Sicheres Verbindungsgateway

Unsere Technologie vereint Data Protection und Bedrohungsschutz in einer sicheren, automatisierten Supporterfahrung

Bis zu

60 %

der von Forrester befragten IT-Führungskräfte nutzen Konnektivitäts-technologie, um Risiken zu reduzieren[1]

Dies wird auch in ausgewählter Dell EMC Hardware und einem Service-Plug-in in OpenManage Enterprise für PowerEdge-Server als Version mit direkter Verbindung implementiert. Dell Technologies Services setzt sich für die Implementierung von Sicherheitsfunktionen ein, die auf Märkten, Bestimmungen und Kundeneinblicken basieren, denn unsere Produkte sollen den Sicherheitszielen und Complianceanforderungen unserer Kunden gerecht werden.

Inhalt

1: Einführung:

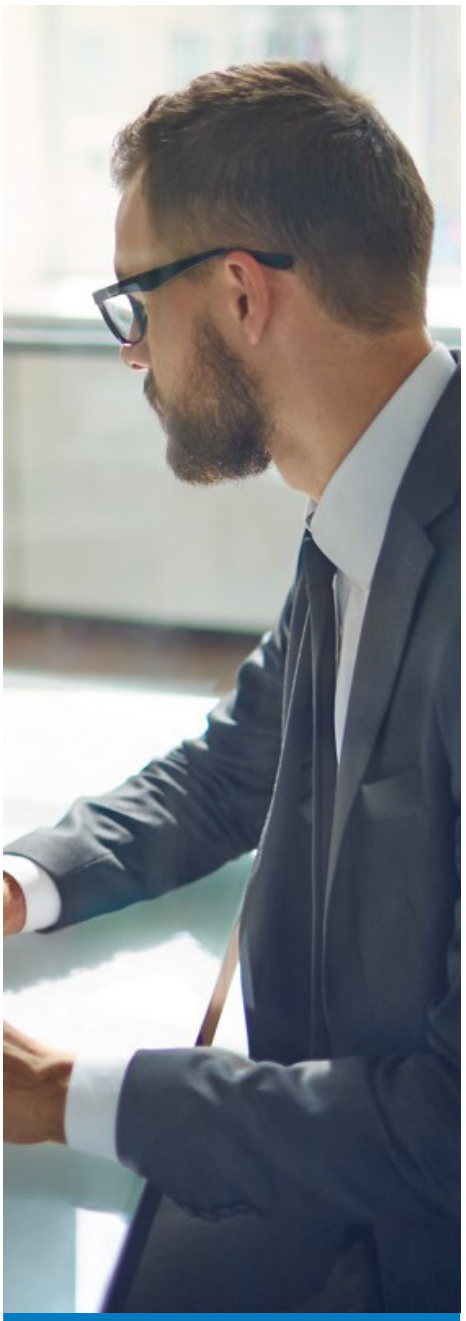
In der heutigen hyperdigitalen Welt nutzen erfolgreiche Innovationsführer zunehmend die Möglichkeit zum Outsourcing des IT-Supports an IT-Serviceanbieter. Laut einer Forrester Consulting-Studie im Auftrag von Dell Technologies Services[1] geben 59 % der befragten IT-Verantwortlichen an, dass die Zusammenarbeit mit dem richtigen IT-Serviceanbieter sie in die Lage versetzt, die Zeit ihrer IT-Mitarbeiter von Routinevorgängen auf Innovationen und strategische Initiativen zu verlagern.

Als führender IT-Serviceanbieter sorgt Dell Technologies Services dafür, dass seine IT-Support-Services und -Technologien keine potenziellen Quellen für Sicherheitsbedrohungen darstellen. Jeden Tag unternehmen wir alles uns Mögliche zur Minimierung der Risiken für unsere Kunden, die von den in ihrer Umgebung bereitgestellten Dell EMC Produkten ausgehen. In diesem Whitepaper wird erläutert, auf welche Weise Sicherheit in das Design, die Implementierung und den Betrieb des sicheren Verbindungsgateways integriert ist und wie dadurch eine sichere automatisierte IT-Supporterfahrung für komplexe Rechenzentrumsinfrastrukturen gewährleistet wird.

Die Sicherheitsarchitektur des sicheren Verbindungsgateways basiert auf mehr als 25 Jahren Pionierarbeit im Bereich IT-Supporttechnologie. Sie wurde für die Abwehr von Bedrohungen und auf den Schutz der Datenintegrität entwickelt. Mit der Technologie werden Kundengeräte kontinuierlich auf Probleme überwacht und im Ernstfall wird eine schnelle Lösung eingeleitet:

- Wir nutzen nur Telemetrie- und Ereignisdaten von aktiven Systemen.
- Wir verschlüsseln Systemstatusdaten für die Übertragung über das Internet per HTTPS mit dem TLS-Protokoll (Transport Layer Security).
- Unsere autorisierten Mitarbeiter des technischen Supports nutzen Multi-Faktor-Authentifizierung für den Remotezugriff auf verbundene Systeme und die Problembehebung auf diesen Systemen.
- Wir verarbeiten, speichern und verwenden Telemetrie- und Ereignisdaten an unseren Standorten mit branchenführenden Sicherheitsverfahren.

Außerdem testen wir die in die Architektur des sicheren Verbindungsgateways und die zugehörigen Prozesse integrierten Sicherheitsmaßnahmen mit mehreren erstklassigen Anbietern wie Secureworks sorgfältig, damit Sie sich auf zuverlässigen Datenschutz und eine sichere Erfahrung verlassen können.



Cyberangriffe und Datenbetrug oder -diebstahl zählen zu den zehn wichtigsten Themen für CEOs.[2]

2: Informationen zum sicheren Verbindungsgateway

Dell Technologies stellt Technologie für sichere Konnektivität bereit, mit der das Rätselraten bei der Problemvermeidung wegfällt. So bleibt Ihnen mehr Zeit für die wirklich wichtigen Projekte. Die Editionen mit der virtuellen Appliance und der Anwendung stellen eine sichere bidirektionale Verbindung zwischen Ihrer Umgebung und Dell Technologies Services bereit, die sich ideal für das zentrale Monitoring von Dell EMC Geräten im gesamten Rechenzentrum eignet, einschließlich Daten-Storage, Servern, Networking, CI/HCI und Data Protection.

Sie können unsere Technologie für ausgewählte Dell EMC Produkte auch flexibel als Version mit direkter Verbindung und mit einem Service-Plug-in in OpenManage Enterprise für PowerEdge-Server bereitstellen. Besuchen Sie Dell.com/Support, um die unterstützten Konnektivitätsoptionen für bestimmte Hardware- und Softwareprodukte von Dell EMC zu überprüfen.

Daten stehen im Mittelpunkt des sicheren Verbindungsgateways. Wir nutzen die Systemstatusdaten aus Kundenumgebungen und korrelieren sie mit den über Jahre gesammelten Incident- und Technikdaten von Außendienst- und technischen Supportteams sowie von Komponentenherstellern.

Zeigen Sie die Dokumente „Reportable Items“ für das sichere Verbindungsgateway und das Services-Plug-in für OpenManage Enterprise an, um Details zu den erfassten Systemstatusinformationen zu erhalten.

