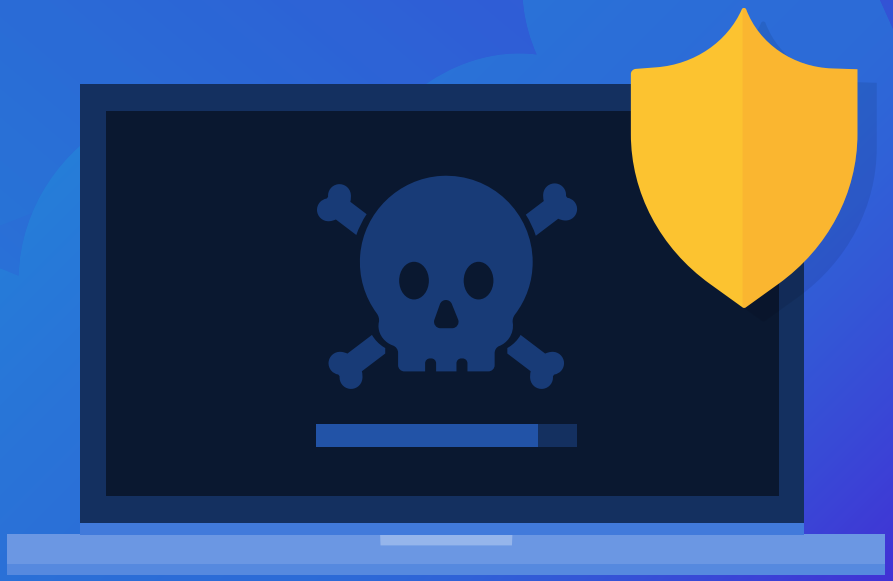
eBook

Backup Under Attack: Protecting Your Last Line Of Defense



Introduction

Your company depends on technology to power everything from payroll to your Wi-Fi network. While you see excellent productivity gains from a digital infrastructure, you are vulnerable to any situation that takes out your systems.

Did you know attacks on small and medium businesses (SMBs) amount to 28%[1] of all cyber attacks in 2020? Hackers look for vulnerabilities in networks, servers, and endpoint devices, to spread ransomware, plant other types of malware, steal user data, and more. According to the Verizon 2020 Data Breach Investigations Report, there are differences between SMBs (less than 1000 employees) and larger enterprises (greater than 1000 employees) when it comes to breaches and attacks. The most notable being that malware attacks are 2x more likely for SMBs.

The focus of this piece is backup, a component of business continuity and disaster recovery (BCDR). Why backup? Because backup is your last line of defense. If a server is infected with ransomware or critical files are deleted in error, you need a backup to restore from. However, not all backups are created equally. For example, restore times can vary widely depending on the solution you have in place. Even worse, your backups themselves may be targeted by hackers. In this piece, we'll explore proven methods that managed service providers (MSPs) are using to help ensure your backups are safe and readily available for fast restores.

It seems that for SMBs, the question of data loss is not *if* it will occur, but *when*.

How Backup Attacks Occur

The Verizon 2020 DBIR report uses the VERIS Framework to categorize threats. According to the framework, threats include:

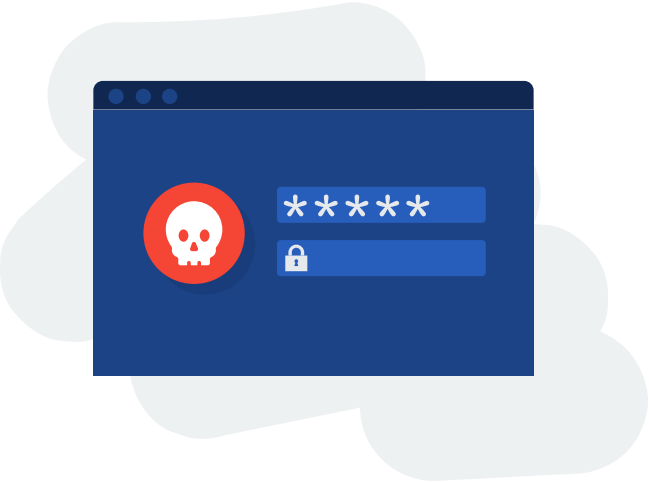
- Malware (Ransomware, viruses, etc.)
- Hacking (Stolen credentials, backdoors)
- Social (Phishing, pretexting)
- Misuse (Privilege abuse)
- Physical (Theft, tampering)
- Error (Misconfiguration, misdelivery, loss)
- Environmental (Power failures, atmospheric conditions)

While all of these can threaten backup security, we will focus on hacking, malware, and errors. According to the report, the hacking occurred in 45% of incidents, errors 22%, and malware 17%.

