CONTINUITY

Storage security related attacks, news, guidelines and more

Over 13K iSCSI storage clusters left exposed online without a password | ZDNet
Attack on iSCSI storage

US says cyber hack poses ‘grave risk’ to critical infrastructure | Financial Times (ft.com)

> The agency also confirmed reports that, once inside a victim’s networks, the hackers were able to pose as other accounts and gain privileged access to certain systems, such as email services, travel services and file storage services.

Offline backups in an online world - NCSC.GOV.UK
Cognizant Hacked, Customers Affected, Maze Ransomware Named (techmonitor.ai)
The NCSC has seen numerous incidents where ransomware has not only encrypted the original data on-disk, but also the connected USB and network storage drives holding data backups

Oklahoma gov data leak exposes FBI investigation records, millions of department files | ZDNet
…the open storage server belonged to the Oklahoma Department of Securities (ODS)

What Happens When A Company Gets Hacked? | Built In
The client wrote that he had come across LNK files in his company’s network attached storage (NAS) — a telltale sign of a rogue AutoIT worm

Security Incident on November 13, 2020 (liquid.com)
In due course, the malicious actor was able to partially compromise our infrastructure, and gain access to document storage

WannaCry NHS attack - lessons for data recovery strategies | PublicTechnology.net
NHS story: Historically, there was little risk to backups themselves, yet ransomware adds a new dimension that threatens and attacks not just the data, but also the backups, as was the case with the WannaCry attack

Babuk Locker (cyberint.com)
Demonstrating the active development, the threat actor identity 'biba99' posted a message on 'RaidForums' (Figure 1), an online forum popular with cybercriminals, suggesting that a '*nix' version is being made available that could target NAS devices and VMware ESXi virtualization hosts alongside the already supported Windows hosts.

Pay2Key Ransomware Joins the Threat Landscape - Security Boulevard
The game developer apparently was given an extension, but to prove they had stolen data the attacker released information pertaining to the victim’s NAS servers and then released a supposed finance-related folder. In both cases, the attackers alleged to have hundreds of gigabytes of data.

2015 but an interesting read – anatomy of an attack for real, step by step, not a marketing effort
A High Performance Computing Cluster Under Attack: The Titan Incident (sagepub.com)
(Involving storage too)

External Audit report – example
Final Audit Report Federal Information Security Mondernization Act Audit Fiscal Year 2020 (opm.gov)
Baseline is a key item

Another Ext. Audit report example
OFFICIAL DFC FY20 FISMA Final Report - A-DFC-21-005-C - Jan. 28 2021.pdf
You can see how they use the NIST SP800-53 controls = the labels we put on our tickets

Another Ext. Audit report example
https://www.doioig.gov/sites/doioig.gov/files/DOIOIG_FY19FISMA_Public.pdf
Baseline

What is the USGCB?
United States Government Configuration Baseline | CSRC (nist.gov)

Report: CSB Discontinued Information Recovery Testing and Off-Site Backup Storage During the Coronavirus Pandemic | EPA's Office of Inspector General | US EPA
CSB Discontinued Information Recovery Testing and Off-Site Backup Storage During the Coronavirus Pandemic
The CSB was at risk of not being able to readily restore information technology operations if they were disrupted during the coronavirus pandemic.

HHS Information Security Program Still 'Not Effective' (govinfosecurity.com)
did not employ automated mechanisms to thoroughly and effectively test system contingency plans
did not consistently implement their processes, strategies and technologies for information system backup and storage, including the use of alternate storage and processing sites.
(word for word the NIST SP 800-53 guide)

Large hospital suffers crippling ransomware attack (ontrack.com)
a large hospital in Germany was hit with a ransomware attack. The ‘Locky’ virus involved had violent effects and many servers were rendered out of action. In addition, core hospital operations became severely limited as the non-infected servers were powered down by the IT staff to prevent further infection. This is a significant problem with highly complex virtualised storage systems, as shutting off the power can cause unexpected problems to occur.
This was unfortunately the case with a Dell EqualLogic PS6500ES storage array used by the hospital, which contained a total of 148 professional hard disks with 100 gigabytes of space each. When the array was started again, the employees noticed that a LUN with two important Oracle databases was no longer displayed by the system and was therefore no longer available.