Mit ausgereiften KI-Modellen unter Einbeziehung von maschinellem Lernen kann unsere Konnektivitätstechnologie Muster finden und anwenden und so gleich beim ersten Versuch das richtige Problem erkennen. Die Lösung ermittelt Hardware- und Softwareprobleme, erstellt eine Supportanfrage und initiiert den von uns ausgehenden Kontakt, damit das Problem behoben werden kann, bevor es kostspielige Folgen hat. Sie prognostiziert Ausfälle auf Serverfestplatten und Rückwandplatinen, die über sicheres Verbindungsgateway verbunden sind. Je nach Art des Problems kann durch die Warnmeldung auch ein automatischer Ersatzteilversand angestoßen werden.

Darüber hinaus ermöglicht die Technologie autorisierten Mitarbeitern des technischen Supports eine sichere bidirektionale Kommunikation für den Remotezugriff auf gemanagte Geräte zum Troubleshooting und zur Problembehebung.

SICHERHEIT FÜR KONNEKTIVITÄT

Drittanbieter-Sicherheits-bewertungen werden regelmäßig für das sichere Verbindungsgateway und die zugehörige Infrastruktur durchgeführt.

Anwendungsbewertungen decken die Sicherheit bei Datenübertragung und API, statische und dynamische Quellcodeanalysen, Prüfungen gemäß CVE (Common Vulnerabilities and Exposures) und OWASP (Open Web Application Security Project) sowie Bibliotheken und Produkte von Drittanbietern ab.

Bei den **Infrastruktur-bewertungen** werden interne und externe Netzwerkgeräte, Server und Serviceanbieter berücksichtigt.

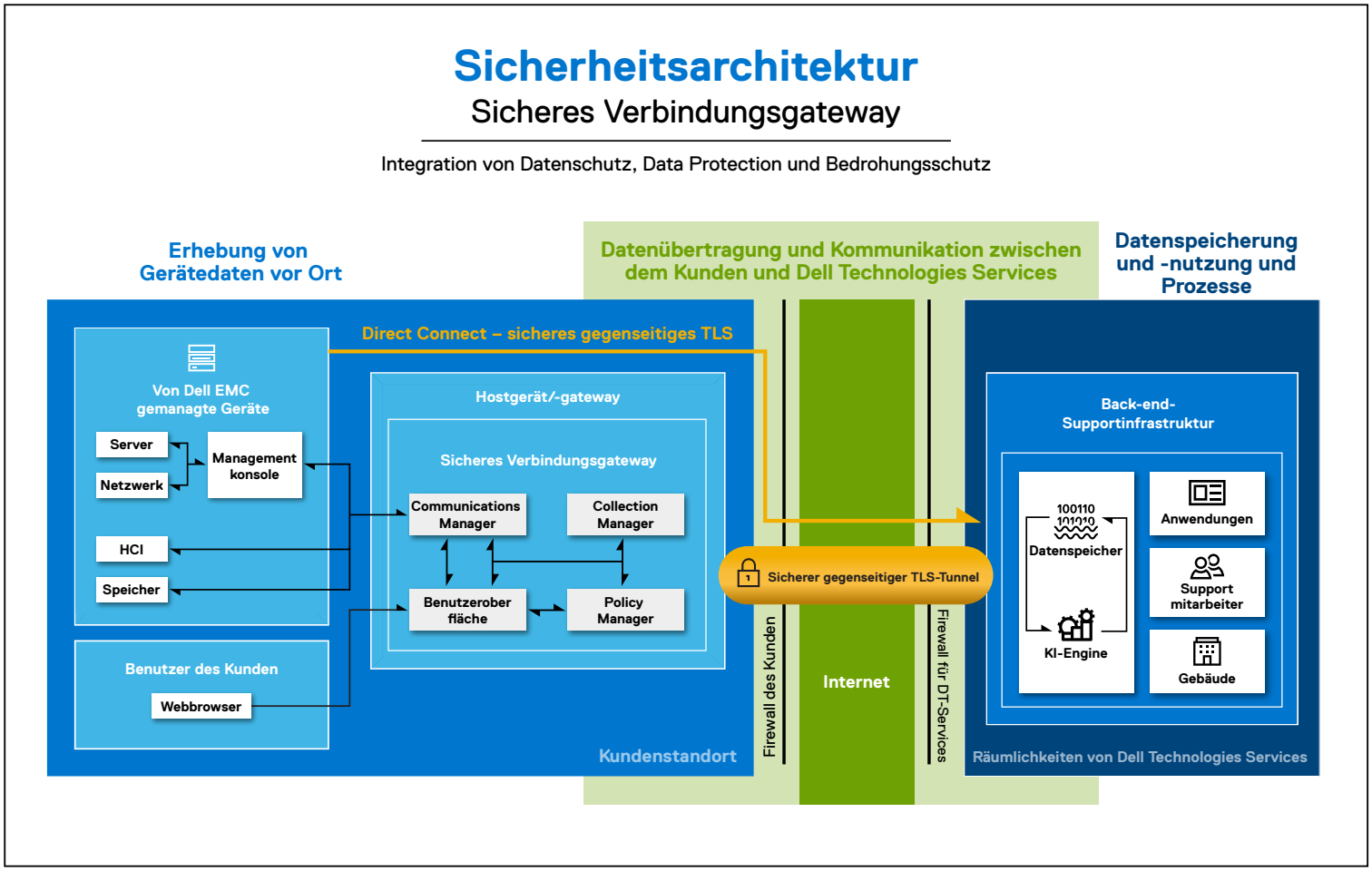
3: Übersicht der Sicherheitsarchitektur

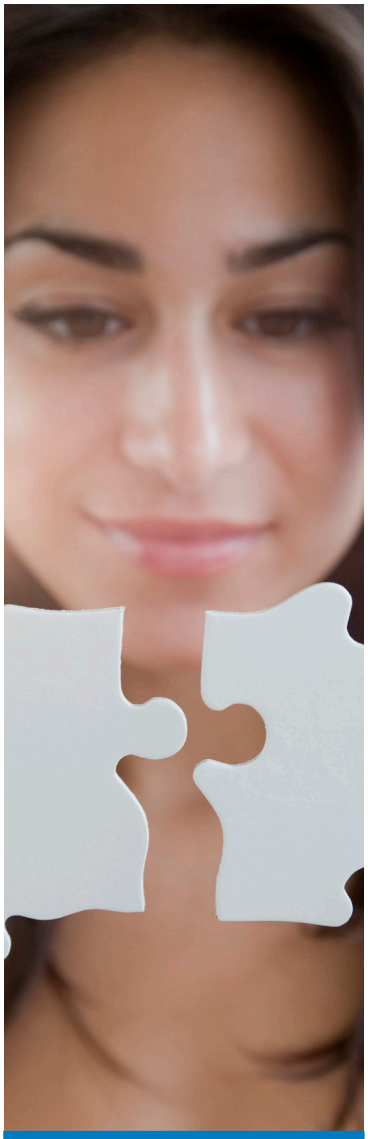
Dell Technologies Services bemüht sich um die Minimierung des Risikos von Sicherheitsbedrohungen in unserer automatisierten, proaktiven und vorausschauenden Konnektivitätstechnologie. Unsere Sicherheitsarchitektur wurde nach strengen Branchenstandards entwickelt. In jeder Phase der Produktentwicklung und -bereitstellung werden messbare, reproduzierbare Sicherheitsverfahren eingesetzt. Weitere Informationen finden Sie in Abschnitt 4.

