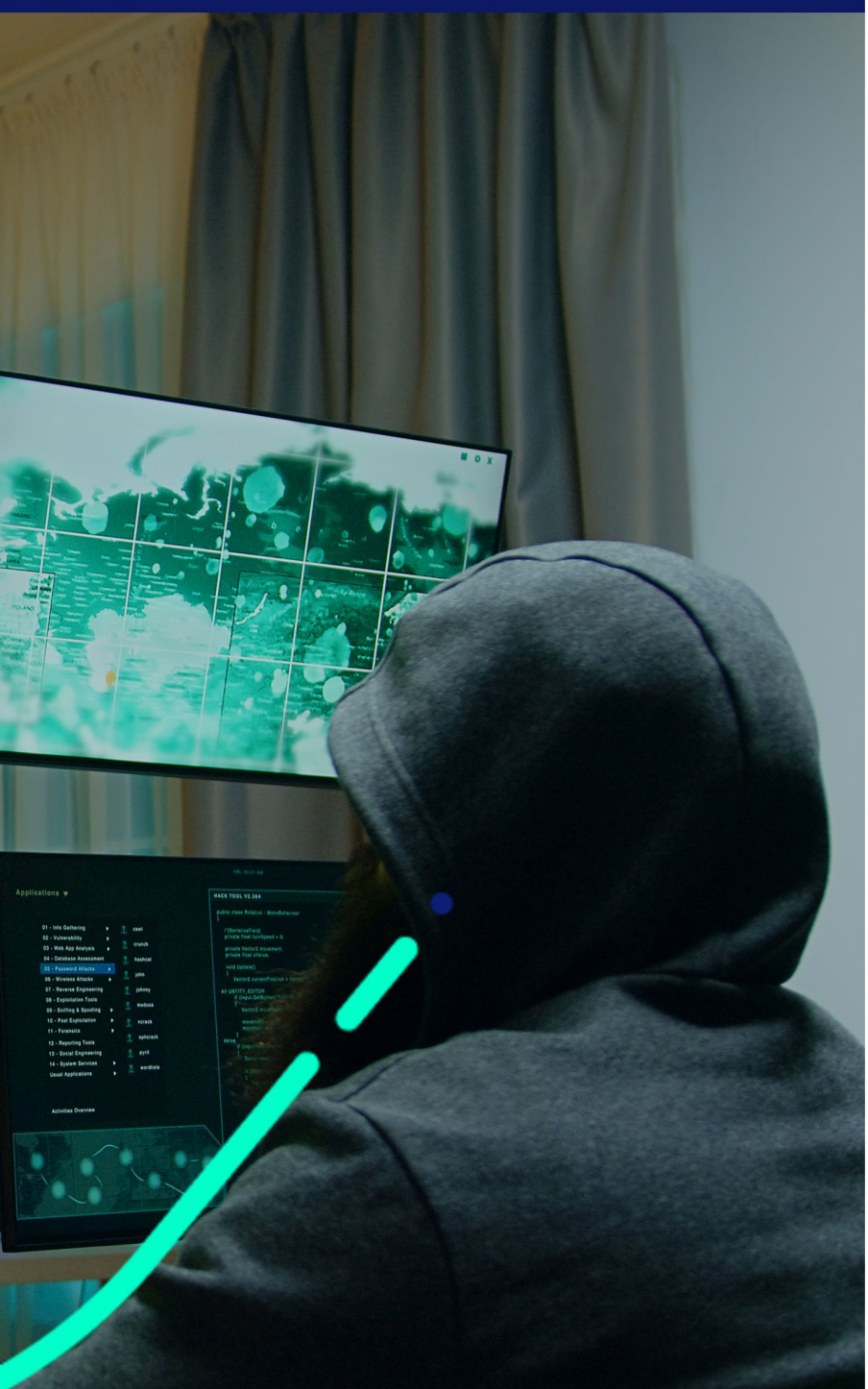
When, Why and How To Create A Secure Backup Strategy

6 Steps to Success

CONTINUITY

Introduction

When data is compromised, the last line of defense is your backup.



In the past year, the tactics being used by cybercriminals have changed. And it puts larger organizations with legacy backup environments at major risk.

The attackers realize that an attack on the backup is the single biggest determining factor to show if the victim will pay the ransom.

And it seems to be working.

The average cost of recovery from a ransomware attack has more than doubled in a year, according to a Sophos survey.

This same report also shows that just 8% of organizations manage to get back all of their data after paying the ransom.

If organizations are unable to recover their data, the impact would be devastating – and not just because of the ransom payment.

The damage could include loss of revenue, significant business disruption, damage to brand reputation, and regulatory fines from compromised consumer data.

The fact that so many victims eventually choose to pay the ransom gives rise to serious concerns about the market's backup security maturity.

Fueled by the expansive media coverage and dramatic financial repercussions of data-centered crimes, organizations are in a race to identify and close the gap.

The Conti ransomware gang has developed novel tactics to demolish backups

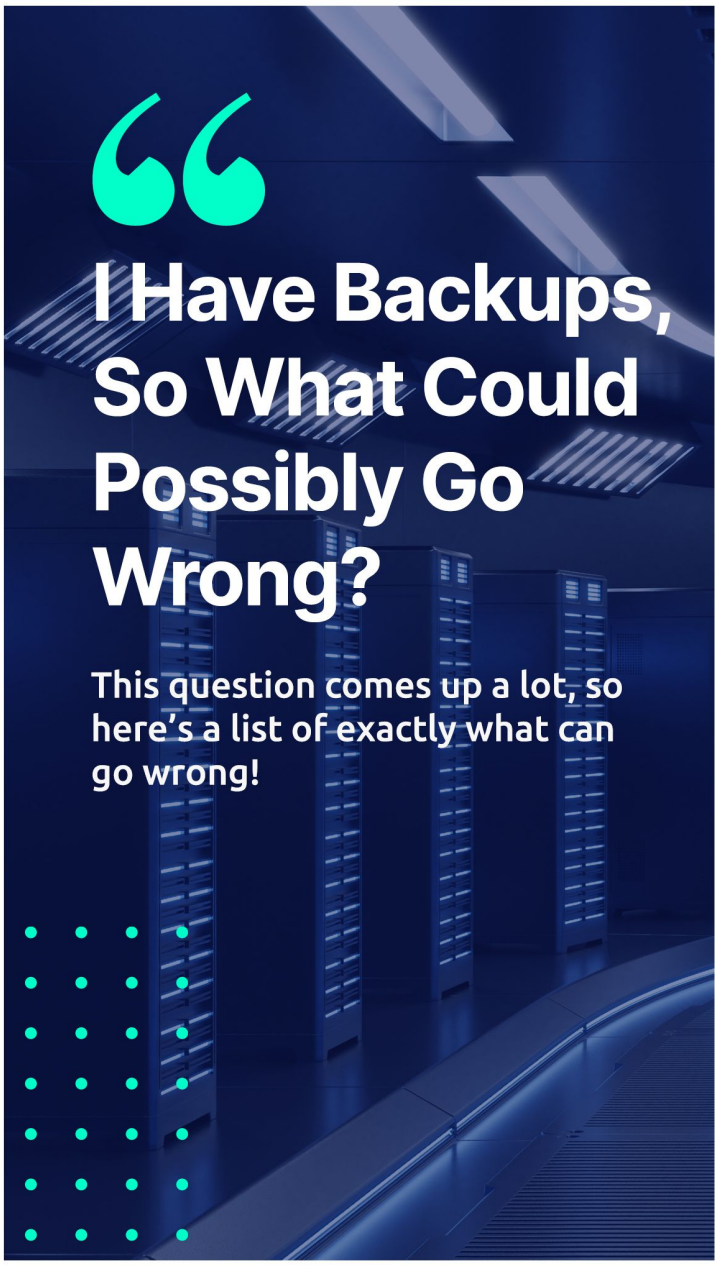
Conti bases its negotiation strategies on the premise that the majority of targets who pay the ransom are “motivated primarily by the need to restore their data.”

According to Palo Alto Networks; “it’s one of the most ruthless of the dozens of ransomware gangs that we follow.”

threatpost

The ransomware gang, Hive, is known to seek out and **delete any backups** to prevent them from being used by the victim to recover their data.

BLEEPING COMPUTER



I Have Backups, So What Could Possibly Go Wrong?

This question comes up a lot, so here's a list of exactly what can go wrong!

01

What if some of the critical data was never backed up? How do you know you're backing up everything? Do you review it on a regular basis?

02

Did you test restore? What if the data that was backed up could not be restored successfully (either because the backup job was not planned correctly, or there was some undetected error, or perhaps you didn't back up critical meta data - such as encryption keys, permissions, etc)

03

Cybercriminals can compromise or sabotage the backups themselves

04

We're not backing up frequently enough and too much data will be lost when

05

We may find that the restore process is undocumented

06

We may find that the actual time to restore is much much longer than we thought (expecting hours, discovering it's days and weeks - e.g., tapes need to be shipped from over the country, and restore takes days and days.)

"While a lot of CISOs effort is directed towards prevention and detection – not enough attention is paid to securing backup environments. This is a glaring blind-spot. Organizations need to fill this major gap to secure their last line of defense."

