4 storage security myths you shouldn't fall victim to

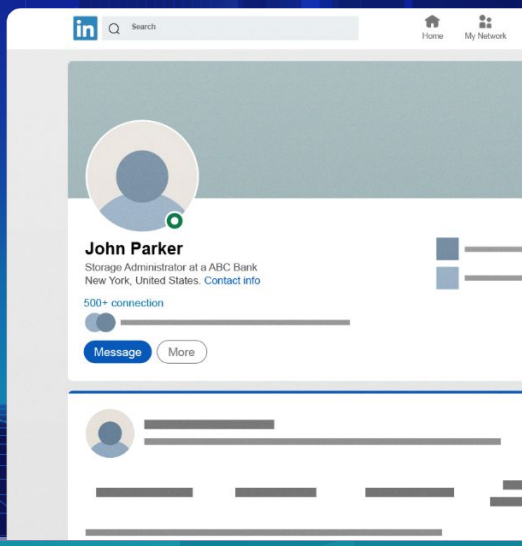
CONTINUITY

MYTH #1:
Storage is too deep to reach and too obscure to attack

This is very far from the truth… Your storage admins can be targeted.

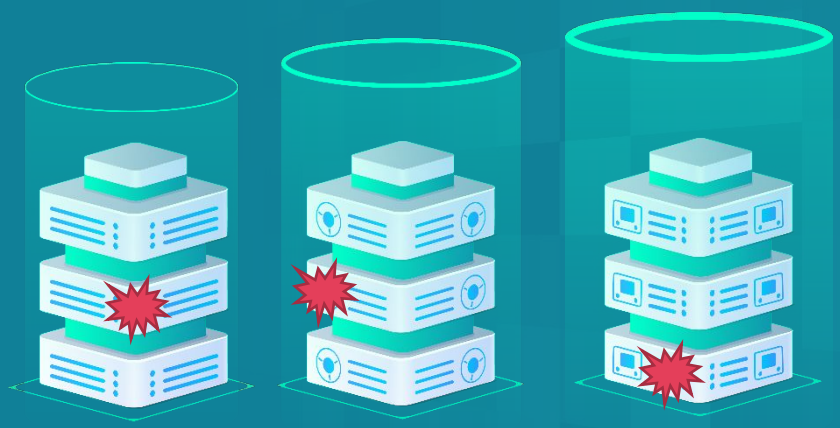
All it takes is a spam email, a misleading link, or a fake software update, which spreads malware.

From here the road to directly controlling the storage device is nice and easy for the hacker



Reality check #1: It's much easier to get into the storage layer than you think! Modern attackers can hack storage systems with ease

MYTH #2:
I have backup. What can possibly go wrong?



1st: Snapshots

If hackers gain access to the storage system, they can easily wipe out these snapshots

2nd: Replication

Hackers with admin credentials will often delete the replicas as soon as they finish with the production storage

3rd: Backup & Archiving

The last line of defense. Hackers will usually immediately delete them upon penetration

Even if your backups are perfect …

Backup is multi-layered

All layers are inherently vulnerable

Reality check #2: Hackers go for the backups first. Most organizations do not secure backups and other types of copies (e.g., replicas & snapshots) well!

MYTH #3:
We already use vulnerability scanning tools that cover storage

I monitor all suspicious activities…

Hmm... does this include storage?

Often – the answer is "no"…

Auditing and logging tools don't go to the level of detail required to protect storage systems. Allowing attackers a very clear path to modify, destroy and steal data without leaving any trace

Reality check #3: Existing tools offer almost zero coverage for storage, storage management, and backup

MYTH #4:
Data secured by multiple layers cannot be breached

New types of ransomware are targeting storage and backup systems.

Data security solutions are ineffective.

Leaving your last line of defense exposed

Storage is the only layer of IT not covered by traditional vulnerability management tools

Reality check #4: Data is rarely secured where it counts most: at the storage layer! This is a huge attack surface

Is it time for more storage security?

	Commonly-held Assumption	Reality
Data	Data is already secured at multiple layers (OS, Database, Network…)	Storage & Backup is where 100% of your data lives!
Attack Surface	Small and deep inside the perimeter/datacenter	Large, vulnerable, and reachable
Threat Level	Most attacks target users, end-points, servers	Number of attacks on storage is small but growing; however, impact can be devastating
Ransomware	Most ransomware encrypts data on end-points/servers; securing storage can't stop that	Storage and Backup is the last line of defense against any ransomware attack – secure data copies & backups essential for recovery!
Existing Tools	Lots of tools already in place for vulnerability scanning (e.g., Rapid7, Nessus, Qualys)	Existing tools offer almost zero coverage for storage, storage management, and backup

CONTINUITY

For more information:

www.continuitysoftware.com | Schedule your Storage Risk Assessment | Follow us on