You don't want to face downtime without knowing exactly what your MSP is doing to bring your systems back up. Let's look at each one, its associated vulnerability, and how MSPs mitigate risk to your backups.

Hacking:

By definition, a hacker is a malicious actor who looks for weaknesses in your computer systems, applications, and networks to compromise the associated systems and/or to steal data. With regards to backup, hackers are increasingly looking at vulnerabilities in both backup software, backup files, and the systems on which backup data is stored.



Hackers have been known to steal the credentials of a backup administrator as a backdoor to access systems and data.

Backup Software: Backup software solutions, by nature, require a high level of access to files, systems, virtual machines, databases, and other aspects of a computing environment. Hackers have been known to steal the credentials of a backup administrator as a backdoor to access systems and data.

Additionally, some backup products maintain a configuration database that stores the credentials required to connect to the systems they backup. If that database is compromised, a hacker could potentially gain access to every protected system.

Backup Files: Backup files can be targets simply because backup file extensions (e.g., BAK), are easy to find. Hackers may gain access to the backup software and either turn off or delete the backup files.

Remote Access: Since many backup products must connect remotely to servers to back them up or to administer backups, using password authentication can open up a path to attack protected systems, simply because passwords are easy to steal.

Backup Encryption: It isn't uncommon for backups to be encrypted. However, if an attacker gains access to the encryption key, they can read the backup and/or change the key to make the data inaccessible. That's why it is essential to follow backup encryption key best practices such as storing the key on a separate machine, physically securing that machine, etc.

Given the importance of a solid backup and business continuity strategy, there are several best practices you should ensure your MSP is following. This will

If one system admin doesn't know what the other is doing and the storage provisioned for backups is removed or deleted, there is a problem.

allow you to screen out vendors that don't give you sufficient protection for your business continuity needs.

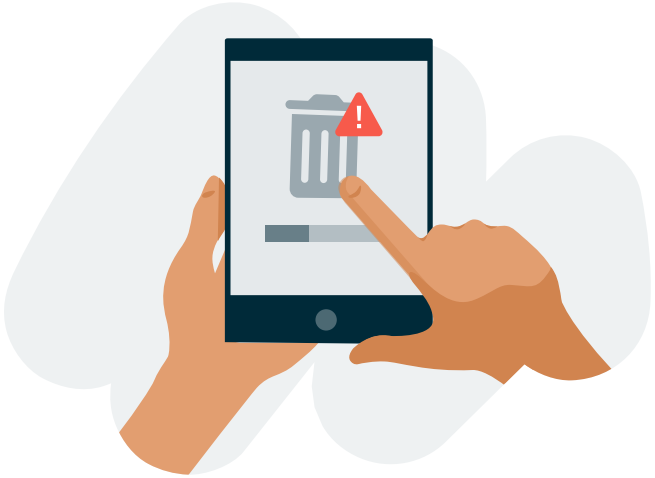
- Uses Two-Factor Authentication (2FA) to control access to the backup software portal.
- If utilizing a backup appliance ensure they cannot connect to it directly via a simple LAN connection.
- Not using passwords for remote access. Instead, they should apply key-based Secure Shell (SSH) authentication instead.
- Make sure that backup copies of your business's data are kept in a safe, secure location - preferably geographically dispersed from the primary data and backups.

Errors:

It's safe to say everyone has experienced that "on no" moment when they have deleted something they didn't mean to delete. Below you will find some common errors that can impact the ability of your MSP to quickly restore what was lost.

Backup file deletion: It is easy to find the file extension name for backups. This makes it easy for malicious actors to find them. However accidental deletion can occur as well. Since backup files can be large, there is nothing to stop someone from "reclaiming the space" used by a large backup file.

Decommission or remove storage: This is an especially important consideration in larger environments with multiple systems administrators. If one system admin doesn't know what the other is doing and the storage provisioned for backups is removed or deleted, there is a problem.



It's safe to say everyone has experienced that "oh no" moment when they have deleted something they didn't mean to delete.

Agent deletion: It's common for servers to come and go, applications to be upgraded, or even virtual machines to be moved, renamed, or deleted. Sometimes during this type of action, the backup software agent and/or entry is deleted, so those machines will no longer be backed up.

Upgrades: Step one of any upgrade is to "backup before you make changes" but what if the upgrade is the backup solution itself? Many legacy backup products rely upon catalogs or indexes of the data that gets backed up. If those catalogs or indexes are overwritten, deleted, renamed, etc. the backups themselves may be unreadable even though the backup file itself exists.

Working with an MSP you trust gives you peace of mind. But how do you know that your MSP is protected against the second most common data breach if they accidentally delete your backup?

- Uses a modern solution that provides numerous point-in-time recovery points as granular as the backups occur (5 minutes to 24 hours for example). The more copies the better!
- Implements access employee controls for backup files, limiting who can delete them.
- Replicates the primary backups. The most common restore occurs from a backup that is less than 48 hours old, so make sure they are replicating a copy of the recent backups to a secure cloud or another server within their organization.
- Protects backup catalogs and indexes from being deleted or corrupted.

Ransomware falls into the Malware category and is the second most common type of malware, according to Verizon's report.

Malware:

Even though Malware decreased overall year-over-year[2], Ransomware falls into the Malware category and is the second most common type of malware, according to Verizon's report.

Ransomware is typically distributed via phishing emails that trick a user into clicking a link or downloading an attachment that installs the malware on their system. Once the ransomware has been installed on a PC or server, it begins searching for files to encrypt. Since ransomware spreads silently, it often isn't detected for weeks, months, or even longer.

After the attackers believe they have thoroughly infiltrated the systems, they then begin encrypting files to make them unavailable to the users. Files may be permanently deleted if the ransom is not paid.

Backup Files: Backup files are just another file type, so they can be encrypted by the ransomware too. If the backup solution has been compromised, there is no way to recover other than paying the ransom. However, paying a ransom does not guarantee an organization will regain access to their data. And since the file extensions for backup solutions are easily attainable, ransomware attackers can go after those files to ensure the compromised systems cannot be recovered.

Work with a trusted MSP to give your organization the right technology strategy and IT support to help your business grow.

Your backup files may be your absolute last line of defense, so how can an MSP protect them?

- Using a backup solution that offers ransomware scanning.
- Keep backup copies offsite in a secure location.
- The more copies the better. With modern backup solutions, granular backups or "snapshots" provide multiple points in time to recover from.
- Reliable BCDR solution in place that allows your MSP to quickly recover your business operations locally or in the cloud when primary systems are compromised.

Summary

Whether it be hacking, malware, or human error, the most common ways of compromising primary data apply to backup also. Cunning attackers want to make sure that recovery of PC, servers, or virtual machines cannot be performed. That is why backup systems are now under attack.

Working with an MSP that is using a reliable business continuity solution is paramount to mitigating risks to your backup. That's why we offer **Datto Unified Continuity** to our clients. A successful business continuity solution that spans the server to the desktop with the flexibility to backup locally, direct to cloud, or both.

Key features of Datto Unified Continuity include:

- Comprehensive protection for servers, virtual machines, SaaS, and PC/Laptops
- Integrated ransomware scanning during backup
- Two-Factor Authentication (2FA) access control
- Services audited for compliance with SOC 2 security and quality standards
- Secure backup appliances that cannot be accessed locally
- Instant local recovery
- The Datto Cloud for offsite backup storage
- Geographically dispersed, replicated data centers
- Optional Infinite Cloud Retention
- Encrypted remote replication
- Optional backup data encryption
- Instant recovery of servers and virtual machines in the secure Datto Cloud
- Exclusive Cloud Deletion Defense™ to protect against accidental or malicious backup deletion
- Point-in-time image recovery

[1] Verizon 2020 Data Breach Investigations Report

[2] Verizon 2020 Data Breach Investigations Report

Business data lives in many places—servers, desktops, laptops, and cloud-based applications. Should critical files be accidentally deleted or your backups be targeted by hackers, you need to have confidence in your data protection plan.

This is why working with an MSP that provides Datto Unified Continuity is not only your last line of defense but your best defense for protecting data from hacking, errors, and malware.

Don't let the stress and burden of IT prevent you from reaching your business goals. Get in touch today if you need expert business continuity services.