Diagramm A enthält eine Übersicht der Sicherheitsarchitektur des sicheren Verbindungsgateways. In den folgenden Abschnitten betrachten wir eingehender, wie unsere Technologie nur die zur Diagnose und Behebung von Problemen benötigten Systemdaten der von Dell EMC gemanagten Geräte sammelt und diese Daten dann mit maximalen Sicherheits- und Datenschutzmaßnahmen behandelt. Folgende Themen werden abgedeckt:

- Erhebung von Gerätedaten vor Ort
- Datenübertragung und Kommunikation
- Datenspeicherung und -nutzung und Prozesse bei Dell Technologies Services

Diagramm A:





Mit den Auditfunktionen von Policy Manager im sicheren Verbindungs-gateway profitieren Kunden von einer zusätzlichen Sicherheitsebene für die Datenerhebung vor Ort

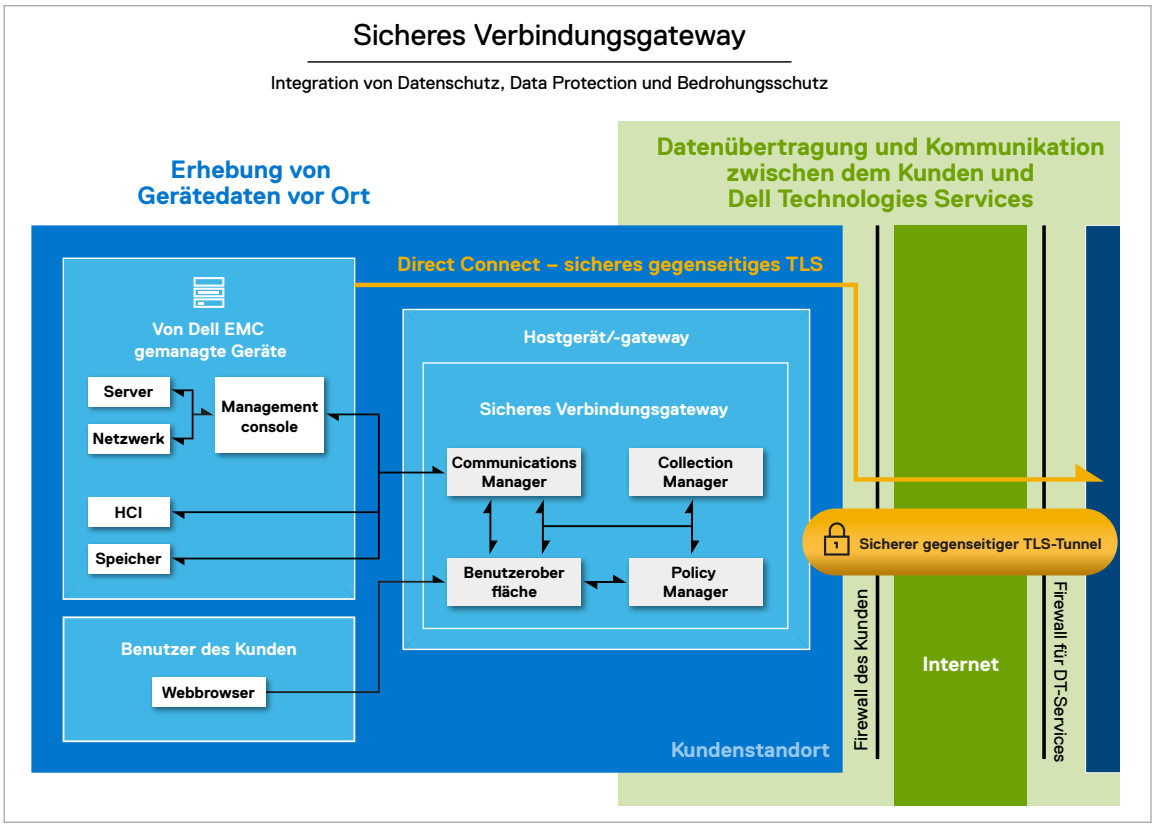
4: Detaillierter Sicherheitsansatz für das sichere Verbindungsgateway

4-1: Sichere Datenerhebung vor Ort

Minimierung der Firewallzugriffspunkte

Das sichere Verbindungsgateway aggregiert die Kommunikation der Dell EMC Geräte und dient als zentraler Eingangs- und Ausgangspunkt in der Firewall des Kunden für alle IP-basierten Remoteserviceaktivitäten (siehe Diagramm B). Durch die Minimierung der Firewallzugriffspunkte für Remote-IT-Supporttechnologie mindert Dell Technologies das Sicherheitsrisiko über die Firewall des Unternehmens.

Diagramm B (Auszug aus Diagramm A – Sicherheitsarchitektur):



Als Gateway vor Ort wird das sichere Verbindungsgateway virtuell auf einem vom Kunden zur Verfügung gestellten Hypervisor bereitgestellt. Jeder Gatewayserver agiert als Proxy und überträgt Informationen an die und von den gemanagten Geräten. Im Fall eines temporären lokalen Netzwerkausfalls kann das sichere Verbindungsgateway auch Connect-Home-Ereignisse in eine Warteschlange einfügen. Diese Gatewayserver verfügen über eine eigene Webbenutzeroberfläche, die auf dem zugrunde liegenden Betriebssystem basiert.

Für einige Kunden ist die Version mit direkter Verbindung zur heterogenen Bereitstellung mehrerer Dell EMC Hardwareprodukte geeignet. Diese Lösung dient als zentraler, sicherer Anlaufpunkt für die Kommunikation über die Firewall des Kunden. Sie ist in die Betriebsumgebung des Produkts integriert und erfordert daher keinen separaten Server für den eingehenden Remotesupport und die Call-Home-Funktionen.

Minimierung der Firewallzugriffspunkte (Fortsetzung)

Für Kunden mit einem PowerEdge-Rechenzentrum, die die OpenManage Enterprise-Systemmanagementkonsole verwenden, ist das integrierte Service-Plug-in eine alternative Implementierungsoption. Dieses Konnektivitäts-Plug-in innerhalb der virtuellen OpenManage Enterprise-Appliance wird auf einem vom Kunden bereitgestellten Hypervisor ausgeführt. Es fungiert als Serviceautomatisierungsschicht von verwalteten Server- und Gehäusegeräten und bietet eine einzige, sichere direkte Verbindung zum Back-end von Dell Technologies Services.

Funktion als sicherer Kommunikationsvermittler

Das sichere Verbindungsgateway fungiert als Kommunikationsvermittler zwischen den gemanagten Geräten, Policy Manager und der Back-end-Support-infrastruktur von Dell Technologies Services. Die Gatewayserver, auf denen die Lösung bereitgestellt wird, sind HTTPS-Handler. Das Gateway nutzt verschiedene Kommunikationsmethoden, einschließlich Geräteer-kennung, Ereignismanagement, Telemetriedate-nerhebung und Telemetriedaten-management. Zu den Nachrichtentypen zählen:

- Heartbeat-Abfrage des Gerätestatus
- Datendateiübertragung (Connect Home)
- Übertragung von Daten zur Lizenznutzung
- Benutzerauthentifizierungsanfragen
- Synchronisierung des Gerätemanagements

Alle Nachrichten werden mithilfe mehrerer Protokolle sicher kodiert. In einem der nächsten Abschnitte gehen wir näher auf die in die Datenkommunikation und -übertragung mit dem sicheren Verbindungsgateway integrierten zusätzlichen Sicherheitsmaßnahmen ein. Hierzu zählen die Verwendung des HTTPS-Protokolls mit End-to-End-TLS-Tunnel (Transport Layer Security) und Verschlüsselung nach Branchenstandard.

