ATEMPO preserving data ecosystems

Modern Data Protection Opportunities & Risks

Ensure business continuity for all your workloads

DATA PROTECTION

An Atempo Tech Paper

One Ransomware attack every **11 seconds** in 2021 (Cybersecurity Ventures)

By 2025, **40%** of all enterprises will require ransomware defense mechanisms (Gartner)

Cybercrime cost in 2021 = **€6,000 billion**. Covid-19 = €9,400 billion (Cybersecurity Ventures - World Bank)

44% of entry point attacks are through phishing Email, malicious links (Data protection trends 2022)

Businesses today must deal with economic crises, global pandemics, ever-changing regulations, and cybercrime.

Increasingly sophisticated ransomware attacks are specifically targeting backup data and administrator functions. AI-based spear phishing and hybrid work - the cyber threat landscape remains tense. Cybercrime-as-a-service is becoming a major business model, and criminal tactics are evolving by the minute. Microsoft 365 is not immune to these cyberattacks. Ultra secure with strong authentication and data encryption, Tina respects industry best practices such as 3-2-1 backup strategy.

Attacks can come from two directions:

- External threats: Hackers attacking the company from the outside, usually for money, but sometimes for political or other reasons. Attacks launched from outside seek to gain access to the network through stolen credentials, software breaches or backdoors.
- Internal threats: Employees cannot be ignored as a threat. In some respects, internal attacks are easier to mount as the attacker already has access to the network and does not need to breach firewalls, even if privilege escalation may still be required.

To prevent risks in hybrid environments, a key requirement is to build security into every stage of software development. A secure-by-design backup solution must meet a couple of requirements:

COMPANIES SHOULD DEVELOP A ZERO TRUST SECURITY CULTURE

Atempo has security teams involved during the whole development process and their duty is to align people, processes, and technology to minimize software risk.

The security teams are actively involved in implementing ISO 27001 standards and in the continuous improvement process.

Another aspect of their job is to follow the latest cybersecurity technology trends and security reports highlighting the latest attacks, subscribe to RSS feeds and organizations such as ANSSI (The National Cybersecurity Agency of France) as well as participate in industry security events (such as the FIC: International Cybersecurity Forum).

A SECURE-BY-DESIGN BACKUP SOLUTION

Security by design is an approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as architecture analysis, continuous testing/penetration testing, authentication safeguards and adherence to best programming practices (such as static code analysis for instance).

For modern web-based backup solutions, such as Atempo Data Protection, security teams respect OWASP Security design principles created to help developers build highly secure web applications. Security teams are focused on applying all Security principles.

We all remember the recent attack on the US based Managed Service Provider which is estimated to have infected up to 2000 global organizations with ransomware. The ransomware targeted a vulnerability in the MSP remote computer management tool to launch the attack.

We see in this example that MSPs can be efficient vehicles for ransomware because they have wide access to many of their customers' networks. This is why Secure-by-design matters for a software provider.

LINUX OS FIRST

Linux systems are rarely infected by malware such as viruses, worms etc., thereby making it as a very secure OS.

Even though security is a very fast evolving topic, the open source nature of Linux enables the frequent release of security patches. In addition, some of Linux features such as memory management, user/kernel memory space separation, virtual memory, log management and file access control make it even more secure. Atempo Data Protection is designed to work with Linux which, when we follow architecture best practices, makes it a very secure solution. Keep in mind that to ensure a high level of security the Linux OS and Atempo Data Protection must be upgraded with the latest patches to avoid any risk of a security breach.

ARCHITECTURE YOUR BACKUP SOLUTION TO RESPECT SECURITY BEST PRACTICES

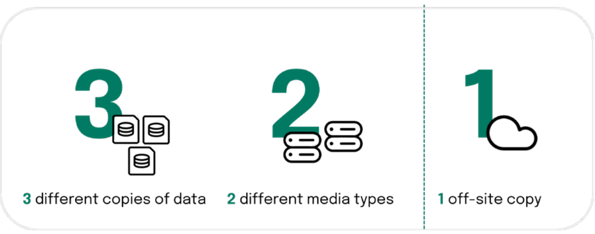
When it comes to configuring your backup solution in hybrid environments a couple of best practices must be taken into account.

- Isolate your backup service and make sure you server is hidden from your Active Directory. Making it invisible avoids risks from ransomware attacks.
- Restrict the number of users that can access your backup servers, and always use secured, encrypted communication between servers and any storage nodes.
- Limit physical access to data backups. However you choose to store your data backups on the server, NAS, tape or cloud, be sure the access is controlled in those

facilities. Encrypt your backups; encryption implemented and managed in the right way serves as an excellent layer of defense.

RESPECTING INDUSTRY BEST PRACTICES AND COMPANY USER DEFINED SECURITY RULES

One of the backup industry's best practice is the 3-2-1 rule. This rule states that you should have 3 copies of your data on two different media (disk and tape for example) with one copy off-site for disaster recovery. The 3-2-1 backup strategy emphasizes the importance of the application of Air-Gapped Protection.



Atempo Data Protection is flexible enough to comply with industry best practices while adjusting to each company specific needs to their own security strategy. For instance, by adding object lock or WORM Tapes as part of the backup strategy.

INCLUDE YOUR BACKUP SOLUTION IN YOUR DISASTER RECOVERY STRATEGY

Data backups can be compromised or destroyed in situations such as a ransomware outbreak, an employee break-in or a natural disaster such as a flood or hurricane. You must have a plan outlining what you are going to do if that time comes. Atempo Data Protection's replication feature helps mitigate the disaster risks and enables the continuity of your backup service.

PRIVILEGE CONTROL

Backup solutions should be able to define precise Role Based Access Control (RBAC) for users to respect the Principle Of Least Privilege (POLP). This principle states that a user should have the minimum set of privileges required to perform a specific task. Atempo Data Protection Solution provide multi-factor authentication (MFA) to increase users data access control.

RESPECTING VENDOR STANDARDS

Atempo technology respects vendor standards guaranteeing protection and recovery. For instance, we respect Microsoft recommendations to use the latest APIs to back up and restore data from the Microsoft 365 Tenant. Atempo Data Protection only uses Microsoft Graph APIs rather than Exchange Web Services APIs (EWS). Microsoft strongly urges partners to use Microsoft Graph APIs when accessing Exchange Online data. It is frequent to find solutions on the market still using EWS APIs for backup and recovery.

.

Atempo Data Protection Zero trust adoption has accelerated its response to the rapid rise of mobile and remote workers. While these trends benefited users and brought new levels of flexibility to IT, they also reduced the ability of the organization to control and secure access to data and network resources. Zero trust brings this control back, tightening up security in the face of permeable network perimeters.

The flexibility of the solution enables a continuous security improvement process and comes with constant innovation to protect and monitor your data.

Update: 03/09/2024