CONTINUITY SOFTWARE

HealthCheck Report

Data Storage Systems: Security Configuration Analysis

Prepared for: XYZ Bank

Issued by: Continuity Software

February 2020

Table of Content

Introduction

XYZ Bank invited **Continuity Software** to perform a data storage security HealthCheck on a subset of its production environment to identify data system security misconfigurations and vulnerabilities.

Data Security Advisor™ addresses the challenges of securing the vulnerable enterprise data storage IT environment. It automatically collects the up-to-date configurations of the enterprise's data storage systems and checks for security misconfigurations and vulnerabilities including violation of vendor security best practices, organizational security baseline configuration requirements, ransomware protection guidelines, non-compliance with information security standards and more. It informs the relevant IT teams of violations and how to repair them in order to close the security gaps that put critical data systems at risk.

Key benefits of Data Security Advisor:

- Meet vendor and community-driven security configuration best practices.
- Automatically validate security baseline configurations.
- Comply with information security standards (ISO, CIS, PCI, NIST, FFIEC and more).
- Provides remediation guidelines for detected misconfigurations and facilitates automatic healing.
- Support all enterprise data storage systems including SAN, NAS, Storage Network, Storage Management, Storage Virtualization, Data Protection Systems and more.
- Tracks and reports on security configuration changes.
- An enterprise-grade solution – A secure and scalable solution that can be easily customized and/or integrated with other management systems.

When a risk is discovered by DSA, a detailed description and the suggested resolution are forwarded to the right IT teams for timely action. **DSA** operation is agentless, secure and non-intrusive.

Such risks are the natural result of a large volume of ongoing changes within a highly complex technology environment. Given the nature of such environments, it is practically impossible to manually identify such issues. Automated, proactive discovery of these irregularities is critical to preventing data security risks and successfully completing Information Security audits.

Executive Summary

Overview

- A subset of the production environment was scanned and analyzed by **DSA**.
- The one-time collection of configuration data was performed using DSA's agentless scan technology, with no impact on production and without installing any software on the target systems.
- The following systems were included in the scan scope:
    - The data systems used by **Payments**, **CRM** and **Billing** applications
    - Storage systems (block, file, object and cloud)
    - Storage virtualization and data protection appliances
    - Storage network

HealthCheck Findings

- Overall 376 storage systems scanned.
- A total of **26 risk types** were detected, consisting of **58 individual risks**.
- The data security vulnerability and compliance risks identified span all layers of the storage infrastructure, including **file and block storage, virtual SAN, storage network, storage management systems** and more**.**
- A detailed, prioritized listing of all 26 risks found is included in this report.

Conclusions

- Significant **data security risks identified for data systems used by Payments, Billing and CRM.**
- Detailed information is available through this report for the compliance risks, vulnerabilities and security best practice violations identified by DSA.
- It is practically impossible to manually identify such risks - though simple to repair once found.
- Similar and other issues may be present in the un-scanned portion of the production environment.
- Running a daily scan on all critical systems at XYZ Bank is highly recommended.
- This report details the risks identified and includes the corrective steps required for remediation.

Analysis Summary

The following table presents a summary of security principles examined by Data Security Advisor and the number of storage devices that have passed or failed to meet the principle.

Category	Security principle	Pass	Fail
Access Control	Access rights granted to authorized users/hosts only	54	2
Access Control	Account lockout	376	0
Encryption	Administrative API sessions are encrypted	186	0
Authorization	All users are restricted by a role	376	0
Malware Protection	Antivirus scanning is enabled	154	0
Malware Protection	Antivirus server redundancy	154	0
Configuration Management	Approved OS release	376	0
Audit	Audit log configuration (Log content)	375	1
Audit	Audit logging is enabled	376	0
Audit	Authorized (secure) time source servers are used	376	0
Authentication	Authorized authentication servers are used	376	0
Audit	Authorized logging servers are used	376	0
Configuration Management	Authorized name servers are used	376	0
Authentication	Central authentication is used	376	0
Authentication	Central authentication server redundancy	376	0
Encryption	Clear-text protocols are disabled	370	11
Authentication	Client certification verification is mandatory	129	0
Encryption	Data at-rest is encrypted	65	0
Audit	External (central) log servers are configured	375	2
Access Control	Fabric access is restricted	204	0
Access Control	Firewall / IPfilter is enabled	376	0
Access Control	Guest/Anonymous user access is restricted	98	3
Access Control	Idle sessions are terminated	376	0
Access Control	Inactive user accounts are disabled	86	0
Encryption	In-flight data (client-server) is encrypted	86	0
Authentication	Initial password change required	248	0
Authentication	Key size meets minimum length requirement	202	0
Authorization	Least privilege	341	0
Access Control	Local user accounts should not be used	375	1
Audit	Logging server redundancy	376	0
Authentication	Maximum password lifetime is restricted	202	0

Authentication	Minimum password length is enforced	202	0
Authentication	Minimum password lifetime is restricted	202	0
Configuration Management	Name server redundancy	376	0
Configuration Management	Name service is enabled	376	0
Services and Protocols	Only enable SNMP if necessary	101	0
Authentication	Password complexity is enforced	202	0
Authentication	Password reuse is limited	202	0
Authentication	Reject password DB updates on all switches	210	0
Authentication	Remove or disable all default (factory) user accounts	374	2
Encryption	Replication traffic is encrypted	86	0
Audit	Retain audit trail history	376	0
Services and Protocols	Secure NFS versions used	147	3
Access Control	Secure SAN (FC) zoning used	198	4
Services and Protocols	Secure SNMP versions used (SNMPv3 or its successors)	324	0
Access Control	Session termination (automatic logoff)	325	0
Services and Protocols	SNMP authentication required	200	2
Services and Protocols	SNMP used in read-only mode	202	0
Access Control	Storage network enumeration is restricted	136	0
Encryption	Strong password hashing algorithm used	343	0
Encryption	Strong SSH MAC algorithm used	89	3
Authentication	Strong storage management host identification	67	0
Audit	Synchronization with authoritative time source is enabled	374	2
Access Control	System use notification is presented	376	0
Audit	Time source server redundancy	376	2
Services and Protocols	Unsecure SMB versions are disabled	136	0
Services and Protocols	Unsecure SSH versions are disabled	174	0
Configuration Management	Use of standard ports	183	0
Authentication	Use of uppercase characters in passwords	202	0
Authentication	Vendor-supplied default passwords are not used	371	5
Malware Protection	Vulnerability identification	366	10
Encryption	Strong encryption used	265	2
Malware Protection	Ransomware protection features used	86	2
Authentication	Password vault used	124	1
… and additional unlisted security principles			
Authentication	Password vault used	19,463	58

Summary of Risk Types

A total of **26 risk types** were detected, consisting of 58 individual risks.

The following table lists all the risks identified, sorted by the priority ("Rating") assigned by a Continuity Software engineer, after a thorough examination of each risk.

ID	Type	Summary	Rating	Check Name
611	EMC VPLEX	Incorrect TLS level configured.	★★★★★	TLS Level
142	Cisco MDS	Unsecure protocols enabled.	★★★★★	Service status – HTTP, TELNET
293	EMC VNX	Unsecure communication between Policy manager and ESRS client.	★★★★★	ESRS – Policy Manager SSL Status
1002	EMC Isilon	Weak SSH message authentication code (MAC) algorithm is used.	★★★★★	SSH MAC strength
283	NetApp	Ransomware protection features are not enabled.	★★★★★	Fpolicy for ransomware
543	Brocade SAN	Zone members are configured with Domain, Port identification.	★★★★★	SAN Fabric - zone member identification
342	Cisco MDS	Local SNMP users are configured with the noAuth security level.	★★★★★	SNMP user authentication
195	EMC Isilon	EMC Isilon OneFS vulnerabilities identified (DSA-2020-045).	★★★★★	OneFS vulnerability scanning
645	EMC Isilon	Unsecure clear-text ftp connections are enabled.	★★★★★	ftp service status
71	EMC XtremIO	XtremIO XMS vulnerabilities identified (DSA-2019-172).	★★★★★	XtremIO vulnerability scanning
282	NetApp	Access to file shares is not restricted by client IP.	★★★★★	NFS export client access list
125	EMC Data Domain	NTP servers are not configured.	★★★★★	NTP status
7	EMC Data Domain	External syslog servers are not configured.	★★★★★	Centralized log server
84	Cisco MDS	External syslog servers are not configured.	★★★★★	Centralized log server
715	EMC VMAX	EMC Vulnerabilities identified (DSA-2019-186).	★★★★★	VMAX vulnerability scanning
627	NetApp	Unsecure snmp community settings.	★★★★★	SNMP community default string
681	VxFlex OS	VxFlex (ScaleIO) OS multiple vulnerabilities identified (DSA-2019-116, ESA-2017-094).	★★★★★	VxFlex OS vulnerability scanning

315	EMC Data Domain	Un-vaulted local user accounts.		Local user account vaulting
81	NetApp	Non-default local user accounts are configured.		Non-default local user accounts
223	NetApp	UID of Unknown/Anonymous user is mapped to an admin user account.		Unknown user UID
354	EMC VMAX	Background Audit logging is disabled on EMC Storage management.		Background Audit logging (no-loss)
360	EMC Isilon	Unsecure NFS versions are enabled.		NFS versions enabled
196	Cisco MDS	Insufficient NTP server redundancy.		NTP server redundancy
603	NetApp	ONTAP Vulnerabilities identified (NTAP-20191024-0001).		ONTAP vulnerability scanning
351	RecoverPoint	RecoverPoint vulnerabilities identified (DSA-2019-078).		RecoverPoint OS vulnerability scanning
755	EMC VPLEX	Default (factory) user accounts are enabled.		root user status