How to protect yourself from ransomware with Nuabee

Cyber-Resilience by Nuabee · https://nuabee.com/documents/how-to-protect-yourself-from-ransomware-with-nuabee/

What is a Ransomware Attack?

A ransomware attack is a specific type of cyberattack where attackers use malicious software to encrypt the victim's data, rendering it inaccessible. The attackers then demand a ransom in exchange for providing the decryption key. Here are the main characteristics of a ransomware attack:

- **Data Encryption:** Ransomware encrypts user files (on workstations or servers), making them inaccessible without the decryption key.
  Ransom Demand: Attackers demand a ransom, often in cryptocurrency, to decrypt the data.
  Rapid Spread: Some ransomware spreads rapidly across networks, infecting many systems in a short period of time.
  Direct Impact: Victims immediately lose access to their data, disrupting operations until the problem is resolved.

Ransomware protection mechanisms

Of course, there are many security measures that can be taken to reduce the likelihood of a company being affected by a ransomware attack, including:

1. **Training and Awareness:** Train employees to recognize phishing attempts and other threats.
2. **Network Security:** Use firewalls, intrusion detection systems (IDS), and virtual private networks (VPNs).
3. **Malware Detection Tools:** Deploy malware detection and prevention solutions (EDR/XDR).
4. **Network Segmentation:** Segment the network to limit the spread of ransomware in the event of an infection.

However, even with all these protective measures in place, there is no 100% guarantee against a successful attack. It is therefore essential to have **recovery measures** in place, the most important of which is offsite data backup.

How Nuabee helps recover from a ransomware attack

Through its outsourced cloud backup solutions, Nuabee provides the following key protections:

1. The first level of protection is obviously the depth of backup copies in the cloud.
    - Even if some data has been encrypted and sent to the cloud, the depth of the backups will allow you to start again from a previous healthy backup, i.e., one that has not been encrypted by the ransomware.

2. Next, it is also a question of the immutability of backups and ensuring that the ransomware has not been able to access the cloud storage space and corrupt the backup data.
   Isolation between the cloud and the customer's production environment (with completely separate AK/SK and dedicated security mechanisms) allows backups to be protected.
   The change in technology between the customer's infrastructure and the backup spaces (S3 storage) ensures a technological break.
   It should not be forgotten that in the context of ransomware encryption, there is 100% entropy of backups, which means that 100% of the encrypted data will be re-uploaded (as in an initial upload).
   Nuabee's monitoring tools can detect this behavior and quickly alert you in the event of data encryption at the source.