Kontrolle der Autorisierungsanforderungen und Zugriffsberechtigungen durch den Kunden

Wenn Geräte vom sicheren Verbindungsgateway im Rechenzentrum eines Kunden überwacht werden, kann der Kunde Autorisierungsanforderungen für Remotezugriffsverbindungen, Diagnoseskriptausführungen und andere zugehörige Aktivitäten mit dem Policy Manager steuern. Kunden können für Mitarbeiter und Ingenieure und Techniker des technischen Supports, die zur Problemdiagnose und -behebung eine Remoteverbindung herstellen, Zugriffsberechtigungen festlegen.

Die Sicherheit für Autorisierung und Berechtigungs-management wird durch die folgenden Funktionen von Policy Manager sichergestellt:

- Das sichere Verbindungsgateway fragt beim Policy Manager regelmäßig Änderungen an den Berechtigungen ab und speichert die Berechtigungen in einem lokalen Cache. Im Fall von Policy Manager gilt:
  - Der Regelsatzcache wird nach dem letzten Abrufzyklus automatisch mit den Konfigurationsupdates aktualisiert.
  - Er ist so konfiguriert, dass er Nachrichten als HTTPS-Listener an einem bestimmten, zuvor vereinbarten Port empfangen kann.
- Wenn beim sicheren Verbindungsgateway eine Remotezugriffsanfrage oder eine andere Aktion eingeht, wird die vom Policy-Manager-Cache empfangene Richtlinie erzwungen.
  - Die Berechtigungen können mit Policys, die auf Gerätetypen oder bestimmten Modellen in einem Gerätetyp basieren, hierarchisch zugewiesen werden.
  - Kunden können die angeforderte Aktion über die Webbenutzeroberfläche von Policy Manager akzeptieren oder ablehnen. Sie können auch mithilfe von Filtern weitere Einschränkungen für Autorisierungen und Aktionen festlegen.

Protokollierung und Auditpfade

Mit den Policy-Manager-Auditfunktionen im sicheren Verbindungsgateway profitieren Kunden von einer zusätzlichen Sicherheitsebene für die Datenerhebung vor Ort. Der Policy Manager erfasst alle Remoteserviceereignisse und -verbindungen, die Ausführung von Diagnoseskripten sowie Übertragungsvorgänge für Supportdateien. Sie werden in der Policy-Manager-Datenbank als Flat-Text-Auditprotokolldateien gespeichert. Policy Manager verfolgt den Zugriff auf sich selbst, Richtlinienänderungen und alle Autorisierungs- oder Zugriffsverweigerungsaktivitäten.

Alle diese Informationen stehen den Kunden wie folgt zur Verfügung:

- Audits werden über die Webbenutzeroberfläche von Policy Manager angezeigt und können nicht bearbeitet werden.
- Auditprotokolle können auch so konfiguriert werden, dass sie an einen Syslog-Server in der Umgebung des Kunden gestreamt werden.

Sicheres Verbindungsgateway

Unterstützte TLS-1.2-Cipher-Suites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Sicherheitsoption für Gerätesteuerung

Da Kunden nicht immer den Policy Manager für das Autorisierungs- und Berechtigungsmanagement aktivieren, stellt das sichere Verbindungsgateway die entsprechenden Sicherheitsfunktionen über die Option zur Gerätesteuerung bereit.

Kunden haben folgende Möglichkeiten:

- Sie können anhand von Gerätetyp, Administratorgruppe, Organisation oder Geschäftseinheit, physischem Standort des Geräts oder anderen selbst gewählten Kriterien individuelle Gruppen erstellen.
- Sie können konkrete Berechtigungen und Zugriffsrechte für diese Gerätegruppen definieren.

Alle Vorgänge des Gerätemanagements, einschließlich Remoteaktivitäten durch Mitarbeiter des technischen Supports, werden protokolliert. Sie müssen auch am Back-end durch einen Mitarbeiter des technischen Supports genehmigt werden.

Auf diese Weise erhalten Kunden die volle Kontrolle und Transparenz für die über das sichere Verbindungsgateway gemanagten Geräte.

Zwei-Faktor-Authentifizierung und Management digitaler Zertifikate

Die Authentifizierung ist eine wichtige Komponente der sicheren Datenerhebung vor Ort. Das sichere Verbindungsgateway verwendet ein digitales Zertifikat als Identitätsnachweis für die Bereitstellung auf dem Gatewayserver des Kunden. Das Zertifikat bindet die Identität des Gatewayservers an ein Schlüsselpaar, das zur Verschlüsselung und Authentifizierung der Kommunikation mit dem Back-end verwendet wird. Die Zertifizierungsstelle (Certificate Authority, CA) von Dell Technologies Services ist das zentrale Repository für die Schlüsselinfrastruktur des sicheren Verbindungsgateways.

Das Management digitaler Zertifikate wird zur Automatisierung der Registrierung des digitalen Zertifikats über unsere private Zertifizierungsstelle verwendet. Dies bewirkt Folgendes:

- Die programmatische Generierung und Authentifizierung jeder Zertifikatsanforderung wird ermöglicht.
- Es wird sichergestellt, dass das Zertifikat nur auf dem Gatewayserver ausgestellt und installiert wird. Das Zertifikat kann nicht auf einen anderen Computer kopiert und dort verwendet werden.

Das sichere Verbindungsgateway verbindet und authentifiziert sich mit dem in unserer Back-end-Supportinfrastruktur bereitgestellten digitalen Zertifikat. Mitarbeiter des technischen Supports stellen per Zwei-Faktor-Authentifizierung in der Umgebung des Kunden eine Verbindung mit dem sicheren Verbindungsgateway her.

4-2: Sichere Datenübertragung und Kommunikation

Sicherer Kommunikationstunnel

Die gesamte Kommunikation zwischen dem Kunden und der Dell Technologies Services Back-end-Supportinfrastruktur wird durch Sicheres Verbindungsgateway vom Standort des Kunden initiiert. So wird ein sicherer End-to-End-Kommunikationstunnel mit TLS-256-Bit-Verschlüsselung (Transport Layer Security) nach Branchenstandard über das Internet erstellt und es erfolgt eine Authentifizierung des digitalen Zertifikats mit Signatur von Dell Technologies Services. Letzteres wird im vorhergehenden Abschnitt zur sicheren Datenerhebung vor Ort detailliert beschrieben.