AXA ransomware attack comes just days after insurer pulled coverage for cyber-attack class in France | The Daily Swig (portswigger.net)
Insurance giant AXA has been hit by a massive ransomware attack

Another indication of how "old" topics like Vulnerability Management & Remediation are getting renewed attention and inspection.
https://www.jdsupra.com/legalnews/cybersecurity-oversight-a-board-7250842

“The multiple underlying risks is daunting but is complicated even more with the increasing importance of overall data management and information governance requirements. Companies face requirements for managing, storing and moving sensitive data to protect against intrusions and breaches, subject to global requirements that vary around the globe.”

“When vulnerabilities are identified and remediation may be required, directors have to oversee plans to mitigate these vulnerabilities and hold those responsible for fixing these problems.”

https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared

https://www.zdnet.com/article/new-ransomware-attack-targets-your-nas-devices-backup-storage/
""“Previously, encryption ransomware targeting NAS was hardly evident in the wild, and this year alone we have already detected a number of new ransomware families focused solely on NAS. This trend is unlikely to fade, as this attack vector proves to be very profitable for the attackers, especially due to the users being completely unprepared for them as they consider this technology highly reliable,” said Fedor Sinitsyn, security researcher at Kaspersky."

Additional data-points, 3rd party publications regarding storage security risk, threats, best practices etc. And the NIST Guidelines cover starting on page 17. Chapter 3 – Threats, Risks, and Attack Surfaces.

Guides / papers / articles:
https://www.snia.org/sites/default/files/ESF/Understanding-Storage-Security-and-Threats.pdf
SNIA: Understanding Storage Security and Threats

https://www.snia-j.org/cmm/images/wh/e-fibre.pdf
SNIA: Storage Security: Fibre Channel Security

https://www.snia.org/sites/default/files/technical_work/SecurityTWG/SNIA-Storage-Mgmt-Security-TechWhitepaper.pdf
SNIA: Storage Security: An overview as applied to storage management

https://fibrechannel.org/wp-content/uploads/2019/08/FCIA-FC-and-Security-Final.pdf
FCIA: Fibre Channel and Security

https://www.snia.org/sites/default/files/security/SNIA-Data-Protection-TechWhitepaper.pdf
SNIA: Storage Security: Data Protection Technical White Paper

https://www.iso.org/standard/44404.html
ISO/IEC 27040:2015 Information technology — Security techniques — Storage security

https://www.snia.org/sites/default/files/technical_work/SecurityTWG/SNIA-Encryption-KM-TechWhitepaper.R1.pdf
SNIA: Storage Security: Encryption and Key Management

https://www.brighttalk.com/webcast/663/422219
Storage Networking Security Series: Security & Privacy Regulations

https://www.brighttalk.com/webcast/663/388591
Storage Networking Security Series: Protecting Data at Rest

https://www.brighttalk.com/webcast/663/443844
Storage Networking Security Series: Securing Data in Transit

Articles / News

https://cyware.com/news/your-nas-devices-are-under-threat-from-ransomware-say-researchers-21cee063
“Previously, encryption ransomware targeting NAS was hardly evident in the wild, and this year alone we have already detected a number of new ransomware families focused solely on NAS. This trend is unlikely to fade, as this attack vector proves to be very profitable for the attackers, especially due to the users being completely unprepared for them as they consider this technology highly reliable,” said Fedor Sinitsyn, security researcher at Kaspersky.

https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.megalocker-ransomware.html
MegaLocker – Ransomware. The ransomware targets NAS storage devices and Samba servers and append either ".crypted" or ".NamPoHyu" to infected files. The malware is known to encrypt remote Samba servers but instead of encrypting locally on the victim’s server the ransomware runs the encryption process at a remote location.

https://securityintelligence.com/news/ransomware-attacks-targeting-organizations-backup-data-storage/
A quarterly threat report found that ransomware attacks are targeting organizations’ network-attached storage (NAS) and backup storage devices.

https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf
Misconfigured network storage solutions. In some cases, firms did not adequately configure the security settings on their network storage solution to protect against unauthorized access. In addition, some firms did not have policies and procedures addressing the security configuration of their network storage solution. Often, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially implemented.
Inadequate oversight of vendor-provided network storage solutions. In some cases, firms did not ensure, through policies, procedures, contractual provisions, or otherwise, that the security settings on vendor-provided network storage solutions were configured in accordance with the firm’s standards.

https://www.globenewswire.com/news-release/2019/07/10/1880925/0/en/Anomali-Discovers-New-Ransomware-Targeting-Consumer-Enterprise-Storage-Devices.html
Anomali, a leader in threat intelligence, today published its latest research blog. It details a new type of ransomware identified by the Anomali Threat Research Team. Designated as “eCh0raix,” it is targeting QNAP Network Attached Storage (NAS) device

https://www.anomali.com/blog/threat-actors-utilizing-ech0raix-ransomware-change-nas-targeting
Synology Inc., a Taiwan-based Network Attached Storage (NAS) company, posted an advisory on safeguarding internet-connected Synology NAS devices from Ransomware attacks

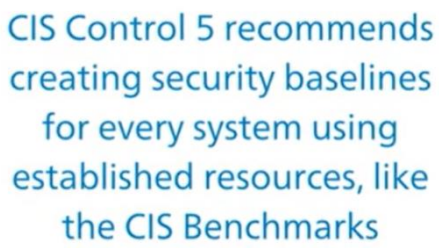
https://krebsonsecurity.com/2020/02/zyxel-fixes-0day-in-network-storage-devices/
Networking hardware vendor Zyxel today released an update to fix a critical flaw in many of its network attached storage (NAS) devices that can be used to remotely commandeer them

Digital Storage Projections For 2021, Part 3 (forbes.com)
“We think that, after the security breaches and malware attacks in 2020, that 2021 will see a major emphasis in developing more comprehensive storage system security.”

About Security Baselines

Definition by CERN: https://security.web.cern.ch/rules/en/baselines.shtml

Definition by CIS Control: https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/



CIS Baseline example ("Benchmark") – for Redhat:
https://www.cisecurity.org/benchmark/red_hat_linux/

(Leading) Definition by NIST: https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/control?version=4.0&number=CM-2

NIST Baseline example ("STIG" = Security Technical Implementation Guide) - Redhat:
https://www.stigviewer.com/stig/red_hat_enterprise_linux_7/

Proposed Baseline for Windows – by Microsoft: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-baselines

Proposed Baseline for Infrastructure device – By Cisco:
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/appendxD.html

Some organizations publish their baseline:
https://www.cu.edu/security/system-wide-baseline-security-standards
https://www.encs.psu.edu/files/2016/10/Minimum-Security-Baseline-v004-2b3qq6h.pdf
https://www.oregon.gov/das/OSCIO/Documents/StatewideInformationSecurityPlan.pdf
https://hhs.texas.gov/sites/default/files/documents/doing-business-with-hhs/contracting/hhs-is-controls-v1-1.pdf

The baseline has 2 parts in essence:

- General security guidance and required controls (security principles)
- Baseline implementation document (by device)

https://searchstorage.techtarget.com/tip/Adopt-data-storage-security-standards-to-ensure-compliance

NIST SP 800-209 (2020) Security Guidelines for Storage Infrastructure

This National Institute of Standards and Technology (NIST) Special Publication (SP) technical standard provides an overview of the development and evolution of storage technology, examines current data storage security threats, and delivers a detailed set of security recommendations and guidance to address storage threats.

NIST SP 800-209 progresses beyond traditional IT infrastructure elements, such as physical and logical security, access control and authentication, change management, configuration management, incident response, and recovery. It examines storage infrastructure issues, including data protection, networks, encryption and storage device security.

A Selection of News and Articles around Threats to Storage

"Cybercriminals behind a string of high-profile ransomware attacks…The unusual move is an attempt to target …network attached storage (NAS) devices"
Linux Variant of REvil Ransomware Targets VMware's ESXi, NAS Devices | Threatpost

"most commonly exploited….Intel SA-00191….Specific Intel firmware is susceptible to security vulnerabilities that may allow hackers to disclose sensitive information, escalate privileges and launch DoS (Denial of Service) attacks…. **NetApp** suite of products… are at risk"
https://resources.infosecinstitute.com/topic/32-hardware-and-firmware-vulnerabilities/

New attack vector opens backdoor inside enterprise disk **storage** arrays and people's **NAS** devices.
Over 13K iSCSI storage clusters left exposed online without a password | ZDNet

"The NCSC has seen numerous incidents where ransomware has not only encrypted the original data on-disk, but also network **storage** drives holding data **backups"**
Cognizant Hacked, Customers Affected, Maze Ransomware Named (techmonitor.ai)

"… hackers were able to gain privileged access to…. File **storage** services"
US says cyber hack poses 'grave risk' to critical infrastructure | Financial Times (ft.com)

"LNK files in his company's network attached **storage** (**NAS**) … sign of a rogue AutoIT worm… a hacker could use that program to get a hold of the company's intellectual property and hold it for ransom."
What Happens When A Company Gets Hacked? | Built In

"…the malicious actor was able to partially compromise our infrastructure, and gain access to document **storage**"
Security Incident on November 13, 2020 (liquid.com)

"…a '*nix' version is being made available that could target **NAS** devices and VMware ESXi virtualization hosts alongside the already supported Windows hosts."
Babuk Locker (cyberint.com)

"… the attacker released information pertaining to the victim's **NAS** servers and then released a supposed finance-related folder…. hundreds of gigabytes of data"
Pay2Key Ransomware Joins the Threat Landscape - Security Boulevard

Some very interesting trends/findings here … the mindset of attackers/Ransomware developers – increasingly targeting specific weaknesses:

What We Learn from MITRE's Most Dangerous Software Weaknesses List | SecurityWeek.Com

MITRE notes "the continued transition to more specific weaknesses as opposed to abstract, class-level weaknesses" as the major difference from earlier lists.

Tyler Shields, CMO at JupiterOne, does, however, pick out two specifics as having particular relevance. “The two biggest changes,” he told *SecurityWeek*, “were ‘Missing Authentication for Critical Function’ jumping up 13 places and ‘Incorrect **Default Permissions**’ jumping up a whopping 22 spots. These are the most common attacks that we are seeing in modern infrastructure and they are completely preventable.”

And Here's the list itself. [CWE - 2021 CWE Top 25 Most Dangerous Software Weaknesses (mitre.org)]

- The Conti ransomware gang has developed novel tactics to demolish backups. Conti bases its negotiation strategies on the premise that the majority of targets who pay the ransom are “motivated primarily by the need to restore their data.” According to Palo Alto Networks; “it’s one of the most ruthless of the dozens of ransomware gangs that we follow.”
  https://threatpost.com/linux-variant-ransomware-vmwares-nas/167511/

- Cybercriminals behind a string of high-profile ransomware attacks, including one extorting $11 million from JBS Foods last month, have ported their malware code to the Linux operating system. The unusual move is **an attempt to target network attached storage (NAS) devices** that run on the Linux operating system (OS). REvil is also targeting NAS devices as another storage platform with the potential to highly impact the affected companies.
  [ThreatPost, July 2021]

- **Hive** – this new ransomware gang is known to seek out and delete any backups to prevent them from being used by the victim to recover their data.
  [Bleeping Computer, November 2021]

- **Synology warns of malware infecting NAS devices with ransomware**
  The NAS maker urges all system admins and customers to change weak administrative credentials on their systems, to enable account protection and auto block, and to set up multi-factor authentication where possible.
  [Bleeping Computer, November 2021]

- **A new variant of the eCh0raix ransomware is able to target Network-Attached Storage (NAS) devices.**
  NAS servers are a privileged target for hackers because they normally store large amounts of data.
  The ransomware was targeting poorly protected or vulnerable NAS servers, threat actors exploited known vulnerabilities or carried out brute-force attacks.
  https://securityaffairs.co/wordpress/120994/cyber-crime/ech0raix-ransomware-qnap-synology.html