Datenblatt

Sicherheitsfunktionen im SANtricity OS für die E-Series

Sicherheit für Ihre Daten – die wichtigste Ressource von Unternehmen

Wichtigste Vorteile

Verbessern von Datenvertraulichkeit, -integrität und -verfügbarkeit
Die Sicherheitsfunktionen und zugehörigen Kontrollen in NetApp SANtricity für die E-Series optimieren die Vertraulichkeit, Integrität und Verfügbarkeit von Daten – der wichtigsten Ressource von Unternehmen.

Sicherheit in der Umgebung des Kunden
Kunden errichten eine sichere Grundlage für die Data Fabric ihres Unternehmens und haben einen Überblick über die Sichtbarkeits- und Sicherheitsfunktionen für eine sichere Infrastruktur.

Anwenden von NetApp und Branchen-Best Practices für Sicherheit
Gemeinsam mit Experten, dem Branchen-Know-how und gängigen Vorgehensweisen von NetApp entsteht eine überprüfte Sicherheitsstruktur.

Einhaltung von Governance- und Compliance-Anforderungen
Bewährte Sicherheits-Best Practices werden angewendet, um Branchenvorgaben und Sicherheit-Compliance einzuhalten und zu unterstützen.

Die NetApp SANtricity Storage-Managementsoftware entwickelt sich weiter und Sicherheit ist dabei ein integraler Bestandteil der Lösung. Die vielen Sicherheitsfunktionen von SANtricity für die E-Series sind unverzichtbar, um die Sicherheit aufrechtzuerhalten und die Best Practices der Branche einzuhalten. Durch diese neuen Funktionen werden Datenvertraulichkeit, -integrität und -verfügbarkeit zur obersten Priorität.

Informieren Sie sich darüber, wie das SANtricity OS 11.50 für die E-Series die Common Criteria-Zertifizierung für Network Device Collaborative Protection Profile (NDcPP) erhielt.

Weitere Informationen zur Laufwerksicherheit und zu Management-Sicherheitslösungen von NetApp finden Sie in den Artikeln TR-4474: NetApp SANtricity Drive Security und TR-4712: NetApp SANtricity Management Security.

Die Herausforderung

Tagtäglich entstehen neue, komplexere Bedrohungen und das Risiko steigt ständig. Von Storage Engineers wird in ihrer Rolle als Administratoren und Betreiber der Datenbestände erwartet, dass sie die Daten während ihres gesamten Lebenszyklus sicher managen.

Die Lösung

Dieses Datenblatt bietet einen Überblick über die neuen und die bestehenden Sicherheitsfunktionen in SANtricity 11.50 und neueren Releases. Darin werden die wichtigsten Elemente vorgestellt, mit denen Sie einen branchenweit bewährten Sicherheitszustand für Ihre wichtigste Ressource schaffen: Ihre Daten.

NetApp®

Sicherheitsfunktionen zur Überprüfung der Zertifikatsannullierung

SOFTWARE ODER FEATURE	FUNKTION	AUSWIRKUNGEN
Überprüfen von Annullierungen mit Online Certificate Status Protocol (OCSP)	Dank OCSP können Applikationen der E-Series, die TLS-Kommunikation wie LDAP over TLS verwenden, einen digitalen Zertifikatsstatus erhalten. Die Applikation erhält eine signierte Antwort, die angibt, ob das angeforderte Zertifikat in Ordnung, annulliert oder unbekannt ist. Für den Common Criteria-Modus ist die Aktivierung von OCSP die bevorzugte Einstellung.	Wenn OCSP aktiviert ist, werden Zertifikate auf Annullierung überprüft und validiert.

Kryptografische Sicherheitsfunktionen

SOFTWARE ODER FEATURE	FUNKTION	AUSWIRKUNGEN
Transport Layer Security für die Managementoberfläche	Die E-Series nutzt TLS v1.2 für sichere Kommunikations- und Administrationsfunktionen in der Managementoberfläche, sichere CLI und REST-API.	NetApp rät von der Verwendung von TLS v1.0 und TLS v1.1 ab, da diese Versionen erhebliche Schwachstellen aufweisen und somit Compliance-Standards wie PCI-DSS nicht erfüllen. NetApp empfiehlt die Verwendung von TLS v1.2 aufgrund seiner Stärke und Integrität.
Verschlüsselung nach FIPS	Die E-Series nutzt für alle verschlüsselten Daten Bouncy Castle, eine Sammlung von in der Kryptografie verwendeten APIs nach FIPS 140-2 Level 1.	FIPS 140-2 Level 1 ist der Branchenstandard für Kryptografieprodukte und -lösungen.

Datensicherheitsfunktionen

SOFTWARE ODER FEATURE	FUNKTION	AUSWIRKUNGEN
Vollständige Festplattenverschlüsselung (FDE)	FDE ist ein hardwarebasierter Verschlüsselungsmechanismus zur Verschlüsselung von Daten auf Self-Encrypting Drives. Für nach FIPS 140-2 zertifizierte FDE-fähige Laufwerke werden vom Laufwerk zur Verschlüsselung der Daten kryptografische Algorithmen nach FIPS 140-2 verwendet.	Verschlüsselung für Daten im Ruhezustand bleibt weiterhin ein wichtiges Thema in der Branche. FDE erfüllt dieses Anliegen und erhält mithilfe weiterer Sicherheitsfunktionen gleichzeitig einen soliden Sicherheitsstatus auf Subsystemebene aufrecht.
Internes FDE-Verschlüsselungsmanagement	Die Funktion für das interne FDE-Verschlüsselungsmanagement ist eine eigenständige Verschlüsselungslösung für Daten im Ruhezustand. Das interne Verschlüsselungsmanagement nutzt FDE, die eine vollständige Festplattenverschlüsselung mithilfe von Self-Encrypting Drives durchführt.	Internes FDE-Verschlüsselungsmanagement ist eine eigenständige Lösung für Unternehmen, die nicht in externe Verschlüsselungsmanagementserver investieren möchten, um auf diese Weise ihre Gesamtbetriebskosten zu senken. Mit dieser wichtigen Sicherheitsfunktion können die Benutzer Daten im Ruhezustand schützen.
Externes FDE-Verschlüsselungsmanagement	Externes FDE-Verschlüsselungsmanagement erfolgt über ein Drittanbietersystem in der Storage-Umgebung, die Authentifizierungsschlüssel, die von Verschlüsselungsfunktionen im Storage-System wie FDE verwendet werden, sicher managt. Das Storage-System verwendet eine SSL-Verbindung, um den externen Schlüsselmanagementserver zu kontaktieren (z. B. Gemalto SafeNet KeySecure) und Authentifizierungsschlüssel mit dem standardisierten Key Management Interoperability Protocol (KMIP) zu speichern oder abzurufen.	Das externe FDE-Verschlüsselungsmanagement ermöglicht die Zentralisierung der Verschlüsselungsmanagementfunktionen in Unternehmen und stellt sicher, dass die Schlüssel nicht in der Nähe der Assets gespeichert werden, sodass das Gefährdungsrisiko reduziert wird.
Secure Erase für FDE-fähige Laufwerke	Mit der Funktion Secure Erase lassen sich Festplatten bereinigen, indem die Daten von einem FDE-fähigen Laufwerk oder einer Reihe FDE-fähiger Laufwerke so entfernt werden, dass sie nicht mehr wiederhergestellt werden können.	Sicherheitsprotokolle für das Ausmustern oder neue Verwenden von Laufwerken schreiben vor, dass die Daten nicht wiederherstellbar sein dürfen.

Sicherheitsfunktionen zur Nachrichtenprotokollierung

SOFTWARE ODER FEATURE	FUNKTION	AUSWIRKUNGEN
Banner für Anmeldung und „Message of the Day“ (MOTD) (SANtricity OS 11.40.1 und höher)	Anmeldebanner werden vor der Authentifizierung in die Ausgabe gedruckt. Über diese Banner können Unternehmen und Administratoren mit den Systembenutzern kommunizieren.	Mithilfe von Anmeldebannern können Unternehmen Betreibern, Administratoren und auch Benutzern mit eingeschränkten Berechtigungen die Bedingungen für eine akzeptable Nutzung eines Systems anzeigen. Die Banner zeigen auch an, wer berechtigt ist, auf das System zuzugreifen.
Sichere Protokollweiterleitung (Syslog über Transport Layer Security [TLS]) (SANtricity OS 11.40.1 und höher)	Die Protokollweiterleitungsfunktion unterstützt Administratoren dabei, Ziele so bereitzustellen, dass sie Syslog- und Audit-Informationen empfangen können. Aufgrund der Sicherheit der Syslog- und Audit-Informationen kann E-Series diese Informationen sicher über TLS mithilfe des TCP-verschlüsselten Parameters versenden.	Protokoll- und Audit-Informationen sind für Unternehmen im Hinblick auf Support und Verfügbarkeit von unschätzbarem Wert. Zudem handelt es sich bei den in Protokollen (Syslog) und Audit-Berichten enthaltenen Informationen in der Regel um sehr sensible Daten. Um die Sicherheitskontrollen und das Sicherheitsniveau aufrechtzuerhalten, müssen die Protokoll- und Audit-Daten sicher gemanagt werden.
Simple Network Management Protocol (SNMP v2c)	SNMP ist ein Standardprotokoll, mit dem Network-Attached-Geräte (E-Series-Array) ihren Status melden können. Die E-Series unterstützt SNMP v2c, das sicherheitsrelevante Verbesserungen beinhaltet (Community-basierte Authentifizierung). Für den Common Criteria-Modus ist die bevorzugte Einstellung die Deaktivierung von SNMP.	Diese Funktion verleiht einer SNMP-Managementapplikation einfache Monitoring-Funktionen für NetApp Storage-Arrays der E-Series.

Funktionen zur OS-Authentifizierung

SOFTWARE ODER FEATURE	FUNKTION	AUSWIRKUNGEN
Digital signierte SANtricity OS Firmware (SANtricity OS 11.40.2 und höher)	In Version 8.42 und höher ist digital signierte Controller-Firmware erforderlich. Wenn die Firmware nicht signiert ist, werden Download-Versuche zurückgewiesen. Darüber hinaus wird am Tagesbeginn für das Array in einem Selbsttest überprüft, ob die Firmware intakt ist.	Dies verhindert, dass unautorisierte oder böswillige Benutzer ein Code-Bundle herunterladen, das nicht von NetApp stammt oder modifiziert wurde.

Sicherheitsfunktionen für die Benutzerzugriffssteuerung

SOFTWARE ODER FEATURE	FUNKTION	AUSWIRKUNGEN
Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)	RBAC in der E-Series gibt Administratoren die Möglichkeit, den administrativen Zugriff der Benutzer auf das Niveau zu beschränken, das für ihre Rolle festgelegt wurde. So können Administratoren Benutzer anhand der ihnen zugewiesenen Rolle managen.	Zugriffssteuerung ist ein wesentliches Element für die Sicherheit. Funktionen wie RBAC bieten Unternehmen die Möglichkeit, festzulegen, wer in welchem Umfang Datenzugriff erhält. Dies dämmt Schwachstellen und Exploits ein, einschließlich Datenexfiltration und Eskalation von Berechtigungen.
Lightweight Directory Access Protocol (LDAP)	Die Authentifizierung und Autorisierung von Verzeichnisbenutzern ist eine grundlegende Funktion für das Implementieren von Storage in IT-Umgebungen von Unternehmen.	Die Konfiguration und Zuweisung von Benutzern von LDAP zur Durchführung von Storage-Managementfunktionen in Storage-Arrays der E-Series wird unterstützt.
Secure Lightweight Directory Access Protocol (LDAPS) für Interaktionen von Verzeichnisdiensten	Die E-Series unterstützt sichere Kommunikation (LDAPS) bei der Interaktion mit LDAP-Servern.	Mithilfe des LDAPS-Protokolls lässt sich die Übertragung sensibler Daten als unverschlüsselten Text vermeiden.
Multi-Faktor-Authentifizierung (MFA) mit SAML 2.0-Technologie	Die in die E-Series eingebettete GUI von SANtricity System Manager unterstützt SAML. Die Authentifizierung kann über einen Identitäts-Provider (IdP) mit SAML gemanagt werden. Ein Administrator stellt die Verbindung zwischen dem IdP-System und dem Storage-Array her und ordnet anschließend die IdP-Benutzer den im Storage-Array eingebetteten lokalen Benutzerrollen zu.	Die Unterstützung des SAML-Standards ermöglicht die Implementierung von Multi-Faktor-Authentifizierungslösungen, sodass die gesetzlichen Identitätsmanagementrichtlinien erfüllt werden können.
Passwortrichtlinie	Diese Funktion ermöglicht dem Administrator, für jeden Controller eine Anzahl an Anmeldeversuchen bei SANtricity System Manager festzulegen, bevor der Benutzer für eine gewisse Zeit gesperrt wird. Dem Administrator stehen zwei Sperrmodi zur Verfügung: Sperrung auf Basis der IP-Adresse (Standardeinstellung) und Sperrung auf Basis des Benutzerkontos. Für den Common Criteria-Modus ist die benutzerbasierte Sperrung die bevorzugte Einstellung. Die E-Series kann so konfiguriert werden, dass die Mindestlänge des Passworts 15 Zeichen umfasst. Die maximale Länge beträgt 30 Zeichen.	Potenzielle Denial-of-Service-Angriffe werden vermieden, da die Angreifer nicht unbegrenzt versuchen können, sich Zugang zum Storage-Array zu verschaffen. Die Festlegung einer längeren Mindestzeichenfolge für das Passwort erschwert das Entschlüsseln und erfüllt gesetzliche Anforderungen.

Sicherheitsfunktionen für die Benutzeroberfläche

SOFTWARE ODER FEATURE	FUNKTION	AUSWIRKUNGEN
Zugriff auf die Konsole über SSH	Mit der E-Series können sich die Benutzer mit der Array-Konsole über SSH verbinden. Für den Common Criteria-Modus ist die Deaktivierung des SSH-Zugriffs die bevorzugte Einstellung.	Der Konsolenzugriff über SSH wird in der Regel zur Fehlerbehebung von Problemen mit dem Storage-Array verwendet. Dies wird normalerweise unter Anleitung vom NetApp Customer Support Team durchgeführt.
Sicherer REST-API-Zugriff auf Protokolle und Ports über sicheres HTTPS-Protokoll	Die E-Series unterstützt die REST-API, die über das HTTPS-Protokoll eine sichere Kommunikationsschnittstelle zwischen dem Storage-Array und dem Management-Client bietet. Für den Common Criteria-Modus ist die Deaktivierung von SYMbol (eine proprietäre Kommunikationsschnittstelle) die bevorzugte Einstellung.	Die REST-API-verschlüsselte Managementoberfläche hilft bei der Durchsetzung von vertraulicher Kommunikation zwischen dem Storage-Array und dem Management-Client.
Sicherer Zugriff auf die Befehlszeilenschnittstelle	Die E-Series implementiert zur Kommunikation mit dem Storage-Array SMcli. Eine sichere CLI stellt für die Kommunikation zwischen Client und Server über das TLS-Protokoll einen sicheren Kommunikationskanal her.	Ein sicherer Systemzugriff ist ein wesentlicher Bestandteil einer sicheren Lösung.

Über NetApp

NetApp ist die Instanz für Daten in der Hybrid Cloud. Mit unserem Portfolio an Hybrid Cloud Data Services, die das Management von Applikationen und Daten über Cloud- und On-Premises-Umgebungen hinweg vereinfachen, beschleunigen wir die digitale Transformation. Gemeinsam mit Partnern helfen wir Unternehmen weltweit, das volle Potenzial ihrer Daten auszuschöpfen und so ihren Kundenkontakt zu erweitern, Innovationen voranzutreiben und Betriebsabläufe zu optimieren. Weitere Informationen finden Sie unter **www.netapp.de**. #DataDriven