can also be combined with whitelisting, real-time executable blocking, etc.

Create a dedicated anti-spam/anti-phishing system, it can either be done using software or by utilizing the dedicated hardware appliances.

The patch procedure within your organization must be highly disciplined and the updates must be applied to all applications and the OS, as soon as the vulnerabilities are detected and a new patch is out.

Use cutting-edge email security techniques like DNSSEC, DANE, SPF, DKIM.

2. Backup solutions

Implement a sophisticated backup solution for your organization's data, it can be either software-based or hardware-based, or even a combination of the two.

Perform regular testing of both your recovery functions (when it comes to your backup solution) and your data in general. All of the data up to several months back should be regularly tested to ensure that it's not compromised from within at the same time as the attack lands.

Check if your backup solution covers all of your data, to ensure that all of it is saved and can be accessed if the worst happens.

As a continuation of the previous point, it's also important that your backed-up data is easily accessible in its backup form, and that your data is safe in general. Follow the 3-2-1 principle: Have three different backups, on two different types of media, and keep one backup off-site.

3. Theft prevention methods

Take advantage of system logs, in order to track data movements.

Implement data encryption technologies for your data in general – mid-transfer and at rest.

Acquire and use extensive DLP (Data Leak Prevention) tools.

Don't forget to analyze your network traffic, to search for unusual data movements within the system.

Use the method of least permissions to protect your databases, folders, and singular files (meaning that you do not give your users any permissions aside from the ones that they need to have in order to do their work properly).

