EVERYTHING YOU WANTED TO KNOW ABOUT

SECURING YOUR STORAGE,

BUT WERE AFRAID TO ASK

CONTINUITY SOFTWARE

Background

Data-targeted attacks have been in the public eye for quite a while now, with Ransomware damage costs predicted to grow more than 57X from 2015 to 2021*.

GROWTH IS PROPELLED NOT ONLY BY THE SURGE IN THE NUMBER OF CYBERCRIME GROUPS SPECIALIZING IN RANSOMWARE, BUT TO A LARGE EXTENT, ALSO BY THE CONTINUAL INCREASE IN ATTACK SOPHISTICATION. RANSOMWARE HAS EVOLVED INTO A FULLY-FLEDGED INDUSTRY, WITH COMPETING GROUPS THAT CONTINUALLY INTRODUCE NEW CAPABILITIES AND TECHNIQUES.

Some of the new trends in data crimes, such as data leak, threat of data exposure and shaming techniques have ignited the media attention, though other, potentially even more devastating are still not widely discussed, which we'll attempt to correct here.

> My prediction for the remainder of 2021 is that there will continue to be more ransomware attacks. It's not exactly a radical statement.
>
> I didn't see a ton of it last year, during COVID, but this year it has been absolutely crazy. I can't tell you how many emergency incident response phone calls and Teams meetings I've had this quarter. I've probably had as many this quarter as I had the whole of last year. So my prediction for this year is much more of the same.
>
> 
>
> serco **Garrett Smiley**
> CISO

Conceptions and misconceptions

A significant portion of the discussion nowadays revolves around ransomware prevention – pointing out common attack vectors, and reviewing means to identify and neutralize attacks.

WHILE AN OUNCE OF PREVENTION IS INDEED WORTH A POUND OF CURE, FOCUSING THE DISCUSSION ON PREVENTION CAN ACTUALLY BE DETRIMENTAL TO A BALANCED DEFENSIVE POSITION (IF HISTORY IS ANY GUIDE, THEN THE FRENCH RELIANCE ON THE MAGINOT LINE IN WWII, CAN DEMONSTRATE THE SHORTCOMINGS OF SUCH APPROACH).

The working assumption must be that an attack can succeed, and proper secondary lines of defense must be put in place to guarantee recovery, especially in view of the following alarming signs:

Surveys indicate a high probability of being attacked **(51% of surveyed organizations were attacked in the last 12 months**)**

More than half of businesses are not confident in their ability to recover from ransomware

A high percentage of attacked organizations choose to pay the ransom

Average cost of recovery is growing YOY, regardless of whether one chooses to pay the ransom or not

Initial recovery typically takes days, while full recovery can take weeks – during which business operations could be severely impacted

> Most ransomware attacks still happen due to vulnerabilities: not enough patch management, not following basic security requirements, and not having basic controls. All of this leads organizations to fail.
>
> 
>
> Standard Chartered **Erdal Ozkaya**
> Regional CISO

Introducing 'backup-targeted attacks'

To a large extent, the ability to recover data after an attack relies on proper data protection techniques. While these are often collectively perceived as "backup", in most but for the very small organizations.

These include, by order of importance: mirrors, snapshots, clones, replicas, dr, backups, and archives (many other solutions exist).

In the early days, ransomware kits would corrupt only data. They quickly evolved to also destroy operating system restore-points and snapshots. Now they're starting to target backup systems, and central storage.

Motivation is obvious. If the recovery mechanisms are destroyed, organizations will have no other choice than to pay the ransom or give up hope of recovering their data.

The gap explained

IT is a combination of infrastructure, configuration, and code – all of which are susceptible to attack (admittedly cloud technologies can sometimes blur the boundaries between configuration and code, or between configuration and infrastructure).

Zooming in on infrastructure, reveals a further division into compute, network, and storage (some also add facility and environmental controls). Significant progress has been made over the last two decades in increasing the security of the network, compute, and code layers.

However, security innovation for storage and data protection remains low, especially for solutions aimed at the large enterprise. This is under the assumption that they are far too deep in the datacenter core to reach, and far too obscure to pose a meaningful attack surface.

WITH THE ASSUMPTIONS NOW PROVEN WRONG BY CYBER CRIMINALS, CISOS NEED TO CLOSE THE GAP.

Unlike an attack on individual endpoints or servers, which can be highly inconvenient to a large enterprise, one that targets central storage or backup can be truly devastating. This is because a compromise of a single storage fabric can bring down thousands of servers.

Furthermore, while recovery of an individual server is relatively straightforward, recovery of a storage fabric is a complete unknown to most CISOs.

Finally, far too often, the actual data, and its recovery copies are kept without sufficient isolation. Think about storage arrays that keep both the primary data and snapshots, or admin accounts that are used to manage both servers and backup.

The gap is also cultural – many CISOs and their teams are not sufficiently familiar with storage, and many storage professionals are not sufficiently security savvy. Security and storage teams are not as versed in working together, as, say, security and network, or security and server teams.

Regulation and industry awareness

Regulators are increasingly paying attention to systems and data recovery. In response, organizations, particularly in the banking & financial services sector, are investing more and more efforts in defining, measuring, and continually improving security controls for data storage and data protection.

Industry awareness is also steadily growing. In 2020, NIST released a Special Publication 800—209, titled "Security Guidelines for Storage Infrastructure", that places significant emphasis on securing and protecting data against attacks.

> The hackers are after our data. In a bank, data is money. This is why I'm a big believer in securing storage
>
> 
>
> Standard Chartered
>
> **Erdal Ozkaya**
> Regional CISO

What is data storage security, and why is it important

Ransomware evolution aside - many publications indicate that there's a time gap between initial malware penetration and actual damage.

For an attacked individual or a small organization, the gap is typically several days. However, when the target is more lucrative (e.g., a financial services organization, nation state, an enterprise with significant restricted Intellectual Property), attackers may choose to let weeks or even months pass, utilizing that time to research, plan, and execute much more elaborate infiltration, including:

- Ensuring significant portions of the IT environment are compromised (lateral spread)
- Infecting central management and control components (e.g., Active Directory, Central Logging systems, Management consoles, image repositories, source code libraries, etc.)
- Disabling data-protection mechanisms, "boobytrapping" them, or "poisoning" future data copies (see more details below)
- Gradually exfiltrate sensitive, proprietary, restricted, or other high-value data (e.g., personal, financial or medical records, state or trade secrets)

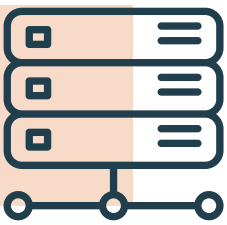
What are some of the storage-specific security challenges, and why do they differ from network and compute security

NIST SP 800-209 provides a detailed overview of storage systems threats, risks, attack surfaces and security recommendations.

While some recommendations are similar to those available for the entire IT infrastructure (e.g., physical security, authentication and authorization, change management, configuration control) other are unique to storage systems, including storage networking (which can be radically different than server networking), and areas of operations related to data protection, data isolation, restoration assurance and encryption.

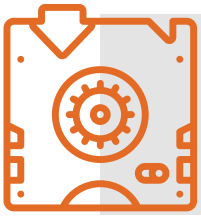
SOME OF THE MORE EXOTIC TACTICS DISCUSSED WOULD INCLUDE:

Compromising storage operating systems, firmwares and drivers. These attacks will rarely be detected by existing vulnerability detection tools, which offer limited (or no) support for storage systems and networks



Exploiting overlooked attack surfaces – from the most obvious storage array factory accounts that are sometimes not removed during installation, to more elusive ones including: servers that can send storage arrays commands through Fibre Channel devices, Roles that can manage both servers and backup systems, unaccounted for Storage API and management servers, various VM appliances that cached store storage management credentials, etc.

Poisoning snapshots and backups. Even when an attack does not succeed in corrupting existing storage and backup systems (e.g., when immutable storage is used), it may still find a way to suspend of corrupt future snapshots or backups. It's then just a matter of waiting long enough before locking production data. By that time, the only remaining valid copies may be too old for any practical use. Most organizations do not test recoverability frequently – so such attacks are likely to go unnoticed



More surgical poisoning tactics could involve compromising backups of operating systems, containers, and application images – thereby constituting a "boobytrap". During recovery from ransomware, the environment might be immediately re-infected.

> Storage is where our core data is stored. And so, vulnerability management, configuration management, and ensuring a strong policy around the governance of all storage devices are absolutely critical
>
> 
>
> HSBC
>
> **Sunil Varkey**
> Global Head of Cyber Security Assessments

Summary and recommendations

In a large enterprise, data storage tends to be a security blind-spot. Analyzing data storage and data protection security posture is a new skill that IT teams must adopt in order to deal with emerging cyber-security threats.

It is recommended to evaluate existing internal security processes to determine if they cover storage infrastructure to a sufficient degree. Some questions you could ask, include:

- Do our security policies cover specific storage, storage networking, and backup risks?
- Are we evaluating storage infrastructure security on an ongoing basis?
- Do we have detailed plans and procedures for recovery from a successful attack on a storage or backup system? Do we test such procedures?
- How confident are we that our storage systems are sufficiently hardened?
- How confident are we that we can recover from a successful ransomware attack?

If needed, third parties and vendors could be consulted, or invited to be involved in such evaluation. Based on the findings, we recommend:

Determining if knowledge gaps exist, and building a plan to address them

Improving security program to address identified gap

Considering the use of automation to continually evaluate the status of storage infrastructure security, in order to proactively address risks.

Finally, we encourage you to learn more about storage security. A good start could be the NIST Guide for Storage Security – co-authored by Continuity Software.

This guide provides CISOs and Heads of Storage with an overview of the evolution of the storage technology landscape, current security threats, and a set of practical recommendations.

CONTINUITY
SOFTWARE