Security Hardening and Ransomware Resilience of Nextcloud AIO

Stavros Kousidis

Bachelor thesis · Published: 2026-10-15

Research question

Which hardening and recovery measures improve the resilience of a Nextcloud All-in-One deployment against selected ransomware-related attack scenarios, and what limitations remain?

Description

Nextcloud All-in-One (AIO) offers an integrated approach to self-hosted cloud storage, including optional backup capabilities. Nevertheless, successful recovery after destructive changes depends on where an attacker has gained control, which credentials are available, and whether recovery data remains independent of the compromised system.

You will develop a threat model for a representative Nextcloud AIO installation and evaluate selected hardening and recovery configurations. Consider distinct attacker capabilities, such as a compromised synchronization account and a compromised application component. Host-level compromise can be analyzed as a boundary case without attempting to solve every possible attack.

Scope and evaluation

Build an isolated deployment using synthetic data. Reproduce two or three controlled scenarios involving unauthorized modification, deletion or encryption-like corruption of files. Compare selected controls and backup configurations against a documented baseline. Measure whether damage is contained, what data can be restored, and the time and operational effort required for recovery. Explain which conclusions depend on assumptions about backup isolation and attacker privileges.

Experiments must remain inside the laboratory. No real ransomware or attacks against third-party systems are required.

Licensing note: Nextcloud AIO and Nextcloud Server use AGPL-3.0. Simply deploying and testing them does not place independent test tools under the AGPL. Modifications to covered components must comply with applicable AGPL obligations, potentially including source availability for network users. Determine the license boundary before modifying upstream code; the general publication policy applies to independent tools.

Expected outcome

A reproducible Nextcloud AIO test environment, a threat model, measured containment and recovery results, and practical recommendations justified by the experiments.

Starting points

- Nextcloud All-in-One: deployment and backup documentation.
- Nextcloud: server hardening guidance.
- BorgBackup documentation.
- NIST SP 1800-11, *Recovering from Ransomware and Other Destructive Events*.

Contact: stavros.kousidis@th-koeln.de
Code publication: open source by default; exceptions require prior agreement (policy).