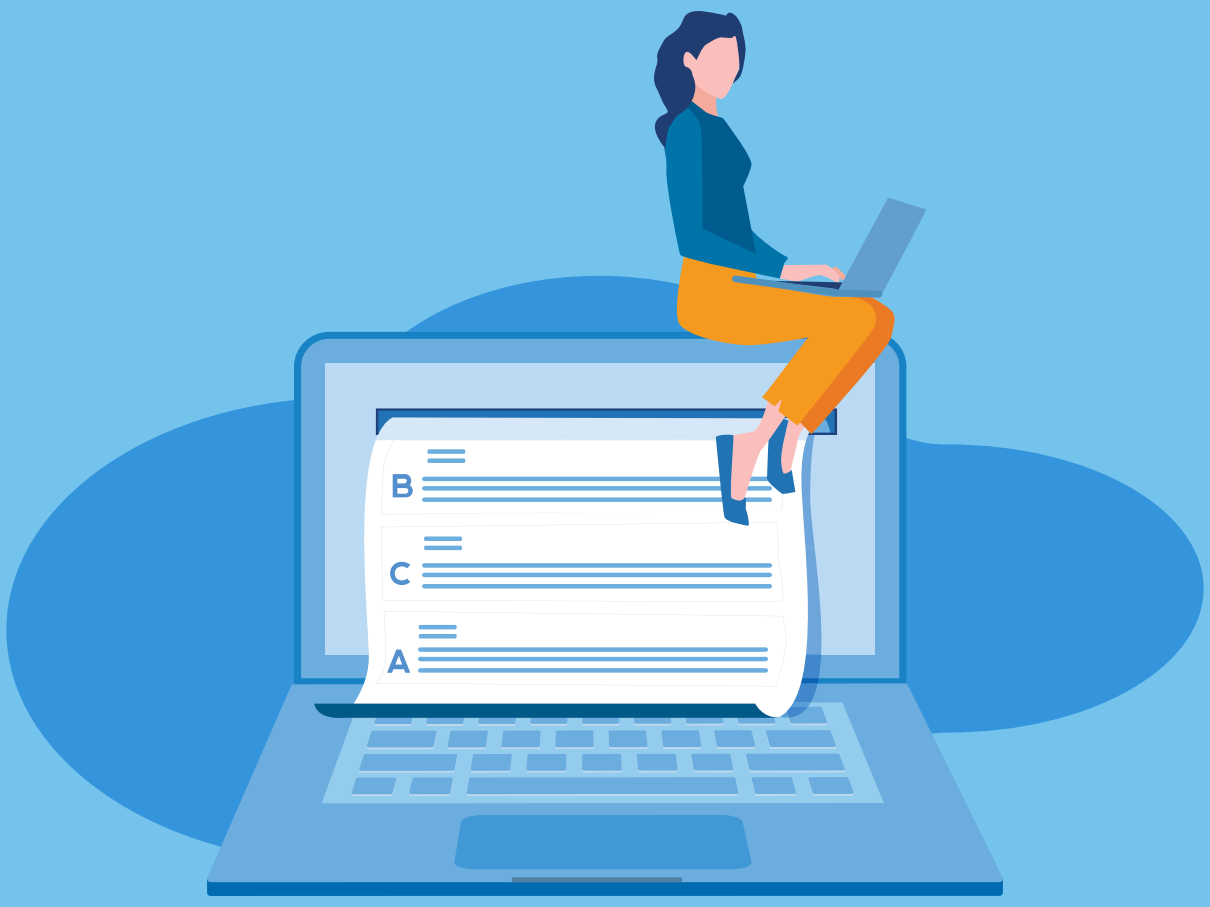
4. Users' knowledge

Regularly conduct simulated phishing attacks to educate your users about the course of action to take, as well as to test your own systems.

Invest in security awareness training for your users, so that they know how to look out for suspicious applications and don't download/execute them.

Set up a clear, easy-to-follow reporting line and workflow for reporting suspected incidents. Let your users know about it!

Response



Respond to a **ransomware attack**.

1. Disconnect the source of the ransomware

Your first step should always be towards limiting the scale of the attack as much as possible, which means that you have to:

- Unplug all affected computers from the network.
- Turn off all wireless data-transmission methods, including Bluetooth, Wi-Fi, NFC, etc.
- Consider every device compromised and treat it as such.

2. Determine the scale of the attack

Right after attempting to limit the extent of the attack, it is essential to find out the scale of the damage so far, which means looking for signs of unusual encryption within different storage locations, such as:

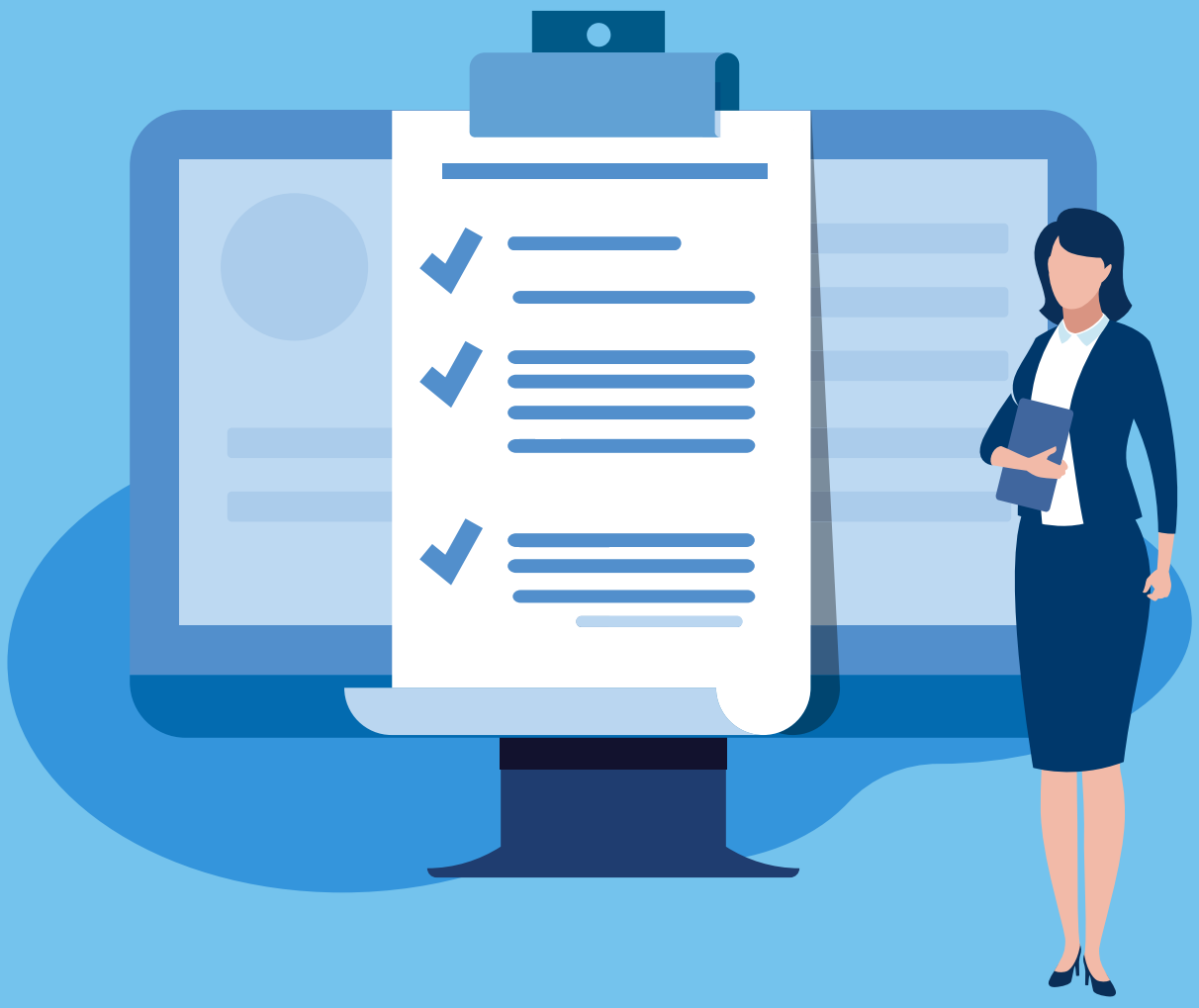
- External hard drives.
- Cloud-based storage locations (OneDrive, DropBox, Google Drive, etc.).
- Mapped or shared drives.
- Various USB storage devices, such as USB drives, attached cameras/-
- phones, and such.
- Various network storage devices.
- Call in local law / police / CERT agencies. In some cases, this may even be a legal requirement. Also, the needed forensics from this point on will be likely above what even your (good!) admin team can do.

3. Find out if any of your data has been stolen

There are different methods for doing that, including:

- Typically, one of the most obvious indications of data theft is some kind of notice from the cyber attackers that your data has been stolen.
- Unusually large files with the archival format (.zip, .7z, etc.) that contain confidential data transmitted over your network.
- Logs and DLP software reports can help find signs of data leaking somewhere.
- You might even find the malware or tools that were used to find and copy your data in the first place.

Check list



What to check in case of suffering a **ransomware attack** in your organisation.

1. **Restore your files** from a backup.

- [ ] Ensure that the initial attack vector is eliminated thus you will not be attacked again.
- [ ] Locate your backups and ensure that all of the files are still in place.
- [ ] Verify the integrity of your backups, and check for corruption signs.
- [ ] It's also recommended to check for shadow copies (if possible) and for
- [ ] previous versions of your files (if it's about cloud storage).
- [ ] Remove the ransomware from your system, one way or another.
- [ ] Restore your backed-up files.
- [ ] Find out the infection vector and how to close it off.

2. If you're trying to **decrypt your files.**

- [ ] This might be attempted mostly in specific cases when it's possible to determine the type of ransomware and there's a decryptor available for that specific strain.
- [ ] To decrypt your files after locating a decryptor you just have to connect all of the storage media with encrypted files...
- [ ] ...and decrypt those files using the decryptor.
- [ ] Find out the infection vector and how to close it off.
- [ ] If decryption is not possible at the time, keep your encrypted files for later, maybe some new solutions will arise helping you retrieving your data.

3. If you're doing **nothing about ransomware.**

- [ ] Remove the ransomware, one way or another.
- [ ] You might want to consider backing up your encrypted files and not deleting them in case you'll be able to decrypt them in the future.

10th anniversary EUROPEAN CYBER SECURITY MONTH

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY