



# Ransomware attacks: Do's and Don'ts

Anyone who suddenly finds themselves facing locked devices and encrypted data should be aware: The attackers have most likely not just penetrated your network to plant their ransomware. Expect that they have already been looking around your systems for some time and may have taken a lot of sensitive data beforehand.

**A clean, functioning backup is the be-all and end-all, but there is more to consider.**







# „Your files are encrypted“

## The right reaction in an emergency situation

The correct assessment of the situation is crucial in the case of cybersecurity incidents. It is a prerequisite for taking the right measures.

The better and faster you understand your options, the more targeted and professional your response and the better your chances of minimising damage - whether it be overpayments, further data loss, damage to reputation, data protection breaches or production stoppages.

### Mistakes you should avoid:

-  **Hand in:** Do not expect the authorities to be able to actively respond to your case immediately or even support you with a team on the ground.
-  **Hurry:** Do NOT respond to the extortionists' ransom note for now, otherwise the clock will start ticking. Strategy is more important than speed.
-  **Keep it secret:** Inform the management about what has happened, what measures have already been taken and what external assistance you need. Make unmistakably clear to what extent your structures are affected and what options are open.
-  **Make decisions:** Even if you use external help, ultimately YOU have to make the decisions for your company - after competent advice. Avoid unnecessary delays, these usually only lead to your data being published.
-  **False expectations:** The matter will not be resolved in a few minutes or hours. Work thoroughly and thus prevent further risks. Do not expect your negotiating skills to change the attackers' minds - even a reduction in the amount demanded is not "part of the game". Never forget that the attacker knows your financial situation very well.
-  **Emotions:** Do not get carried away by your emotions. It is neither easy nor pleasant to negotiate with criminals. Emotions only lead to reactions that you certainly do not need. Therefore, go for 100% professionalism.

## Measures and decisions you should take now:

- ✓ **Snapshot:** Record as quickly as possible which areas and network segments are affected and to what extent. The more profound your assessment of the situation, the clearer and faster you can determine your options.
- ✓ **Analysis:** Get clarity, also about the type of Trojan or Ransom-as-a-Service. Most attacker groups provide clear, structured instructions and clues.
- ✓ **Teamwork:** Put together a competent team of internal and external experts, who consult, decide and act together.
- ✓ **Communication:** Keep partners and customers informed. An open communication strategy can protect your stakeholders from being attacked via your infrastructure or suffering data loss. Also be aware of the legal requirements for reporting data breaches.
- ✓ **Negotiating partner:** At the latest when the blackmailers make contact, you should have a professional negotiator at your side.
- ✓ **Security:** Set up secure communication channels and financial transaction facilities where applicable - prepare everything to ensure security and integrity.
- ✓ **Law enforcement:** File a complaint and contact your national cybercrime reporting centre.
- ✓ **Emergency plan:** Follow your emergency plan for ransomware attacks - or write it now at the latest.

### *Prevention tips*

Diversify your **backup and storage strategies**. Ensure that backups are also stored externally and are available.

Strengthen your protections against **email-based attacks** now, evaluate your **endpoint solutions** and control **remote access tools**.

Optimise your **network segmentation** to contain an infestation and invest in measures for **early detection** of anomalies and system vulnerabilities.

## Prepare now for possible attacks

With 304 million ransomware attacks in 2020 - 62% more than the previous year - and the ransomware-as-a-service business model, the question is not *if* but *when* you will fall victim to a corresponding attack.

Company size is not a measure of probabilities: Several easier targets are often more lucrative than one large, hard-to-reach one. The rule of thumb is therefore: the lower the protective barriers, the greater the danger.

### Pay the ransom or not?

The question of whether or not you should pay the demanded ransom seems the most important at first - but it is far from the only one. Again, a well thought-out strategy counts.

The clock is ticking - start your actions in the following order:

- **Incident Response** to prevent existing and further third-party accesses
- **Investigation** to ascertain the reason for and extent of the damage
- **Recovery Plan** to determine the ways and means back to business capacity
- **Teambuilding** with internal and external specialists
- **Communication** with your stakeholders
- **Confrontation** with the attackers

Keep the following goals in mind when making decisions:

- **Business capacity**, as far and safe as possible
- **Control** over your systems
- **Communicate** expectations and goals regularly
- **Update** your ransomware emergency plan with your learnings

Consider the following aspects:

- Risk from **compromised data**
- Status and condition of your **Back-ups**
- Effort for **resetting** the locked devices
- Time and costs until **resumption of business activity**
- **Financial solvency**
- Costs for **public relations**
- Costs as a result of **data loss**

## Emergency plan for security incidents in IT, OT or IoT environments

Cyber security incidents can affect any company or organisation. The decisive factor in all response measures is speed. Fast and targeted actions significantly reduce the technical and financial impact of cyber-attacks.

Do not waste time searching for available experts: With **IKARUS 24/7 incident.response** you receive targeted measures for investigation, threat hunting and cleaning up your systems within a maximum of four hours.

<https://www.ikarussecurity.com/en/it-ot-iot-security/ikarus-24-7-incident-response>

## We will be happy to advise you!

From endpoint protection and EDR capabilities to email security, APT protection and 24/7 incident response services, you can find all the information and services you need to protect IT, OT and IoT environments from ransomware and other cyber threats at [www.IKARUSsecurity.com](http://www.IKARUSsecurity.com).

Sales Hotline: +43 1 58995-500 | Email: [sales@ikarus.at](mailto:sales@ikarus.at)

**MANDIANT**



### About IKARUS Security Software

The Austrian cyber security specialist IKARUS Security Software GmbH has been developing and operating leading security technologies since 1986 - from its own scan engine to cloud services for the protection of endpoints, mobile devices and email gateways to the modular threat intelligence platform.

Together with its technology partners Mandiant, FireEye and Nozomi Networks, IKARUS expands its own portfolio with internationally market-leading technologies and is *the* Austrian point of contact for incident response and global and local threat intelligence for IT/OT/IoT security.