tributech

The Key to Resisting Ransomware Attacks

Safeguarding Data Integrity

In today's digital age, the threat of ransomware looms large over organizations of all sizes and industries. The alarming surge in ransomware attacks has left businesses vulnerable to significant financial losses, reputational damage, and operational disruptions. To combat this growing menace, it is crucial for companies to set up relevant technologies and processes before an attack and therefore minimize negative business impact.

In this whitepaper, we will explore how data integrity protection, when used in conjunction with robust backup solutions and comprehensive data security tools, strengthens defense against ransomware and significantly reduces damage.

INTRODUCTION

Data integrity refers to maintaining the accuracy, consistency, and reliability of data over its entire lifecycle. Adding data integrity protection to backup solutions, and data security tools can form a powerful trio in the fight against ransomware attacks. As organizations face an increasing threat of data breaches, it is essential to understand the relevance of combining these three elements to safeguard critical information. This powerful combination of tools is also highlighted by the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST). They are actively engaged in helping organizations address the challenge of ransomware and other data integrity events. The NIST Special Publication 1800-26 is a series of practice guides focusing on data integrity and the relevance for ransomware and other destructive events.

Data integrity protection forms the foundation of a robust ransomware defense strategy. It involves implementing a comprehensive set of security measures to safeguard data from unauthorized access, modification, or deletion. We will outline how data integrity protection can be incorporated within a company's security landscape following the five functions of the Cybersecurity Framework Version 1.1 published by NIST:

- Identify
- Protect
- Detect
- Respond
- Recover

Identify & Protect: Understanding the Value of Data Integrity & Fortifying Data Integrity Defenses

Before an organization can effectively protect its data from ransomware attacks, it must first identify and comprehend the value of its critical (data) assets. By assessing the importance and vulnerability of data, organizations can prioritize their protective measures accordingly. Identifying critical data sets ensures that the most valuable information is shielded from potential ransomware threats and therefore from the threat of data corruption and destruction.

To protect these assets, it is necessary to establish baselines of all relevant data which allows the monitoring of any change to the integrity of the data and therefore any adversarial manipulation.

Additionally, implementing automated and regular backup procedures in concert with the integrity monitoring helps to establish trust in data when it needs to be recovered.

Detect & Respond: Timely Threat Detection is Crucial

Ransomware attacks can rapidly evolve, making early detection vital to minimize the potential impact. Implementing robust monitoring and detection mechanisms help organizations respond promptly to any signs of compromise.

Having an intrusion detection system (IDS) or advanced endpoint security solution (EDR) in place is a valuable starting point in protecting a company against ransomware attacks. However, there are several scenarios where this protection is not enough:

- if your existing security tools are not configured correctly
- Known or zero-day vulnerabilities that can be used by attackers to bypass existing security controls
- adversarial manipulation from insiders or social engineering attacks

Additionally, if intruders manage to gain access to a company's IT or OT infrastructure, they also have the opportunity to manipulate or fake data without the existing security measures noticing.

Therefore, it is key to use the advanced monitoring functionalities of data security tools and implement an end-to-end data integrity protection. This enables the company to detect anomalies in the access, use or modification of data at an early stage.

A seaming-less integrated data integrity monitoring can immediately detect data tampering within the relevant assets and provides an additional early indicator of a cyber-attack. The challenge is to establish an end-to-end monitoring across complex data pipelines and also across different system layers. Otherwise, this leaves an open door for intruders to tamper or „poison“ important information.

This is especially relevant in combination with SIEM tools, where log integrity monitoring is crucial to immediately identify if log tampering has been used to hide the traces of an attack (See Blog Post: Log Data Integrity).

To respond to an integrity attack, it is important to provide the security teams with all relevant information immediately. Therefore, data integrity monitoring tools and data security tools need to be able to provide detailed and fine-granular information of the tampered data and what error occurred (tampered origin, integrity, etc).

The Forensics/Analytics capability also uses the provided details to discover the source and effects of any destructive event on data and enables security teams to

1) limit the impact of a destructive event on the organisation and its data, and
2) make the necessary changes to prevent similar events in the future.

When these components work together, security teams and their tools are enabled to detect a loss of data integrity and respond to the event immediately.

Recover: Data Integrity Restoration and Business Continuity

Despite robust preventative measures, ransomware attacks can sometimes succeed. In such cases, the ability to recover data swiftly and accurately is crucial.

In order to recover from a loss of data integrity, an organization must have taken action already before the ransomware attack occurred. One crucial capability to have in place is the ability to backup data, in order to store copies that an organization has prioritized. This allows companies to restore compromised data from non-compromised previous versions in existing backup files. For a successful recovery it is key to start the data integrity monitoring as close to the source as possible and establish an end-to-end integrity protection. Only using the integrity protection of data backup solutions leaves an open attack vector between the initial data source and the time when it is backed up. This can negatively influence operations although a successful recovery from a backup was possible.

This requires organizations to prioritize the following steps during the recovery process:

1) Isolation and Containment: Immediately isolate affected systems to prevent the spread of ransomware within the network. Disconnecting compromised systems from the network limits the damage inflicted.
2) Secure Data Restoration: With regular backups, organizations can restore their data to a pre-attack state. Verifying the integrity of backups is essential to ensure the restored data is tamper-proof and free from malware or adversarial manipulation. With a fine-granular identification of the tampered data only affected data needs to be restored or sorted out, which reduces the amount of lost data and also speeds up the recovery process, saving valuable time and resources.
3) Incident Response and Forensics: Conducting a thorough investigation after an attack helps identify vulnerabilities, determine the root cause, and refine security measures to prevent future incidents. Sharing information with law enforcement agencies can aid in apprehending the attackers. Having the ability to use tamper-proof logs for digital forensic increases the possibility of finding vulnerabilities and ways how an attacker could hide his traces.