Dementsprechend haben Verbindungen über das sichere Verbindungsgateway folgende Eigenschaften:

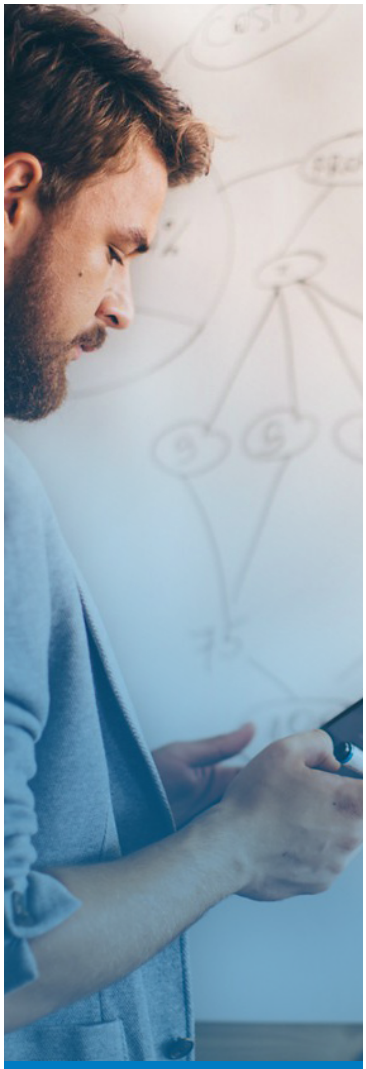
- **Zuverlässige Datenübertragung:** Jede übermittelte Nachricht umfasst eine Nachrichtenintegritätsprüfung mithilfe eines Nachrichtenauthentifizierungscodes. So werden unbemerkte Datenverluste oder -manipulationen bei der Übertragung verhindert.
- **Private, sichere Sitzung über TLS:** Im Zuge der symmetrischen Verschlüsselung mit Algorithmen nach Branchenstandard werden eindeutige Schlüssel für jede Verbindung generiert. Die Kommunikation kann während der Verhandlung nicht unbemerkt geändert werden.
- **Authentifizierte Parteien:** Da diese Verbindung sicher ist, identifiziert sie die kommunizierenden Parteien und authentifiziert sie mithilfe von Kryptografie mit öffentlichen Schlüsseln. Dieser Ansatz verhindert Spoofing und MITM-Angriffe (Man-in-the-Middle-Angriffe).

Kommunikation durch den sicheren TLS-Tunnel

Der Gatewayserver gewährleistet mithilfe des TLS-Tunnels eine sichere Umgebung für die folgenden Funktionen: Heartbeat-Abfragen, Remotebenachrichtigungen und Remotezugriff. In diesem Abschnitt und in Diagramm C werden diese zentralen Kommunikationsprozesse und -protokolle für die automatisierte, proaktive und vorausschauende Erfahrung mit unserer Technologie näher erläutert.

Heartbeat-Abfrage

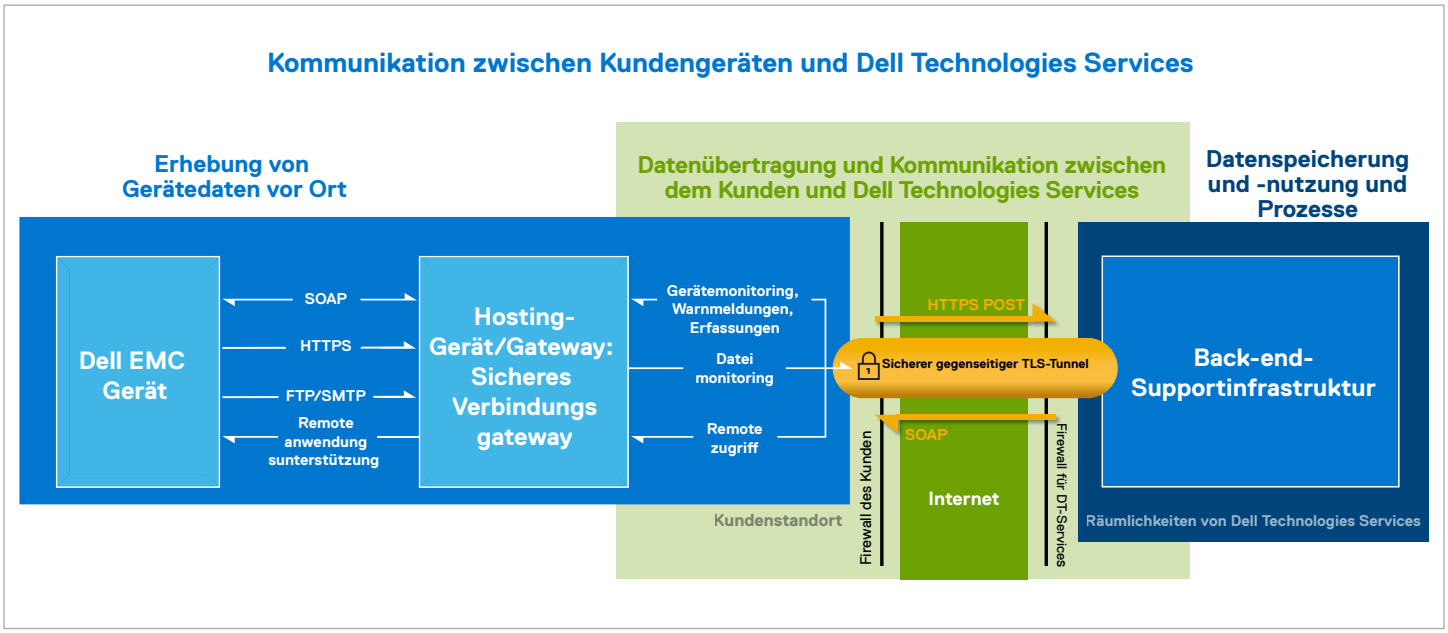
Kundensysteme müssen verbunden sein, um vom sicheren Verbindungsgateway profitieren zu können. Per Heartbeat-Abfrage wird der Verbindungsstatus von Geräten überprüft und die gesammelten Telemetriedaten werden regelmäßig an das Back-end kommuniziert. Die Daten identifizieren außerdem den Gatewayserver, auf dem das sichere Verbindungsgateway bereitgestellt wurde.



Die branchenführende Authentifizierung schützt Verbindungen vor Spoofing und Man-in-the-Middle-Angriffen.

Kommunikation durch den sicheren TLS-Tunnel (Fortsetzung)

Diagramm C: Sicherheitsarchitektur



Remotebenachrichtigung oder Connect-Home-Funktion

Das sichere Verbindungsgateway dient als sichere Brücke, über die Geräte Ereignisdateien an das Back-end senden. Dies umfasst Fehler, Warnmeldungen, Warnbedingungen, Zustandsberichte, Konfigurationsdaten und den Status der Skriptausführung.

- Wenn eine Warnmeldung generiert wird, wird eine Ereignisdatei generiert und an das sichere Verbindungsgateway gesendet.
- Die Datei wird vom sicheren Verbindungsgateway über die HTTPS-Listener-Services empfangen.
- Für Legacy-Produkte, die FTP- und/oder SMTP-Listener für das sichere Verbindungsgateway verwenden, werden die Dateien verschlüsselt und übertragen.
- Das Gateway komprimiert die Datei und sendet sie durch den TLS-Tunnel an das Back-end. Anschließend wird die Datei aus dem Listener-Verzeichnis gelöscht.
- Die Datei wird dann am Back-end zur Analyse dekomprimiert.
- Das sichere Verbindungsgateway kann die Dateien auch durch den verschlüsselten Kommunikationstunnel an das Back-end senden. Darüber hinaus kann das Gateway so konfiguriert werden, dass die Failover-Kanäle verwendet werden, d. h. FTPS oder der E-Mail-Server des Kunden.

Die Systemmonitoringdaten von verschiedenen Komponenten eines aktiven Systems werden gesammelt, damit Dell Technologies Services eine adaptive, intelligente und beschleunigte Supporterfahrung bereitstellen kann. Die System-ID, die zur Identifizierung des betreffenden Systems erforderlich ist, ist die einzige Angabe zum Unternehmen, die von den Geräten erfasst wird. Wenn wir feststellen, dass ein Ersatzteil proaktiv versendet werden sollte, verwenden wir vorhandene Kontaktinformationen, die sicher auf Dell Technologies Servern gespeichert wurden.

Eine vollständige Liste der System-monitoringsdaten, die von einem aktiven System erfasst werden, einschließlich der außerhalb des routinemäßigen 24-Stunden-Zyklus erfassten Daten, finden Sie in den Dokumenten „Reportable Items“ für das sichere Verbindungsgateway und das Services-Plug-in für OpenManage Enterprise.

Remotezugriff

Unsere technischen Supportteams greifen auch remote auf die Geräte an einem Kundenstandort zu, um Probleme zu beheben oder gerätespezifische Aktionen durchzuführen. Durch asynchrones Messaging wird sichergestellt, dass die Remotezugriffssitzung durch das sichere Verbindungsgateway vom Kundenstandort aus initiiert wird. Als Nächstes wird folgendermaßen eine sichere Remotezugriffssitzung erstellt:

- Nach der Sitzungsauthentifizierung am Back-end von Dell Technologies Services fordert ein Mitarbeiter des technischen Supports Gerätezugriff an. Er nennt dabei die Service-Request-Nummer (sofern verfügbar) und andere Geräte- oder Benutzerkennungen.
- Die Remotezugriffsanfrage wird am Back-end in die Warteschlange gestellt, bis das Gateway die Heartbeat-Nachricht des Geräts an das Back-end sendet, um sie abzurufen.
- Daraufhin sendet der Back-end-Server eine Antwort mit Anforderungsinformationen, der Back-end-Serveradresse und einer eindeutigen Sitzungs-ID zum Herstellen der Verbindung zum Gateway.
- Das sichere Verbindungsgateway verwendet das lokale Repository zum Ermitteln der lokalen IP-Adresse des Geräts. Anschließend werden anhand der vom Policy Manager zwischengespeicherten Policy die Verbindungsberechtigungen überprüft.
- Wenn zulässig, stellt das sichere Verbindungsgateway eine separate persistente TLS-Verbindung zum Back-end-Server her. Die TLS-Verbindung wird immer vom Gateway initiiert. Der Back-end-Server kann keine eingehende Verbindung zum Gateway-Server initiieren. Auf diese Weise wird sichergestellt, dass keine Sicherheitslücken für externe Angriffe vorhanden sind.

Die Kommunikation fließt durch den Tunnel zwischen dem sicheren Verbindungsgateway und dem Back-end-Server, bis sie beendet wird oder nach einem Zeitraum der Inaktivität ein Timeout auftritt.

Netzwerksicherheit

Alle Netzwerkmonitoringkomponenten befinden sich hinter einer Firewall und werden von unserem Netzwerksicherheitsteam gemanagt. Der Netzwerkdatenverkehr wird streng kontrolliert. Der gesamte eingehende Datenverkehr wird über bestimmte Ports übertragen und nur an die entsprechenden Adressen im Zielnetzwerk gesendet.

4-3: Sicherer Daten-Storage sowie sichere Datennutzung und -prozesse

Sicherheit bei Speicherung und Nutzung

Physische Sicherheit

Dell Technologies Services hostet die meisten Daten zum sicheren Verbindungsgateway, einschließlich der Anwendungs-, System-, Netzwerk- und Sicherheitskomponenten, in einem Rechenzentrum in den USA, das auf hohe Verfügbarkeit und Sicherheit ausgelegt ist. Die Daten werden durch zahlreiche Maßnahmen geschützt, u. a. durch physische Sicherheit. Hier einige der verwendeten Funktionen:

- Sicherheitskräfte vor Ort
- Kameras
- Falsche Eingänge
- Fahrzeugsperren
- Spezielle Parkplätze
- Panzerglas und durchschusshemmende Wände
- Einsatz eines nicht gekennzeichneten Gebäudes

Zu den Rechenzentren, in denen sich die Infrastruktur befindet, haben nur autorisierte Mitarbeiter Zugang. Dies wird mit Smartcards kontrolliert.

Logische Sicherheit

Die vom sicheren Verbindungsgateway generierten Daten werden gemäß der Dell Datenschutzerklärung gespeichert.

Der logische Zugriff auf die Infrastruktur von Dell Technologies Services (Server, Lastausgleich, Netzwerkfreigaben usw.) wird durch interne Tools eingeschränkt, die gemäß den IT-Richtlinien geprüft und bewertet werden:

Logische Sicherheit (Fortsetzung)

- **Server- und Datenbanksicherheit:** Server und Betriebssystemkomponenten befinden sich auf standardmäßigen Images, die Sicherheitsüberprüfungen unterzogen wurden. Es finden regelmäßige Überprüfungen der von der Anwendung verwendeten Sicherheitsupdates statt, einschließlich der von Microsoft und anderen Softwareanbietern veröffentlichten Updates. Wenn wichtige Sicherheitsupdates veröffentlicht werden, werden sie zunächst auf Nicht-Produktions-Images getestet und in der Regel zeitnah auf die Liveserver angewendet, um Risiken zu vermeiden.
- **Audits:** Proprietäre Protokolle aus dem Gerätemonitoring werden beibehalten, sind jedoch nur für autorisierte Infrastruktur und Anwendungen von Dell Technologies Services zugänglich. In diesen Protokollen werden alle Versuche zur Anmeldung oder zum Zugriff auf das Betriebssystem oder die Webserverkonsole des sicheren Verbindungsgateways aufgezeichnet.

Die von der IT gemanagten Builds werden gemäß den von CIS (Center for Internet Security) empfohlenen Best Practices für Sicherheit gehärtet. Sicherheitsrichtlinien nach Branchenstandard werden auch auf allen Servern und Netzwerkkomponenten implementiert.

Und schließlich werden in der Umgebung mit dem sicheren Verbindungsgateway sowohl lokale hohe Verfügbarkeit innerhalb des Rechenzentrums als auch eine identische Infrastruktur in einem separaten Rechenzentrum verwendet. Die einzigen Ausnahmen bilden Technologien, die an sich schon hoch verfügbar sind, beispielsweise Big Data-Cluster und Private Clouds. Für Data Analytics nutzt Dell Technologies Services Cloud-Umgebungen, die wir vollständig kontrollieren und managen, einschließlich Private Clouds, Hybrid Clouds und Public Clouds.

Wir nutzen einen reproduzierbaren, sicheren Entwicklungsprozess für Produkte und Anwendungen.

Authentifizierung

Das sichere Verbindungsgateway verwendet Dell MyAccount für die Authentifizierung bei Dell Technologies Services und Betriebssystemanmeldegruppen für die On-the-Box-Authentifizierung.

Gruppen wie dem Datenbankadministrationsteam und dem operativen Supportteam, die Zugriff auf Komponenten des sicheren Verbindungsgateways haben, werden separate Aufgaben und Zugriffsrechte zugewiesen. Alle Updates für die Produktionsumgebung durchlaufen ein festgelegtes Änderungskontrollverfahren, das Prüfungen und Ausgleichsverfahren beinhaltet.

Sicherheit für Prozesse

Sicherheitsbewusste Community

Wir bieten einen mehrstufigen rollenbasierten Sicherheitsschulungslehrplan, um neue und vorhandene Mitarbeiter über die job-spezifischen Best Practices für die Sicherheit und die Verwendung relevanter Ressourcen zu informieren. Dell Technologies ist bestrebt, eine sicherheitsbezogene Kultur in der gesamten Community zu schaffen. Darüber hinaus ist unsere Entwicklercommunity Teil des Security Champion-Programms von Dell, das Shift Left Security in unseren Softwareentwicklungspraktiken fördern soll.

