INFOGRAPHIC

# Ransomware: how to prevent attacks and heal damage

The ransomware threat is imminent, and chances are high your company will fall victim. But that doesn't mean you can't put measures in place to limit the damage. We categorize these measures in four sections: Identify, Prevent, Detect and Heal.

## Identify

- Find your **crown jewels** – data your company absolutely cannot afford to lose. Prioritize the protection of these crown jewels.
- Make a **risk assessment**, to locate the most vulnerable spots and to determine the maximum damage an attack could cause.
- Appoint one or more **security ambassadors** in your company, who keep information security on the agenda.
- Make sure you have a clear picture of the number of devices in your network, and the level of protection on these devices (e.g., up to data software and security).

## Prevent

- Train your staff on internet and e-mail safety. Most threats can be avoided with **knowledgeable staff**.
- Set up a regular **back-up schedule**, so you can always restore a recent backup when ransomware hits. This could severely limit data loss.[1]
- Enable **network segmentation** to isolate an infected area from the rest of your IT environment, thus limiting the blast radius of attacks.
- Establish a 'zero trust' architecture to reduce the attack surface: restrict access to your data and applications when the participant's identity is not verified.

## Detect

- **Endpoint protection** will not be enough to stop ransomware, but it is still vital to block malicious activity and spot security incidents. To avoid an overload of security alerts this requires a tailored approach, protecting your crown jewels.
- Advanced security solutions can detect anomalies within your data and are useful to spot suspicious activities in an early stage.
- A **Security Operations Centre (SOC)** can provide you with a single point of contact to detect security incidents, but also to share knowledge about common threats.
- Time is of the essence when security incidents occur. They should not only be reported, but also be followed by an adequate incident response. Establish what this plan of action entails for your business.

## Heal

- Although paying the ransom may be tempting to get your business up and running again, on average, it's not a solution to guarantee full data recovery.[2]
- Database dumps with ransomware keys are sometimes made public, as well as **decryptors** to unlock ransomware. Again, there's no guarantee, but these solutions may prove helpful in some cases.[3]
- Specialized companies can try to decrypt your data, but this is an expensive, painstakingly, and time-consuming process (without the guarantee that all data will be recovered).
- Restoring a backup is the best solution to recover data and resume business activities fast. But in a lot of cases, ransomware encrypts your backups as well. Use an immutable backup instead, which is unchangeable and thus unaffected by ransomware.

**Even if you manage to recover your data, it remains essential to find the cause of the attack. The malware that triggered the ransomware could already be present in your restored backup. Read more on an adequate backup strategy in our blog.**


BPSOLUTIONS
Papendorpseweg 99
3528 BJ Utrecht

T +31 30 303 2900
E info@bpsolutions.com

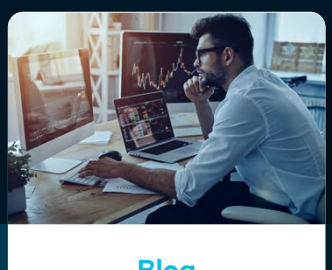
www.bpsolutions.com


BPSOLUTIONS

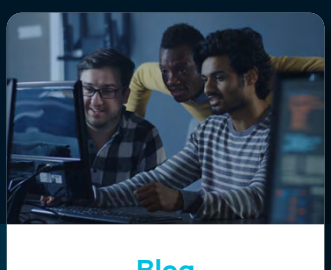
SOURCES

1 https://www.gartner.com/en/documents/3995229/detect-protect-recover-how-modern-backup-applications-ca
2 https://secure2.sophos.com/en-us/content/state-of-ransomware
3 https://www.nomoreransom.org/en/index.html

## FURTHER READING

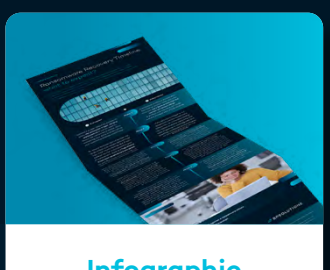


**Blog**
Seven reasons why it's time to bart your backup
Read blog



**Blog**
A ransomware attack every two seconds in 2031
Read blog

**Infographic**
Ransomware Facts & Figures
Download



**Infographic**
Ransomware Recovery Timeline: what to expect?
Download