

Backup Under Attack: Protecting Your Last Line Of Defense



Introduction

Attacks on SMBs amount to 28%¹ of all cyber attacks in 2020. Hackers look for vulnerabilities in networks, servers and endpoint devices, to spread ransomware, other types of malware, steal user data, and more. According to the Verizon 2020 Data Breach Investigations Report, which can be found [here](#), 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 to help ensure your backups are safe and readily available for fast restores.

“Attackers prefer short paths and rarely attempt long paths²”

How Backup Attacks Occur

The Verizon 2020 DBIR report uses the [VERIS Framework](#) to categorize threats.

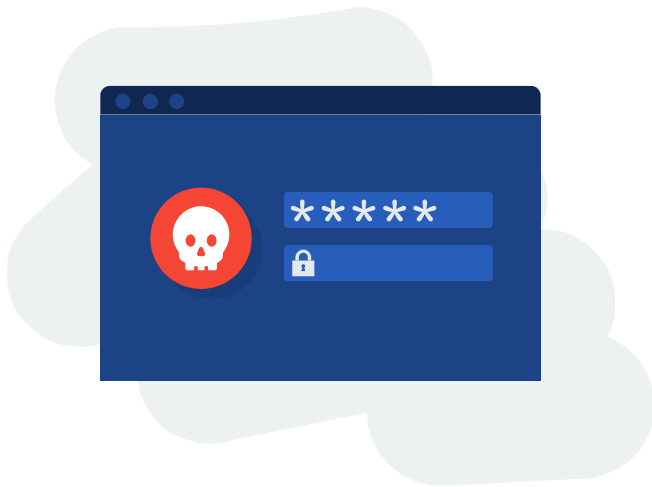
According to the framework, threats include:

- 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, for the purpose of discussion we will focus on hacking, malware, and errors. According to the report, **hacking occurred in 45% of incidents, errors 22%, and malware 17%**. Let's look at each one and its associated backup vulnerability, and how you can mitigate risk to your backups.

Hacking:

By definition, a hacker is a malicious actor who looks for weaknesses in 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. Additionally, if you are using a remote monitoring and management solution (RMM) to administer backups, this could also be a point of attack.

Backup Encryption: It isn't uncommon for backups to be encrypted. However, if an attacker gains access to this key, they have the ability to 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 secure that machine, etc.



If one sysadmin doesn't know what the other is doing and the storage provisioned for backups is removed or deleted, you've got a problem.

Given the importance of a solid backup and business continuity strategy, there are several best practices you should follow.

- Use Two-Factor-authentication (2FA) to access your backup software admin portal.
- If you utilize a backup appliance ensure you cannot connect to it directly via a simple LAN connection.
- For remote access, do not use passwords. Utilize key-based SSH authentication instead.
- If you are using a separate product to administer backups, such as a RMM tool, make sure it also has 2FA.
- Make sure that you keep backup copies in a safe, secure location - preferably geographically disperse from the primary data and backups.

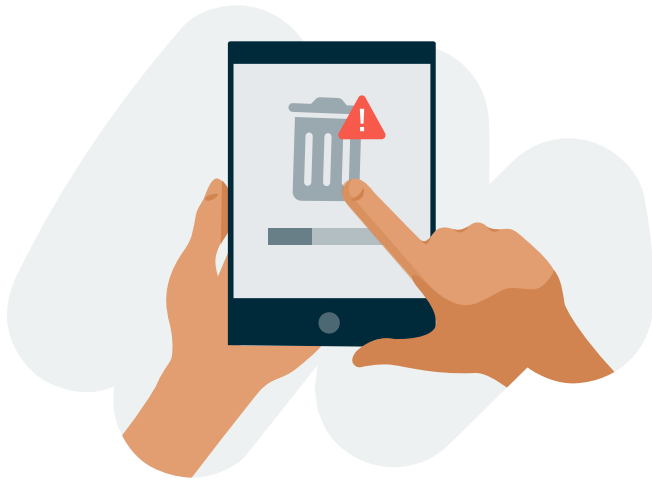
Errors:

It's safe to say everyone has experienced that "oh no" moment when they have deleted something they didn't mean to delete. Below you will find some common errors that impact your ability to restore.

