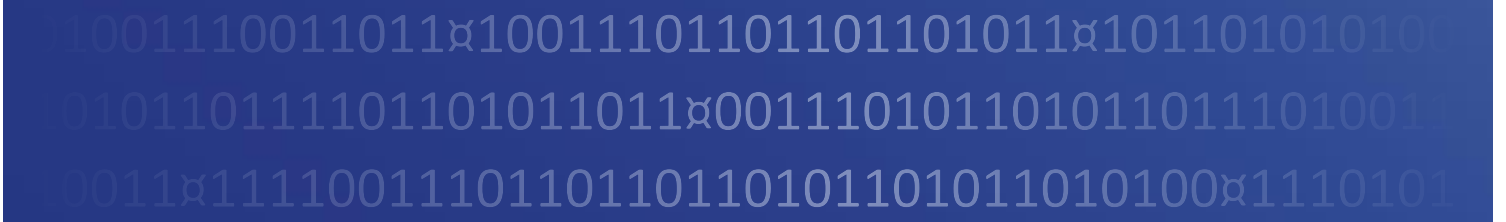
Expect the best, plan for the worst. Protect your data!



Again and again malicious software manages to break through generic protection programs. In such a case, you undoubtedly wished you planed ahead. There is nothing wrong hoping for the best but you should always prepare for the worst. It is worth it. Luckily there are software available that will keep your data secure and let malware bounce off. Software tailored especially to the protection of backups and can therefore work with more precision than generic protection software.

Learn more, Why?, What, How

WHY?

Ransomware is becoming a growing threat for companies of all sizes and branches. The number of attacks are rapidly increasing. At the same time, it is becoming more difficult to protect oneself from these attacks. When a computer becomes infected with ransomware, it poses a threat of colossal damage to the whole company, and now the target is the backup server.

And… unfortunately, there are examples to prove it:

> A 4 Billion € revenue company with 15 000 employees was hit by hackers and all data were encrypted. Several data copies/data centers were affected and the company was not able to communicate, pay bills, order material, pay wages etc. The only way to get the company back online before going bankrupt was to restore from tape.
>
> Restore from “reduced” tape resources was estimated to take 4 weeks!
>
> With additional tape hardware, client was back online after 2 weeks!

What

What to do if you suspect you are under attack?

- Stop the Backup server
- Startup the server in MAINTenance

This specifies that the server is started in maintenance mode, and that administrative command schedules, client schedules, client sessions, storage-space reclamation, inventory expiration, and storage-pool migration are disabled.

Why? Because your last good backup of all files are changed to inactive version and you don't want to lose those files by running an expire inventory that will potentially make that happen.

Additional ways to protect your backup (and more!):

- Tape is not a modern solution, but proven in battle.
- Cloud is a new way of securing your data offsite, and the objects are worm-ish.
- What if I could make my Backupserver to act as a WORM device?

The more barriers there are between an infected system and its backups the harder it will be for the ransomware to get to it

How? Blocky!

Blocky is a software product designed to protect your data from ransomware attacks “Your Last Line of Defense”

Your Last Line of Defense

How Blocky works?

Blocky generates a fingerprint of every process and it prevents any write acess, if the fingerprint is not explicitly allowed for this process or application.

Why Blocky?

The common ways of protection are airgap. Blocky is able to prevent damage, even if a virus invades and even disabled the Blocky protection.

The effective protection of Blocky4Backup is guaranteed by a security module. As a gate to your data, it enables access to you first – of course only for authenticated processes. That means there is no way for malware through this gate.

Let´s Talk!

Cristie Nordic is specialized in data availability working with data loss protection and primary data storage since 1997. We provide storage and backup as a service for Enterprise-class and modern workloads, no matter where you want to keep it (on-prem, cloud or hybrid).

In short - We make your data available, anytime, anywhere!

CONTACT