Entwicklung

Unser interner **SDL (Secure Development Lifecycle Standard)** ist eine gemeinsame Referenz, die die Produktorganisationen von Dell Technologies für Benchmarks von sicheren Produkt- und Anwendungsentwicklungsaktivitäten im Vergleich mit den Erwartungen am Markt und den in der Branche gängigen Verfahren nutzen. Im SDL werden Sicherheitskontrollen festgelegt, die die Produktteams beim Entwickeln neuer Funktionen nutzen sollen. Er deckt Analyseaktivitäten und vorgeschriebene proaktive Kontrollen in den wichtigsten Risikobereichen ab. Mit den Analyseaktivitäten, beispielsweise Bedrohungsmodellierung, statische Codeanalysen, Scans und Sicherheitstests, sollen Sicherheitsmängel im gesamten Entwicklungslebenszyklus erkannt und behoben werden. Die vorgeschriebenen Kontrollen sollen sicherstellen, dass die Entwicklungsteams beim Programmieren defensiv vorgehen und so bestimmte gängige Sicherheitsprobleme vermeiden – u. a. diejenigen aus den Top 10 von OWASP (Open Web Application Security Project) oder den Top 25 von SANS. Das sichere Verbindungsgateway hat

Entwicklung (Fortsetzung)

das Dell SDL Maturity Framework zur Implementierung von Sicherheitskontrollen in Übereinstimmung mit Branchenstandards übernommen.

Der Code für das sichere Verbindungsgateway wird mit der Methodik der agilen Softwareentwicklung entwickelt. Der Code wird kontinuierlich mit Automatisierungssoftware nach Branchenstandard integriert. Die Codeversionen werden mithilfe von sicheren Gruppenberechtigungen eingecheckt und kontrolliert.

Jede Softwareversion durchläuft in Übereinstimmung mit unseren Sicherheits-Policies eine Sicherheitsbewertung. Diese umfasst Folgendes:

- Bewertung von Sicherheitslücken durch Penetrationstests
- Drittanbieter-Sicherheitstests mit mehreren erstklassigen Anbietern, beispielsweise Secureworks
- Bewertung für Authentifizierungs-, Autorisierungs- und Identitätsmanagementlösungen
- Alle Bibliotheken und Komponenten von Drittanbietern werden mit branchenführenden Lösungen für die Softwarekompositionsanalyse gescannt. Außerdem werden Dell Security Advisories für bestimmte Sicherheitsverbesserungen kommuniziert.
- Datenklassifizierung mit unserer globalen Sicherheits-organisation. Dieser Prozess vereint Datenschutz und Sicherheit zum Schutz elektronischer Daten.

Die Anwendungen werden auch Sicherheitsaudits und Governance unterzogen.

Changemanagement

Der Changemanagementprozess von Dell Technologies entspricht den von unserem unternehmenseigenen Change Management Board vorgegeben den Best Practices der ITIL Foundation. Alle Änderungen werden über Änderungsanfor-derungstickets gemanagt. Nutzer, die zum Initiieren von Änderungen auf unser System zugreifen, müssen an ITIL-Schulungen teilnehmen und sich mit dem SDL vertraut machen. Bei allen auf die Back-end-Infrastruktur angewendeten Updates und Upgrades erfolgt eine Versionskontrolle für die ordnungsgemäße Nachverfolgung und Rückverfolgbarkeit. Das Team verwendet einen automatisierten Build-Prozess zum Anwenden neuer Builds bzw. zum Widerrufen von bereitgestellten Builds oder Hotfixes.

Für die am Standort des Kunden installierte Anwendung kann je nach Kundenwunsch ein Upgrade erfolgen. Jede auf Dell.com/support hochgestufte Version enthält Informationen zu den eingeführten Änderungen und ggf. bekannten Einschränkungen.

Alle neuen Funktionen und Änderungen werden von unserem Produktmanagementteam gepflegt und mit einem Planänderungsprozess priorisiert, der vom Change Control Board überprüft und genehmigt werden muss.

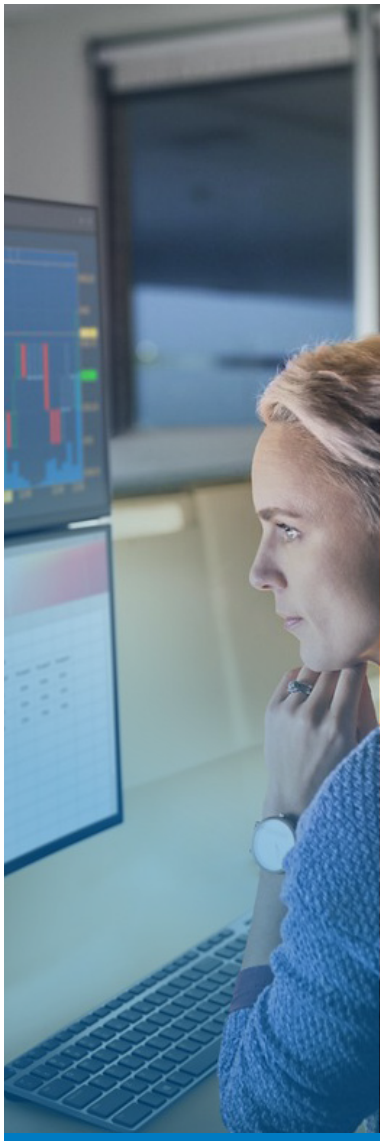
Risikomanagement für Lieferketten

Dell Technologies befolgt in jeder Phase des Lebenszyklus aus Planung, Beschaffung, Erstellung, Auslieferung und Rückgabe branchenführende Best Practices. Wir haben einen umfassenden Ansatz zum Schutz unserer Lieferkette, einschließlich der Förderung internationaler SCRM-Standards und Best Practices, damit wir am internationalen Markt weiterhin als zuverlässiger ICT-Lieferant gelten.

Weitere Informationen über unsere Verfahren für Assurance in der Lieferkette finden Sie hier.

Incident Reporting

Jeder Mitarbeiter von Dell Technologies, der verdächtige Aktivitäten beobachtet oder ein Problem mit der Cybersicherheit oder eine Bedrohung vermutet, ist verpflichtet, diesen Incident sofort unserem CSIRT (Incident Response Team) zu melden. Dies umfasst auch eine Schwäche oder Lücke in einem Sicherheitsprozess, die sich auf unsere Umgebung auswirken können oder zu einem Verstoß gegen Systeme und/oder Daten führen könnte. Das CSIRT startet dann eine vollständige Untersuchung des Incident und die Person, die den Incident meldet, stellt alle Artefakte und Details bereit, die zur Durchführung der Ermittlungen durch das CSIRT erforderlich sind. Das CSIRT-Team verwendet den CSIRT Incident Response Plan, in dem ein formeller Prozess für die Reaktion auf Dell interne und nicht kundenbezogene Cybersicherheits-Incidents und deren Behebung erläutert wird. Diese Incidents können potenzielle Bedrohungen für Dell Ressourcen, Computernetze oder Datenverarbeitungsgeräte sowie für Dell und die entsprechenden Tochtergesellschaften, Mitarbeiter, Serviceanbieter, Partner oder Kundendaten darstellen.