Backup file deletion: As mentioned earlier, 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 sysadmin doesn't know what the other is doing and the storage provisioned for backups is removed or deleted, you've got 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 not uncommon for servers to come and go or applications to be upgraded or even a virtual machine to be moved, renamed or deleted. Sometimes in the midst of 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.

So how do you protect against the second most common data breach and keep yourself from issuing a "mea culpa" if you are the one to delete the backups?

- **The more copies the better.** Modern backup software doesn't have the problems or level of overhead legacy solutions have when it comes to backups. Most modern solutions can provide numerous point-in-time recovery points as granular as the backups occur (5 minutes to 24 hours for example).
- **Implement access controls** for backup files, limiting who can delete them.
- **Replicate your primary backups.** The most common restore occurs from a backup that is less than 48 hours old, so why not replicate a copy of the recent backups to a secure cloud or another server within your organization.
- **If you have backup software that utilizes catalogs or indexes,** be sure to back them up. Also, look for modern backup solutions that aren't as easy to corrupt.

Malware:

Even though Malware decreased overall year-over-year³, Ransomware which falls into the Malware category is on the rise and is now the second most common type of malware, according to Verizon's report.

Ransomware is typically distributed via phishing emails which then tricks 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 then begins searching for files to encrypt. Since ransomware spreads silently, it may take some time before making itself known.

After the attackers believe they have thoroughly infiltrated the systems, they then begin encrypting files that will be made unavailable to the users and possibly deleted if the ransom is not paid.

Backup Files: As discussed earlier, backup files are just another file type, so they can be encrypted by the ransomware too. If your backups have been compromised, there really is no way to recover other than paying the ransom. 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.




Ransomware which falls into the Malware category is on the rise and is now the second most common type of malware.

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

- **Be proactive and scan for ransomware during backup.** Most modern backup solutions offer ransomware scanning as an integral part of their solution.
- **Keep backup copies offsite in a secure location.** If your primary systems are compromised, including the (on-prem) local backups, you can restore your compromised systems locally or in the cloud with the untouched backups that have been stored in a secure, immutable, cloud storage repository.
- **The more copies the better.** With modern backup solutions, granular backups or “snapshots” provide multiple points in time to recover from.
- **Consider BCDR solutions** that allow you to recover business operations quickly 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, which is why backup solutions are now under attack.



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



Learn more about Datto Unified Continuity →

Datto Unified Continuity is a business continuity solution that spans the server to the desktop with the flexibility to backup locally, direct to cloud or both. Key tenets of Datto Unified Continuity include:

- Comprehensive protection for servers, virtual machines, SaaS, and PC/Laptops
- Integrated ransomware scanning during backup
- 2FA to access the Datto Portal to administer backups
- Secure backup appliances that cannot be accessed locally
- Instant local recovery
- The Datto Cloud for offsite backup storage
 - Secure, 2FA access and SOC II compliance
 - Geographically distributed data centers for security and data sovereignty
 - Optional Infinite Cloud Retention
 - Encrypted remote replication
 - Optional backup data encryption
- DRaaS instant recovery in the Datto Cloud
- Exclusive Cloud Deletion Defense™ to protect against accidental or malicious backup deletion
- Point-in-time image recovery

Business data lives in many places—servers, desktops, laptops, and cloud-based applications. This is why [Datto Unified Continuity](#) is not only your last line of defense, but your best defense for protecting data from hacking, errors

¹Verizon 2020 Data Breach Investigations Report

²Verizon 2020 Data Breach Investigations Report

³Verizon 2020 Data Breach Investigations Report