George Eapen
Group CIO / Petrofac

Backup Attack Horror Stories

To a large extent, the ability to recover data after an attack relies on proper data protection techniques.

While these are often collectively perceived as “backup”, in most enterprises, these include: mirrors, snapshots, clones, replicas, DR, backups, and archives.

In the early days, ransomware kits would corrupt only data. They quickly evolved to also destroy operating system restore-points and snapshots. Now they’re starting to target backup systems, and central storage.

The motivation is obvious. If the recovery mechanisms are destroyed, organizations will have no other choice than to pay the ransom or give up hope of recovering their data.

Ransomware evolution aside - many news items indicate that there’s a time gap between initial malware penetration and actual damage.

For an attacked enterprise (especially, financial services organizations, nation states, and organizations with significant restricted Intellectual Property), cybercriminals may choose to let weeks or even months pass, utilizing that time to research, plan, and execute much more elaborate infiltration, including:

- *Ensuring significant portions of the IT environment are compromised (lateral spread)*
- *Infecting central management and control components (e.g., Active Directory, Central Logging systems, Management consoles, image repositories, source code libraries, etc.)*
- *Disabling data-protection mechanisms, “boobytrapping” them, or “poisoning” future data copies (see more details below)*
- *Gradually exfiltrate sensitive, proprietary, restricted, or other high-value data (e.g., personal, financial or medical records, state or trade secrets)*

(INSPIRED BY REAL EVENTS)

SCENARIO

Ransomware groups want to do everything possible to force a bank to pay a ransom.

They do this by destroying a bank's data and its backup copies – to prevent recovery of their data.

The cybercriminals compromise a bank employee's PC, and infect it with malware.

Within a few hours, they infect other employee devices, and eventually find the login details to the bank's backup systems.

The cybercriminals discover that a large portion of the backups can be deleted. However, some of the backups are stored on immutable media, which cannot be deleted.

They now decide to step it up a notch, to prevent the bank from recovering their data.

With time on their side, they begin poisoning the new backups.

They do this by gradually replacing the backed-up data with junk data.

So far, so good! The backup administrator is not alerted to the changes in the bank's backup.

The cybercriminals now wait, as the bank gradually backs-up less real data and more junk data.

After a few months, with the immutable backup files now poisoned, the attackers start to delete the rest of the backup files, stored in the regular storage.

They also begin encrypting the production data.

The infrastructure team try to restore the data, only to find that most of the backup has gone. And the only copies left are 90 days old.

All the new records, transactions, and customer information are poisoned!

The bank is left with very little choice, but to pay the ransom.

In this scenario, the cybercriminals were successful, because the bank didn't have any way to detect configuration changes to their backup, and to secure against unauthorized changes.

Cybercriminals now routinely attempt to encrypt or delete an organization's backups as part of any attack. Success for the adversary is critical here because without backups, the victim must pay handsomely to recover their data. Resilient backups are simply backups that cannot be destroyed by an adversary — even one who has acquired administrative credentials.

At the simplest level, robust resiliency can be achieved by backup to removable drives, or to tapes which are then removed from the tape library.

While immutability – whether implemented as a single, double, or triple immutable approach – is helpful in remediating cyberthreats, it is only the beginning of a comprehensive protection practice.

Recommendations

It’s time to harden your storage and backup.

Analyzing backups and data protection security posture is a new skill that IT teams must adopt in order to deal with emerging cyber-security threats.

Here are a few questions to help you check how secure your backups are:

- Do your security policies cover specific backup risks?
- Are you evaluating backup infrastructure security on an ongoing basis?
- Do you also backup the configuration of your environment (Active Directory, security settings, FW rules, device configuration, storage and backup configuration, encryption keys, etc.)?
- Do you have detailed plans and procedures for recovery from a successful attack on a storage or backup system? Do you test such procedures?
- How confident are you that your backup systems are sufficiently hardened?
- How confident are you that you can recover from a successful ransomware attack?

It is critical to evaluate existing internal security processes to determine if they cover backup infrastructure to a sufficient degree.

6 steps for success

01

Assign higher priority to improving the security of storage and backup

02

Build up knowledge and skill sets – and improving collaboration between Infosec and IT infrastructure teams

03

Define comprehensive security baselines for all components of storage and backup

04

Use automation to reduce exposure to risk, and allow much more agility in adapting to changing priorities

05

Apply much stricter controls and more comprehensive testing of storage security and the ability to recover from an attack. This will not only improve confidence, but will also help identify key data assets that might not meet the required level of data

06

Include all aspects of storage and backup management, including often-overlooked key components such as Fibre-Channel network devices, management consoles, etc.

CONTINUITY

WWW.CONTINUITYSOFTWARE.COM