These capabilities, combined with their roles before an event has occurred, allow an organization to appropriately recover from a loss of data integrity.

Why data backup tools and data security solutions are not enough

In today's digital world, it's vital for businesses to back up their data. That's why they often rely on backup solutions from leading companies like Rubrik, Acronis, and Veeam. These companies help businesses keep their data safe and ensure everything can get back to normal quickly if there's a data loss or cyberattack.

In addition to that, data security tools provide a range of features to address various data security challenges. One of their core functionalities is to identify and classify sensitive data, allowing companies to understand where it resides, who has access to it, and how it's being used. By monitoring user behavior and file activity, Varonis helps detect and alert on potential insider threats and external cyberattacks, enabling timely incident response and mitigation.

Both solutions leave an open gap – the end-to-end integrity monitoring of data and logs. Having the possibility of monitoring data origin and integrity across system layers and across the whole lifetime of the data provides the needed end-to-end protection needed for an increased resiliency against ransomware attacks.

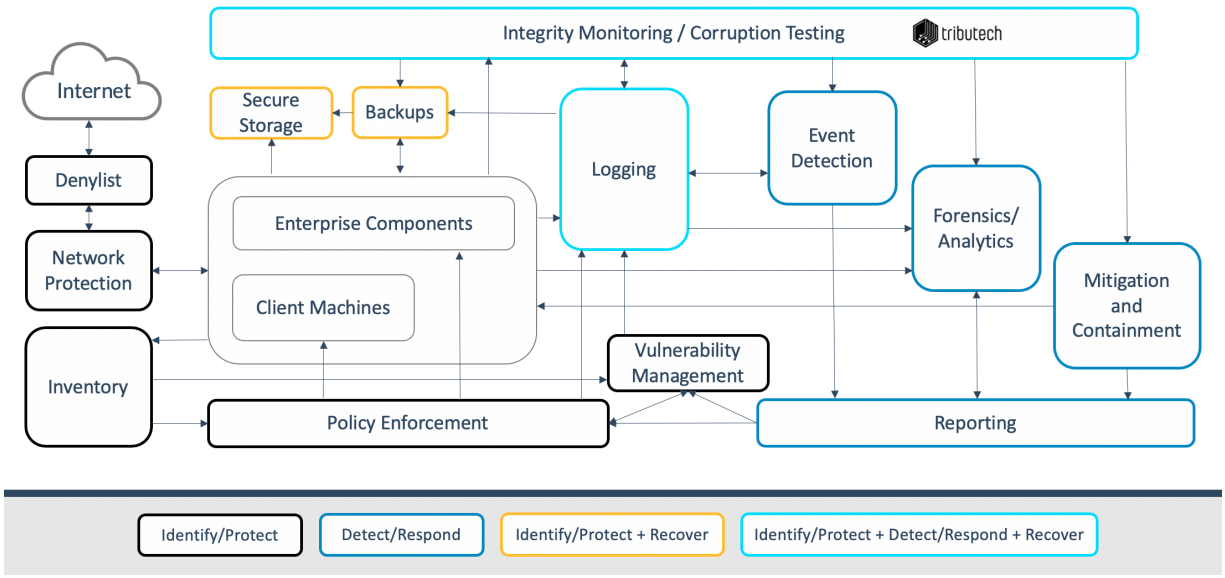
How Tributech can increase a company's resiliency against ransomware attacks

Tributech's data notarization technology adds unique data protection by ensuring data integrity across the whole lifecycle and also across system layers. Especially in conjunction with other security tools it significantly increases the resiliency against cyber-attacks targeting a company's most valuable asset – the data.

This additional monitoring and protection capabilities can easily be added to a company's security tools and provide a notarized and verifiable data foundation – no matter if it is used for device data from an OT environment, log data, or data from applications or a database.

The benefits that increase the resilience against ransomware attacks are

- Integrity monitoring of all relevant data within a company
- Data integrity protection starting at source adds value for backup strategy
- Immediate detection of data tampering
- Fine-granular details for forensic analysis
- Advanced log data integrity monitoring
- Recovery of only tampered data necessary



Reference architecture for Integrity Monitoring based on NIST1800-26
Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf

Conclusion

As the frequency and sophistication of ransomware attacks continue to rise, safeguarding data integrity becomes paramount for organizations of all kinds. By adopting a proactive approach that encompasses the stages of identify, protect, detect, and recover, businesses can bolster their resilience against ransomware threats.

Identifying critical data assets lays the foundation for effective protection. Employing a multi-layered security approach, including an end-to-end data integrity monitoring & protection enables a timely detection of ransomware activities.

Remember, data integrity protection is not a one-time effort but an ongoing commitment. By prioritizing data integrity at every stage, implementing robust backup solutions, and leveraging comprehensive data security tools, organizations can significantly enhance their resilience against ransomware attacks. Together, these elements form an interconnected security system that safeguards critical information, protects reputations, and enables business continuity in the face of ever-evolving cyber threats.