cpl.thalesgroup.com/de

THALES
Building a future we can all trust

Lösungen von Thales zur Verhinderung von Ransomware-Angriffen

Diese Lösungen von Thales erfüllen die Vorgaben des NIST Cybersecurity Framework – wir beraten Sie, wie Sie Ransomware-Angriffe vermeiden

Ransomware-Angriffe sind seit vielen Jahren ein Problem, aber besonders in jüngster Zeit verursachen sie deutlich mehr Schäden. Die Ziele der Kriminellen sind vielfältig – von kritischer Infrastruktur bis hin zu Krankenhäusern und dem Einzelhandel – und es werden zweistellige Millionenbeträge als Lösegeld gefordert. Heute, da die führenden Politiker der Welt diese Angriffe auf hochrangigen Gipfeltreffen erörtern, übernehmen die Regierungsbehörden eine aktive Rolle bei der Aufklärung und der Bereitstellung von Ressourcen für Unternehmen und Organisationen, um sich vor Angriffen zu schützen.

NIST-Leitfaden zur Verhinderung von Ransomware-Angriffen

Das National Cybersecurity Center of Excellence (NCCoE) hat unter Schirmherrschaft des National Institute of Standards and Technology (NIST) einen Leitfaden herausgegeben, der erläutert, wie Datenbestände identifiziert und vor Ransomware geschützt werden können. Die Cybersecurity Special Publication (SP) 1800-25 legt die Schritte dar, die für eine umfassende Strategie zum Schutz von Datenbeständen erforderlich sind. Sie zeigt zudem, dass es kein Patentrezept gegen die Bedrohungen durch Ransomware gibt.

Lösungen von Thales zur Vorbeugung von Ransomware

Die Lösungen für Datensicherheit und Zugriffsverwaltung von Thales erfüllen die wesentlichen Vorgaben des Leitfadens zur Cybersicherheit von NIST zum Schutz von Unternehmen vor Ransomware. Das branchenführende Portfolio von Thales versetzt Unternehmen in die Lage:

- sensible Daten zu erkennen und entsprechend ihres Risikos zu klassifizieren
- robuste Kontrollen der Identitäts- und Zugriffsverwaltung einzuführen
- sensible Data-at-Rest und Data-in-Transit mithilfe von Verschlüsselung und Tokenisierung zu schützen und zu kontrollieren
- die Datensicherheit durch intelligente Gegenmaßnahmen zu gewährleisten

Im Folgenden finden Sie einen Überblick, inwieweit unsere Lösungen dem Leitfaden zur Cybersicherheit von NIST entsprechen, sowie Empfehlungen zu Ransomware

Diese Lösungen von Thales erfüllen die Vorgaben des NIST Cybersecurity Framework – wir beraten Sie, wie Sie Ransomware-Angriffe vermeiden

Kategorie	Anforderung	Lösungen von Thales
IDENTIFIZIEREN **Risikobewertung (ID.RA)**	ID.RA-1: Gefährdete Daten werden identifiziert und dokumentiert.	**Thales CipherTrust Data Discovery and Classification** lokalisiert strukturierte und unstrukturierte sensible Daten, die Vorschriften unterliegen – in der Cloud, in Big Data und in traditionellen Datenspeichern. Über eine einzige Oberfläche erhalten Sie einen umfassenden Einblick in Ihre sensiblen Daten und den Grad der Gefährdung. Auf diese Weise können Sie bessere Entscheidungen hinsichtlich möglicher Sicherheitslücken treffen, Maßnahmen priorisieren und Ihre Cloud-Transformation und den Datenaustausch mit Dritten sichern.
SCHÜTZEN **Zugriffskontrolle (PR.AC)**	PR.AC-1: Identitäten und Zugangsdaten werden ausgestellt, verwaltet, verifiziert, widerrufen und für berechtigte Geräte, Benutzer und Prozesse geprüft. PR.AC-3: Fernzugriff wird verwaltet. PR.AC-4: Zugangsberechtigungen und Autorisierungen werden unter Einbeziehung des Least-Privilege-Prinzips und der Aufgabentrennung verwaltet.	**SafeNet Trusted Access bietet zentrales Zugriffsmanagement**, mit dem Unternehmen über verschiedene Plattformen hinweg einheitliche Authentifizierungsrichtlinien verfolgen können, indem sie die Bereitstellung und Verwaltung eines verteilten Tokenbestands automatisieren und vereinfachen sowie gleichzeitig eine Vielzahl an On-Premises-, Cloud-basierten oder virtuellen Ressourcen sichern. **SafeNet Trusted Access bietet außerdem serienmäßig Multi-Faktor-Authentifizierung** mit der größten Auswahl an Authentifizierungsmethoden und Formfaktoren an. So können Kunden verschiedene Anwendungsfälle, Sicherheitsniveaus und Bedrohungsvektoren mit einheitlichen, zentral verwalteten Richtlinien angehen, die über ein in der Cloud oder vor Ort bereitgestelltes Authentifizierungs-Backend verwaltet werden. **CipherTrust Transparent Encryption kontrolliert den Zugriff** auf Ihre unternehmenskritischen Daten engmaschig und legt fest, wer Zugriff auf bestimmte geschützte Dateien/Ordner hat und wer welche Operationen durchführen darf. • Verhindern Sie, dass Administratoren ihre Privilegien missbrauchen, um Lesezugriff auf sensible Dateien oder Datenbanken zu erlangen. • Erstellen Sie strikte Richtlinien, um den Zugriff auf Backup-Archive zu kontrollieren, und verschlüsseln Sie Sicherungskopien, um die Exfiltration von Daten zu verhindern. • Führen Sie Aufgabentrennung ein, sodass Datenbanknutzern Lese-/Schreibzugriff gewährt wird, während Backup-Software nur Leserechte für die entsprechende Datenbank hat.

Kategorie	Anforderung	Lösungen von Thales
SCHÜTZEN **Datensicherheit (PR.DS)**	PR.DS-1: Data-at-Rest sind geschützt	**Die CipherTrust Data Security Platform** kombiniert Datenerkennung und -klassifizierung, Datenschutz sowie unerreichte granulare Zugriffskontrollen mit zentraler Schlüsselverwaltung – alles auf einer einzigen Plattform. Dadurch müssen für die Sicherung von Daten und allgegenwärtige Compliance-Kontrollen weniger Ressourcen bereitgestellt werden und die Risiken für Ihr gesamtes Unternehmen reduzieren sich deutlich. • **CipherTrust Transparent Encryption** bietet Data-at-Rest-Verschlüsselung, Kontrolle von privilegierten Benutzerzugriffen und detaillierte Audit-Protokollierung für Datenzugriffe, ohne dass Änderungen an bestehenden Anwendungen vorgenommen werden müssen. IT-Organisationen können so Richtlinien aufstellen, um zu verhindern, dass betrügerische Prozesse und unbefugte Benutzer Ihre sensibelsten Daten entschlüsseln und diese nach Exfiltration offengelegt werden. Dadurch schützen sie Unternehmen vor Ransomware-Angriffen. Agenten schützen die Daten in Dateien, Beständen und Datenbanken auf Windows-, AIX- und Linux-Betriebssystemen auf physischen und virtuellen Servern in der Cloud und in Big-Data-Umgebungen. • **CipherTrust Application Data Protection** bietet Kryptofunktionen wie Schlüsselverwaltung, Signieren, Hashing und Verschlüsselungsdienste über APIs an, damit Entwickler Daten problemlos auf dem Anwendungsserver oder dem Big-Data-Knoten sichern können. • **CipherTrust Tokenization** wird als Lösung mit und ohne Vault angeboten und kann zur Reduzierung der Kosten und Komplexität der Einhaltung von Datenschutzvorschriften wie PCI DSS beitragen. • **Die Lösungen von CipherTrust Database Protection** integrieren Datenverschlüsselung für sensible Felder in Datenbanken mit sicherer zentraler Schlüsselverwaltung. Eine Änderung der Datenbankanwendungen ist nicht erforderlich. CipherTrust Database Protection unterstützt Oracle, Microsoft SQL Server sowie IBM DB2- und Teradaten-Datenbanken. • **Der CipherTrust Manager ist die zentrale Verwaltung der Plattform**. Er ermöglicht Unternehmen, kryptographische Schlüssel zentral zu verwalten, granulare Zugriffskontrollen bereitzustellen und Sicherheitsrichtlinien festzulegen. Der CipherTrust Manager verwaltet Schlüssel über ihren gesamten Lebenszyklus einschließlich Erstellung, Zerstörung, Import und Export, stellt rollenbasierte Zugriffskontrolle für Schlüssel und Richtlinien bereit, unterstützt zuverlässige Prüfung und Berichterstattung und bietet entwicklerfreundliche REST APIs. Er ist FIPS-140-2-konform bis Level 3 und als physisches Gerät sowie als virtuelle Anwendung erhältlich. **Luna Hardware-Sicherheitsmodule** erstellen, speichern, schützen und verwalten kryptographische Schlüssel zur Sicherung sensibler Daten und kritischer Anwendungen. Luna HSM verfügen über die meisten Zertifikate der Branche einschließlich Common Criteria, FIPS 140-2 Level 3, ITI und weitere. Die international anerkannten, zertifizierten HSM bieten Ihrer Infrastruktur ein kryptographisches Fundament, dem Sie voll und ganz vertrauen können. Die Luna HSM von Thales dienen als Vertrauensanker für vorhandene und neue Technologien einschließlich Public Key Infrastructure (PKI) sowie als sicherer Speicherort der Schlüssel für Code Signing, um die Integrität des Code zu erhalten. Thales bietet zudem eine maßgeschneiderte Code-Signing-Lösung für Unternehmen an, die auf Luna HSM, Container und REST API beruht und on-premises, als Cloud-HSM-Dienst und in hybriden Umgebungen bereitgestellt werden kann. **Data Protection on Demand (DPoD)** ist eine Cloud-basierte Plattform, auf der eine breite Auswahl von Cloud-HSM und Schlüsselverwaltungsdiensten über einen einfachen Online-Marktplatz angeboten wird.

Kategorie	Anforderung	Lösungen von Thales
SCHÜTZEN Datensicherheit (PR.DS)	PR.DS-2: Data-in-Transit werden geschützt.	**Thales High Speed Encryptors** sind die ideale zertifizierte und bewährte Lösung zur Sicherung von Data-in-Motion einschließlich zeitkritischer Voice- und Videostreams für Unternehmen und Regierungsbehörden: • Network Encryptors der CN-Reihe sind Netzwerkgeräte, die Data-in-Transit unabhängig von der Netzwerkschicht (Layer 2, 3 und 4) verschlüsseln. Diese Hardware-Encryptors sind laut FIPS 140-2 Level 3, Common Criteria und NATO zertifiziert und stehen auf der DoDIN APL. • Bei der CV-Reihe handelt es sich um gehärtete virtuelle Appliances, die mithilfe von Network Function Virtualisation (NFV) robuste Verschlüsselung für Data-in-Motion über Hochgeschwindigkeits-Carrier-WAN und SD-WAN-Links hinweg anbieten.
RESPOND (RS) Minimierung (RS-MI)	RS.MI-3: Neu identifizierte Sicherheitslücken werden minimiert oder als akzeptable Risiken dokumentiert.	**CipherTrust Intelligent Protection** vereint die risikoorientierte Erkennung sensibler Daten mit richtlinienbasierter transparenter Verschlüsselung, um das Risiko einer Offenlegung von Daten automatisch zu minimieren. Es unterstützt Unternehmen dabei, Geschäftsrisiken zu visualisieren und Abhilfemaßnamen zu automatisieren, um sich so vor Ransomware-Angriffen zu schützen. Mit **SafeNet Trusted Access** können Unternehmen das Risiko von Ransomware minimieren. Sie erhalten einen unmittelbaren, aktuellen Audit Trail aller Zugriffsereignisse in allen Systemen. Umfangreiche automatische Berichte dokumentieren alle Aspekte der Durchsetzung und Authentifizierung von Zugriffen. Darüber hinaus streamt der Dienst automatisch Protokolle an externe SIEM-Systeme.

Eine umfangreiche Auswahl an Lösungen zur Einhaltung des NIST-Leitfadens zur Cybersicherheit.

Die Lösungen von Thales verfügen über einige der wichtigsten Funktionen, die der Leitfaden zur Cybersicherheit von NIST verlangt. Dennoch kann kein einzelnes Unternehmen ein Lösungspaket anbieten, das wirklich alle Anforderungen der NIST erfüllt. Daher arbeitet Thales mit über 400 Partnern zusammen, die zu den führenden Technologieanbietern der Welt gehören, um Kunden eine umfangreiche Auswahl an Lösungen und Integrationen zur Einhaltung des NIST-Leitfadens zur Cybersicherheit anzubieten. Wenden Sie sich an uns, wenn Sie mehr darüber erfahren möchten, wie wir Sie dabei unterstützen können, nicht nur Ransomware-Angriffe, sondern auch schädliche Malware, Insiderbedrohungen und sonstige Advanced Persistent Threats zu verhindern.

Über Thales

Thales ist ein international führender Anbieter im Bereich Datensicherheit, dem Regierungen und die bekanntesten Unternehmen der Welt beim Schutz ihrer sensibelsten Daten ihr Vertrauen schenken. Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, verlassen sich beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

> cpl.thalesgroup.com/de <

Kontakt – Alle Bürostandorte und Kontaktinformationen finden Sie auf cpl.thalesgroup.com/contact-us