Security issues regarding backups

Tamás Hetesi

CTO, Crosssec Solutions


WARRANTY VOID • IF SEAL BROKEN •
WARNING!!
DO NOT COVER
BREATHER HOLE
Quantum.
Fireball lct
lct 10 3.5" SERIES
N143
POWER REQ: 5/12V ⎓ 600/900mA
WWW.QUANTUM.COM
WARNING: REMOVAL OF LABEL, COVER
OR TOP SCREWS VOIDS WARRANTY
15.0AT P/N LB15A011 Rev 01-A

3-2-1

backups = safety,
backups = hazards

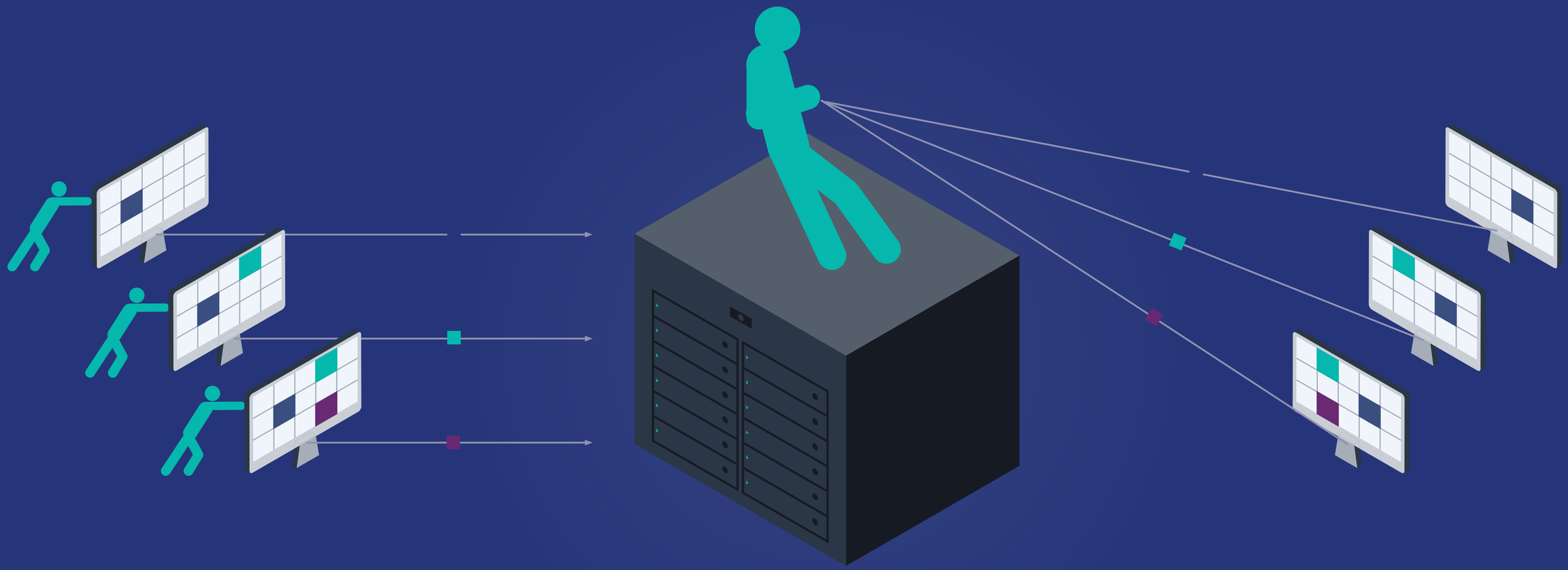
- Setting up backups is not fun
- Monitoring backups is not fun
- Testing restores is not fun

- And they also introduce new security issues

Intrusion scenarios

- Extra copies to steal
- Denial
- Tampering
- Payload delivery

push vs pull



Pull

- (Privileged) access to all clients
- Backup server intrusions affect all clients
- Payload delivery: write to disk, execute

Push

- Owning a client = access to snapshots
- Multi-tenant: others' snapshots?
- Hard to scale
- Remote management: no longer pure push

Push - payload delivery

Write to disk, get it restored

- wait
- prompt a restore
- breach test restores

Some community favorites are inadequate

Simple is just too simple

- rsync
- rsnapshot
- rdiff-backup

Also: most clever home baked scripts

Restoring backups after an incident

- Files > full images
- Restores are stressful, don’t skip security
- Clients like to salvage wrecks

A fun exercise

How easy / fast it is to find the last known good snapshot?

- minutes? hours?
- good to know
- should not be entirely manual

Remedies

- Verify remote server identity
- Encryption
- Data hashes and verification
- Dumb protocols, restricted shells

Remedies

- Append-only backup targets
- Intrusion checking freq vs backup retention
- `# encfs --reverse` for software you don’t trust
- Declarative infrastructure: skip system files

Recap

- Push and pull has their own problems
- Hashing, verification is important
- Test restores in sealed environments
- Avoid disk images
- Checklists save your bacon, include security

Backups = frienemies. Respect them.

Tamás Hetesi

tamas.hetesi@crosssec.com

tams@tams.hu

crosssec
SOLUTIONS