PACKETFABRIC

Ransomware and Data Protection Best Practices

PACKETFABRIC

The Rise of Ransomware

Data protection has always been a top priority for IT teams, but the rise of ransomware attacks during the pandemic have made data protection simultaneously more urgent and complex. While IT and business operations teams were focused on getting increasingly cloud-based and Internet-delivered infrastructure and applications working to accommodate remote work, the criminal world took advantage of the increased digital attack surface. Ransomware has been growing since its invention in 1989, but 2020 was the worst year by far, with 2021 not far behind. Some illuminating statistics from Crowdstrike, IBM Security and Heimdal Security as aggregated by Atlas VPN[1].

56% OF ORGANIZATIONS WERE TARGETED BY A RANSOMWARE ATTACK IN 2020

THE AVERAGE PAYOUT PER ATTACK WAS $1,100,000

RANSOMWARE MADE UP A WHOPPING 81% OF ALL FINANCIALLY MOTIVATED CYBER ATTACKS IN 2020

Dual threats from Ransomware

In its baseline form, the simplicity of a ransomware attack is its genius. Ransomware can create devastating damage without actually stealing or removing any data. A relatively minor slip up in an organization's security systems, due to an employee that succumbs to a phishing attack, can unleash a worm which busily encrypts crucial data systems and locks up business operations, rendering them unusable until the ransom is paid and the unlock code is applied.

But the denial of service angle isn't the only threat from ransomware. Many ransomware variants such as Maze, Shade, and Nemty also copy pre-encrypted data to attackers' servers, creating additional ransom leverage for attackers based on the threat of releasing sensitive data on the Internet that can trigger huge regulatory fines. For example, a Maze attack on the City of Pensacola led to the release of Gigabytes of data on the Internet.

PACKETFABRIC

Going beyond physical data protection techniques

Data protection has traditionally focused on data loss or in accessibility due to physical disruptions such as power outages, extreme weather, terrorism and civil unrest, network connectivity cuts, and damage to spinning disks. This includes such aspects as:

Automated Backups

Creating robust and frequent backups of critical data, orchestrated by backup software or SaaS solutions.

Duplication

Geo-replication of data so that no one location holds all the critical data. The data is automatically and systematically duplicated in geographically diverse locations – preferably 1000 miles or more apart.

Redundancy

Including techniques such as disk mirroring/parity to provide basic protection against single device failures. This also includes more advanced techniques such as erasure coded system, distributing data amongst multiple discs so no one failure or bit corruption can damage your data. Good storage erasure encoding offers 8+3 protection (an extra 3 data blocks used to protect an original 8 data, thus allowing recovery with up to 3 failures), which offers eleven nines of data durability.

While all of the above techniques are critical aspects of data protection, increased measures are needed to ensure data accessibility and privacy in the face of the rising ransomware threat.

PACKETFABRIC

Multi-Layer Data Protection

Organizations need multi-layer ransomware data protection as part of a comprehensive backup and business recovery plan. Two key elements are the isolation and protection of systems against attack; and sound Recovery Point Objective (RPO) and Recovery Time Objective (RTO) planning for such attacks using a combination of online, nearline and offline backups.

Systems to be covered by the protection and recovery plan include:

- ✓ Websites, communication, and other business systems, which should be isolated from other systems and protected via traditional backups.

- ✓ Database, file systems, and file servers that are critical dependencies for web and other business systems using modern cloud or hybrid file systems enables data to be replicated to the cloud and versioned to protect copies of data against ransomware. Further, most modern cloud or hybrid file systems allow recovery back to any specific time - allowing data to be recovered from a point before it was compromised.

- ✓ Laptop/desktop machines - Local storage is particularly vulnerable, since phishing is the most common ransomware attack vector. Aside from security practices and techniques to prevent ransomware, there are various data protection strategies ranging from policies that discourage use of local storage to enforced cloud-based backups.

Plan and communicate

Your RTO/RPO and business impact analysis provide the foundation for understanding your data protection requirements. You can then identify, evaluate and choose data protection strategies to achieve the RTO/RPO, to be integrated into your business continuity plan and cost model. The data protection plan and design enables the IT organization to clearly communicate risks along with required protection coverage and budget to business decision makers.

Encrypt end-to-end

A fundamental element of ransomware protection is end-to-end encryption. By encrypting data-in-flight and data-at-rest, you assert multiple layers of protection. First, encrypting all data makes it harder for ransomware attacks to identify the most sensitive data. Second, it prevents malicious software or systems acting as a man in the middle to collect data as it is used/moved around the network. Lastly, it also prevents ransomware criminals from threatening to expose your data publicly, should they be able to successfully penetrate your systems. The “key” to this strategy is to store and encrypt your data encryption keys in a separate location, to achieve encryption key decoupling. This prevents attackers from accessing your encrypted data and keys in the same data store.

Leverage immutability and versioning

An immutable backup means that the copy of your data is fixed, unchangeable, and can never be deleted. Not by a rogue employee, a ransomware attacker or a simple mistake. Once you have stored an immutable backup it cannot be altered or changed and that gives you the confidence to know that ransomware cannot delete or encrypt your immutable copies and hold you hostage to them. Data immutability is supported by some, but not all cloud storage providers.

Immutable backups take many forms. For example, a single immutable copy of data can be backed up at a specific point in time. Modern backup systems utilize versioning and other techniques to offer greater flexibility and speed via point in time recovery to reclaim versions of data from just before an attack.

The trade-off of maintaining immutable and/or potentially versioned copies of your data is simply that you need to absorb additional storage costs. Given the immense expense of a successful ransomware attack, this additional expense is worthwhile.

Create Decoys

In response to the explosion of ransomware exploits, the FBI has reportedy adopted a new policy as part of their IDLE (Illicit Data Loss Exploitation) program. IDLE recommends that organizations that are targeted or under attack by ransomware criminals (i.e. everyone) should create decoy batches of data that make it harder for attackers to identify true high-value data.

PACKETFABRIC

PACKETFABRIC

Secure Cost-Predictable Hyper-Connected Cloud Storage

PacketFabric Space offers globally distributed, secure, high-performance S3 object storage, connected by the 50Tbps+ PacketFabric NaaS. The Space platform offers automated geo-replication, 8+3 erasure encoding, end-to-end encryption, versioning and data immutability.

PacketFabric Space supports AWS-compatible S3 WORM (Write Once, Read Many) APIs and capabilities for object governance, compliance and legal-hold. Space supports S3 versioning and object locking. Object locks allow for either retention periods and legal hold (indefinitely enforced until explicitly withdrawn), or both concurrently. Object lock retention modes can be set on a per object bucket, or as a default policy for all object bucket creation.

This is a core component and part of any Cloud Backup and Business Recovery plan. Those plans need to use other systems and components as well. PacketFabric can help you work on your business continuity planning and recommend partners who would also be able to help.

LEARN MORE ABOUT PACKETFABRIC SPACE AT

https://www.packetfabric.com/cloud-storage