Branchenweite Zusammenarbeit an Best Practices für die Produkt-sicherheit

Reaktion auf Sicherheitslücken

Dell Technologies möchte Kunden bei der Minimierung von Risiken im Zusammenhang mit Sicherheitslücken in unseren Produkten unterstützen. Zu diesem Zweck stellen wir Kunden zeitnah Informationen, Hilfestellung und Gegenmaßnahmen zu Bedrohungen durch Sicherheitslücken zur Verfügung. Unser PSIRT (Product Security Incident Response Team) ist für die Koordination der Antwort und die Offenlegung bei allen uns gemeldeten Sicherheitslücken in Produkten zuständig. Alle offengelegten Sicherheitslücken in Dell Technologies Produkten sind online verfügbar.

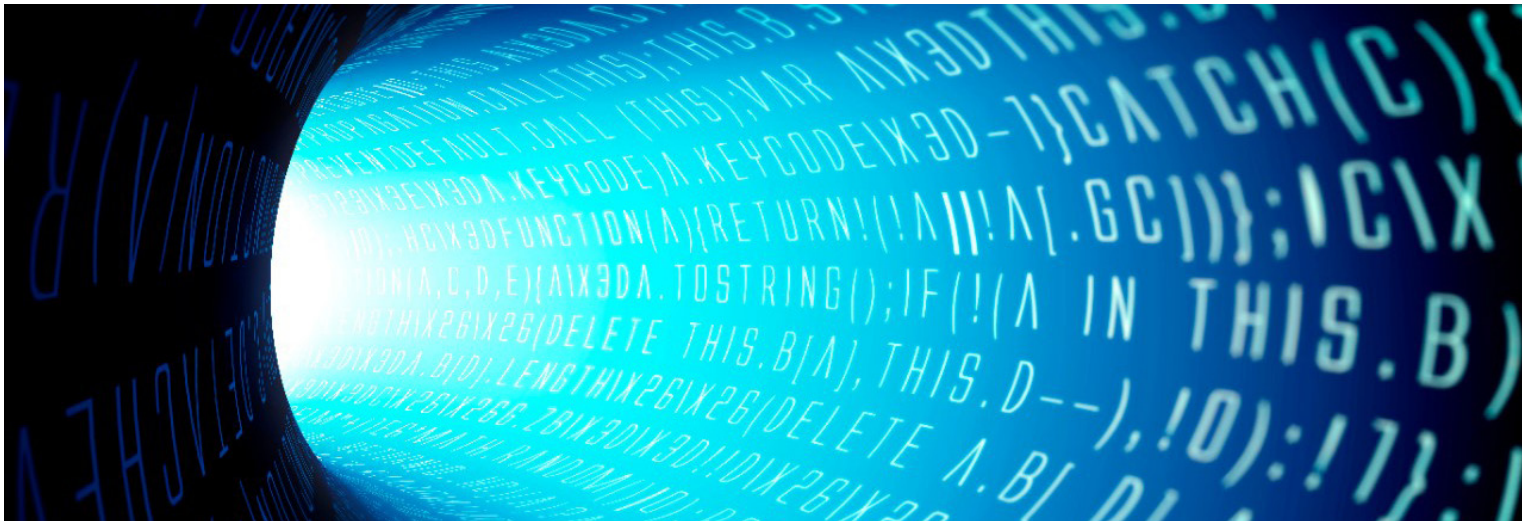
Weitere Informationen zu unserer Policy für die Reaktion auf Sicherheitslücken

Branchenmitgliedschaften

Dell Technologies ist Mitglied in mehreren branchenweiten Gruppen für die Zusammenarbeit mit anderen führenden Anbietern. Gemeinsam definieren, optimieren und teilen wir Best Practices für die Produktsicherheit und treiben die sichere Entwicklung weiter voran. Beispiele für die Zusammenarbeit in der Branche:

- In Gestalt der Entität EMC hat Dell SAFECode (Software Assurance Forum for Excellence in Code) mitbegründet und führt dort aktuell den Vorsitz im Vorstand. Zu den übrigen Vorstandsmitgliedern zählen Microsoft, Adobe, SAP, Intel, Siemens, CA und Symantec. Die Mitglieder von SAFECode teilen und veröffentlichen Verfahren und Schulungen für Software Assurance.
- Dell Technologies ist aktives Mitglied von FIRST (Forum for Incident Response and Security Teams). FIRST ist eine führende Organisation, die als weltweit führend bei Incident Response und bei der Reaktion auf Sicherheitslücken gilt.
- Wir beteiligen uns aktiv am OTTF (Open Group Trusted Technology Forum). Das OTTF fördert die Entwicklung eines globalen Lieferkettenintegritätsprogramms mit einem zugehörigen Framework.
- Dell war 2008 eines der ersten neun vom BSIMM-Projekt (Building Security In Maturity Model) bewerteten Unternehmen und beteiligt sich auch weiterhin am Projekt. Ein Vertreter von Dell Technologies sitzt im BSIMM Board of Advisors.
- Dell Mitarbeiter waren Gründungsmitglieder des IEEE Center for Secure Design, das im Rahmen der IEEE Cybersicherheitsinitiative eingeführt wurde, um Softwarearchitekten zu helfen, gängige Mängel beim Sicherheitsdesign zu verstehen und zu beheben.

Besuchen Sie unser Security and Trust Center, um Ressourcen und Lösungen zu finden, die Ihnen bei der Suche nach Antworten auf Ihre Fragen zur Unternehmenssicherheit behilflich sind.



Branchenspezifische Sicherheitsstandards

Unsere Mitarbeiter sind aktiv an Normungsgremien und Branchenkonsortien beteiligt, die sich auf die Entwicklung von Sicherheitsstandards und auf die Definition branchenweiter Sicherheitsverfahren konzentrieren. Hierzu zählen:

- CSA (Cloud Security Alliance)
- DMTF (Distributed Management Task Force)
- FIRST (Forum for Incident Response and Security Teams)
- INCITS (InterNational Committee for Information Technology Standards)
- ISO (International Organization for Standardization)
- IETF (Internet Engineering Task Force)
- The Open Group
- OASIS (Organization for the Advancement of Structured Information Standards)
- SAFECode (Software Assurance Forum for Excellence in Code)
- SNIA (Storage Networking Industry Association)

ISO 9001-Zertifizierung

Dell Technologies ist nach ISO 9001 zertifiziert. Das Unternehmen führt regelmäßige vierteljährliche Audits und Complianceprüfungen für alle seine Entwicklungs- und Fertigungszentren durch.

5: Fazit

Unsere Konnektivitätstechnologie bietet eine mühelose IT-Supporterfahrung mit automatisierten proaktiven und vorausschauenden Warnmeldungen, die maximale Verfügbarkeit für kritische Rechenzentrumsinfrastrukturen gewährleisten. Kunden, die mit Dell Technologies Services zusammenarbeiten, können sich darauf verlassen, dass wir eine zuverlässig private und sichere Erfahrung für die Erfassung, Kommunikation, Übertragung, Nutzung und Speicherung ihrer Telemetriedaten bereitstellen.

Wenn Sie Fragen haben oder weitere Informationen benötigen, besuchen Sie **DellTechnologies.com/SecureConnectGateway**

1 Quelle: „The Role Of IT Services Providers Expands To Strategic Collaboration", eine von Forrester Consulting im Auftrag von Dell Technologies im April 2021 durchgeführte Studie

2 Quelle: Weltwirtschaftsforum, Global Risks Report 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf