Bewertung der Sicherheitsaussagen bezüglich der AWS Nitro System APIs

Amazon Web Services, Inc.
Version 1.0, 11. April 2023

Erstellt von
John Redford
Xiang Wen Kuan

Erstellt für
Amazon Web Services

1 Zusammenfassung

Überblick

Im letzten Kalenderquartal 2022 wurde die NCC Group von Amazon Web Services (AWS) mit der Überprüfung der Architektur des AWS Nitro Systems beauftragt. Diese Überprüfung wurde im ersten Kalenderquartal 2023 unternommen. Hierbei lag der Schwerpunkt auf spezifischen Aussagen von AWS zur Sicherheit der APIs des Nitro –Systems.

Nachfolgend wird das Nitro System beschrieben: (Diese Beschreibung basiert auf Informationen, die in öffentlich verfügbaren Dokumenten enthalten sind)[1]:

> Das AWS Nitro System vereint speziell entwickelte Serverdesigns, Datenprozessoren, Systemverwaltungskomponenten und eine spezielle Firmware. Es liegt als Plattform allenseit Anfang 2018 eingeführten Amazon-EC2-Instanzen zugrunde. Das Nitro System hat drei Hauptkomponenten:

> - Speziell entwickelte Nitro-Karten: von AWS entwickelte Hardwaregeräte, die eine umfassende Systemsteuerung und Virtualisierung der Ein-/Ausgabe (E/A) ermöglichen, unabhängig von der Hauptplatine mit deren CPUs und Speicher.
> - Nitro-Sicherheitschip: unterstützt einen sicheren Startvorgang des Gesamtsystems auf der Grundlage einer Hardware-Vertrauensbasis, der Fähigkeit, Bare-Metal-Instanzen bereitzustellen, sowie einer umfassenden Schutzvorkehrung, die unbefugte Änderungen der Systemfirmware am Server verhindert.
> - Nitro-Hypervisor: ein bewusst minimierter und Firmware-ähnlicher Hypervisor mit einer starken Ressourcenisolierung und einer von einem Bare-Metal-Server kaum zu unterscheidenden Leistung.

AWS trifft mehrere Sicherheitsaussagen, dass das Nitro System einen Zugriff auf Kundendaten durch AWS-Mitarbeiter verhindert. Diese werden im Kapitel Aussagen aufgeführt.

Das Nitro System wurde entwickelt, um die in diesen Aussagen beschriebenen Sicherheitsziele zu erreichen. Das System beinhaltet eine Gesamtinfrastruktur für die Verwaltung und Überwachung des Systems, die sowohl die Hardwareebene, als auch die Bereitstellung und Anwendung von Systemen, bis zum Ende ihrer Lebensdauer, abdeckt. Es gibt keine sekundären oder alternativen Möglichkeiten, für AWS, auf Nitro-EC2-Hostsysteme zuzugreifen. Aufgrund einer sehr gründlichen Vorgehensweise sowie des Einklangs von Sicherheitszielen und -anreizen und nachhaltigen und realistischen Geschäftspraktiken, hat AWS ein System entwickelt, das sehr strengen Sicherheitsansprüchen gerecht werden kann, und das Kundendaten ausreichend schützt.

Hinsichtlich des Designs entdeckte die NCC Group keine Lücken im Nitro System, die diese Ansprüche gefährden würden. Bei allen Designs gibt es Kompromisse. AWS hat sich für ein Design entschieden, bei dem die Auswirkungen einer böswilligen Gefährdung mit denen eines geringen Hardwarefehlers vergleichbar sind.

Projektumfang

Als Teil der Bewertung durch die NCC Group wurden Aussagen zur Sicherheit des Designs der administrativen Nitro-APIs verifiziert, sowie zu den Prozessen, mit denen Nitro-APIs erstellt und verwaltet werden. AWS-Systemadministratoren führen mithilfe der Nitro-APIs verschiedene klar definierte Aufgaben durch. Dazu gehören die Entwicklung und Bereitstellung von Softwareelementen des Nitro Systems, die verwendete Infrastruktur sowie die Verfahren für die Erstellung und Bereitstellung einer NitroSystemumgebung.

1. Sicherheitsdesign des AWS Nitro System https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html.

Die Bewertung durch die NCC Group beinhaltete folgendes:

- Die Nitro –System APIs, deren Anfragen, Funktionalität, Entwicklungs- und Bereitstellungsprozesse sowie die benötigten unterstützenden Infrastrukturelemente.
- Die Funktion und Aufgabe von AWS-Systemadministratoren mit autorisiertem Zugriff auf Nitro System APIs.
- AWS-Mitarbeiter, bei denen es sich nicht um Systemadministratoren handelt, einschließlich Entwicklern des Nitro Systems und Personen, die Mitarbeiter verwalten und ihnen bestimmte Aufgaben und Befugnisse zuweisen.
- Die Überprüfung des Nitro Systems und seiner Umgebung, sodass sichergestellt werden konnte, dass keine alternativen Systeme vorhanden oder designbedingt erforderlich waren.

Die folgenden Elemente waren nicht Bestandteil der Bewertung:

- Bewertung der EC2-Steuerebenen-Services im Allgemeinen.
- Bewertung des Nitro-Hypervisors, der Nitro-Firmware und der Nitro-Software auf Nitro-Karten.
- Bewertung von Nitro-Karten.
- Bewertung der physischen Umgebung und der physischen Sicherheitskontrollen.

Prüfungsmethode

Die Prüfung erfolgte größtenteils anhand von Interviews des AWS-Nitro-Entwicklungsteams und der von AWS bereitgestellten Designdokumentation. Die NCC Group führte Interviews mit mehreren "Distinguished Engineers" im Nitro-Team durch, einschließlich des leitenden Entwicklers. Diese Interviews erfassten den Ursprung und die Designziele des Systems sowie dessen operative Merkmale und Einschränkungen. Zusätzlich wurden Informationen in Form von Dokumenten und Bildschirmteilungen bereitgestellt, damit sich die NCC Group ein umfassendes Bild von der Sicherheit des Nitro Systems machen konnte. Die bereitgestellte Dokumentation enthielt umfangreiche interne Details zum Design des Systems.

Die Bewertung beinhaltet jedoch weder eine detaillierte Überprüfung der Implementierung bestimmter Komponenten noch praktische Tests oder technische Validierungen. Die Bewertung der Sicherheitsaussagen basiert darauf, ob das Design des Nitro Systems (wie beobachtet) ausreichend ist, die Sicherheitsaussagen zu untermauern und aufrechtzuerhalten. Da es sich um eine Prüfung auf Designebene handelt, würde eine Sicherheitsaussage als 'nicht untermauert' bewertet werden, sobald das Design selbst die Erfüllung eines Sicherheitsziels verfehlt.

Projekteinschränkungen

Die Bewertung der Nitro –System –APIs fand zu einem bestimmten Zeitpunkt, und in einem bestimmten Zeitraum statt, Da sich Sicherheitsgefährdungen und Angriffstechniken ständig weiterentwickeln, , sollten die Ergebnisse dieser Bewertung nicht als Bestätigung dienen, dass die aktuellen Sicherheitsmaßnahmen einen angemessenen Schutz vor zukünftigen Bedrohungen bieten. Darüber hinaus beziehen sich die Aussagen der NCC Group auf das System, wie es im Bewertungszeitraum bereitgestellt wurde. Sie sind keine Zusicherungin Bezug auf zukünftige technische Änderungen oder Abweichungen von Richtlinien. Der sichere Startvorgang und die Interaktion von Nitro-Karten waren ein Faktor der Bewertung. Die Bewertung der Sicherheit dieser Systeme im Falles eines physischen Angriffs waren jedoch vom Umfang dieses Projekts ausgeschlossen bzw. Teil anderer Projekte.

Wie dargelegt, beruht die Bewertung der Nitro System APIs auf den Aussagen von AWS-Mitarbeitern sowie der von AWS bereitgestellten Designdokumentation. ADie NCC Group kann jedoch keine Gewähr für die Richtigkeit der Informationen oder der entsprechenden Schlussfolgerungen sowie die Übereinstimmung von Implementierung und Design

übernehmen. Alle Aussagen zur Nitro Systemleistung beziehen sich ausschließlich auf dessen Design.

2 Nitro-System-Design

Einleitung

Die von der NCC Group durchgeführte Projektplanung und Designprüfung der Nitro Systemarchitektur durch Interviews und Dokumentenanalyse dauerte einige Monate. Ziel der Bewertung was es, festzustellen, ob die Nitro Systemarchitektur die Sicherheitsaussagen von AWS ausreichend untermauert. Das Bewertungsteam der NCC Group betrachtete das System aus der Sicht der AWS-Systemadministratoren, d. h. Personen mit nicht öffentlichem Zugriff auf die Umgebung, sowie aus der Sicht von Nitro Systementwicklern und anderen AWS-Mitarbeitern.

Die Prüfung ergab auch:

- Dass AWS-Systemadministratoren allein über Nitro System APIs mit den Instanzen-Hosts interagieren I können, da keine andere Möglichkeit besteht, sich anzumelden, Verbindungen herzustellen, oder anderweitig Zugriffsberechtigungen zu erhalten, und
- Dass außer den AWS-Systemadministratoren keine anderen AWS-Mitarbeiter diese APIs nutzen können.

Ziele des Nitro-System-Designs

Geringste Zugriffsberechtigung

Das Nitro Systemdesign folgt dem Prinzip der geringsten Zugriffsberechtigung. Dadurch soll folgendes verhindert werden:

- Zugriff auf Kundendaten.
- Zugriff zur Ausführung beliebiger Befehle oder Codes.
- Änderung von Instanzens mit besonderen Patches oder Softwareversionen.
- Migration von Daten oder Speichern zu einer anderen Instanz oder Umgebung.
- Fehlende Aufzeichnung von Aktivitäten.
- Notfallverfahren zur Umgehung oder Aufhebung von Sicherheitsvorkehrungen.

Das NitroSystemdesign wurde so an den grundlegenden Anforderungen der Umgebung ausgerichtet, dass es mit geringeren Verfügbarkeitsausfällen, wie z.B. herkömmlichen Hardwareausfällen oder Zwischenfällen, relativ problemlos umgehen kann. Die Auswirkungen eines potenziellen Missbrauchs durch einen böswilligen Benutzer wären mit solchen Ausfällen zu vergleichen.

Redundanz und Zero Trust

Die Nitro -SystemkKomponenten sind daraus aufgelegt, redundante und mehrstufige Sicherheitskontrollen durchzuführen. Das Design stellt sicher, dass Authentifizierung und Autorisierung mehrfach überprüft werden. Für die Entwicklung und Bereitstellung von Softwareänderungen sind mehrere Pfade erforderlich. Die Instanz-Hosts prüfen die Zulässigkeit von Zugriffen, bevor angeforderte Aktionen ausgeführt werden.

Vertraulichkeit und Integrität

Im gesamten Umgebungsdesign werden strenge Verschlüsselungs- und Signaturkontrollen angewendet. Das Nitro Systemdesign stellt insgesamt sicher, dass die gesamte Nitro Systemkommunikation sicher verschlüsselt wird und alle bereitgestellten Nitro Systemkomponenten signiert und validiert werden. Um die Wahrscheinlichkeit einer Kompromittierung der Schlüssel für den Schutz von Kommunikation und Softwareupdates zu verringern, stellt das Design sicher, dass die Vertrauensbasis ('Root of Trust') auf geschützten Systemen liegt, deren Sicherheitsverwaltung nicht für niedrigere Zugriffsebenen verfügbar ist.

Überprüfung und Überwachung

Alle Nitro System API-Anfragen werden in einer sicheren CloudWatch-Umgebung mit mehrstufigen Zugriffskontrollen aufgezeichnet. Die Aufzeichnungen werden kontinuierlich auf

sensible Anfragen oder Aktivitätsmuster überwacht, um das entsprechende Personal auf die betroffenen Systeme aufmerksam zu machen. Diese Überwachung und die Reaktion und Verhalten des Personals werden regelmäßig getestet. Interne Red-Team Tests belegen, dass diese Mechanismen funktionieren und effektiv sind.

Designanreize

Die Designanreize stimmen mit den grundsätzlichen Anreizen, denen AWS und seine Mitarbeiter folgen, überein. In manchen Umgebungen entsteht selbstverständlich eine Zugriffshierarchie. Oft haben in solchen Fällen nur einige wenige Administratoren vollständigen Zugriff auf vielzahlige Unternehmenssysteme, oft auch auf solche Systeme, die wiederum den Zugriff auf andere Systeme kontrollieren. Es gibt jedoch keinen Grund für AWS-Mitarbeiter, einen ähnlichen Zugriff auf Kundendaten zu haben. Vielmehr widerspricht es den Geschäftszielen von AWS, dass Mitarbeiter jemals einen solchen Zugriff erhalten. Das Nitro Systemdesign sowie dessen Entwicklung und Bereitstellung untermauern daher das Unternehmensprinzip, , dass kein AWS-Mitarbeiter jemals Zugriff auf Kundendaten haben sollte. Interne AWS-Prozesse im Bereich der Zugriffs- und Berechtigungsverwaltung, durch die die Befugnisse von Mitarbeiterndefiniert werden, spiegeln dieses Prinzipebenfalls wider.

Öffentliche Nitro-System-Dokumentation

Viele Details des NitroSystemdesigns sind an mehreren Stellen verfügbar.

- Sicherheitsdesign des AWS Nitro Systems.
  https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html
- Modellprüfungs-Startcode in AWS-Rechenzentren.
  https://link.springer.com/chapter/10.1007/978-3-319-96142-2_28
- AWS re:Inforce 2019: Sicherheitsvorteile der Nitro-Architektur (SEP401-R).
  https://www.youtube.com/watch?v=kN9XcFp5vUM

3 Aussagen

Aussagen zum Sicherheitsdesign des Produkts

AWS bestätigt, dass Nitro Systemhosts eine bestimmte Richtlinie zum Schutz von Kundendaten befolgen und macht in dieser Hinsicht folgende Aussagen:

1. Es gibt keinen Mechanismus, über den sich Mitarbeiter von Cloud-Serviceanbietern beim zugrunde liegenden Host anmelden können.
2. Administrative APIs können nicht auf Kundeninhalte auf dem zugrunde liegenden Host zugreifen.
3. Es gibt keinen Mechanismus, über den Mitarbeiter von Cloud-Serviceanbietern auf Kundeninhalte zugreifen können, die in Instanzen-Speichern und verschlüsselten 'EBS-Volumes' gespeichert sind.
4. Es gibt keinen Mechanismus, über den Mitarbeiter von Cloud-Serviceanbietern auf verschlüsselte, über das Netzwerk übermittelte Daten zugreifen können.
5. Zugriffe auf administrative APIs erfordern stets eine Authentifizierung und Autorisierung.
6. Zugriffe auf administrative APIs werden stets erfasst und aufgezeichnet.
7. Hosts können ausschließlich eine getestete und signierte Software ausführen, die über einen authentifizierten und autorisiertenService verteilt wird. Mitarbeiter von Cloud-Serviceanbietern können Code nicht direkt auf den Hosts einsetzen.

Analyse der Aussagen

1. Es gibt keinen Mechanismus, über den sich Mitarbeiter von Cloud-Serviceanbietern beim zugrunde liegenden Host anmelden können.

Systeme stellen designbasiert keinen Mechanismus bereit, der einen Zugriff auf eine 'Shell' oder einen ähnlichen Mechanismus zur Ausführung beliebiger Befehle ermöglichen könnte. Es gibt weder dieMöglichkeit, einen solchen Mechanismus zu aktivieren oder anzuwenden, noch gibt es Ausnahmefälle oder andere externe Mechanismen.

Analyse: Die NCC Group stellt fest, dass die Nitro Systemarchitektur diese Aussage vollständig untermauert. Es gibt keine Anzeichen dafür, dass Mitarbeitern von Cloud-Serviceanbietern solche oder gleichwertige Zugriffe auf Hosts ermöglicht werden können.

2. Administrative APIs können nicht auf Kundeninhalte auf dem zugrunde liegenden Host zugreifen.

Die administrativen APIs führen keine Aktionen aus, um auf Kundeninhalte zuzugreifen oder diese offenzulegen. Es gibt keine APIs, die Inhalte an Orte verschieben könnten, an denen einZugriff auf sie möglich wäre. Es gibt keine APIs, die den Schutz von Kundeninhalten einschränken oder aufheben würden.

Analyse: Die NCC Group stellt fest, dass die Nitro Systemarchitektur diese Aussage vollständig untermauert. Die administrativen APIs können nicht auf Kundeninhalte auf dem zugrunde liegenden Host zugreifen. Diese Funktion ist nicht vorhanden.

3. Es gibt keinen Mechanismus, über den Mitarbeiter von Cloud-Serviceanbietern auf Kundeninhalte zugreifen können, die in Instanzen-Speichern und verschlüsselten 'EBS-Volumes' gespeichert sind.

Die administrativen APIs enthalten keine Funktion, die einen Zugriff auf Kundeninhalte im Instanzen-Speicher ermöglichen könnten, und können auch nicht verwendet werden, um die Bedingungen zu schaffen, unter denen dies möglich wäre. Instanzen-Speicherelemente und 'EBS-Volumes' sind im Ruhezustand ausnahmslos verschlüsselt.

Nicht verschlüsselte EBS-Speichervolumes stehen jedoch als Kundenoption zur Verfügung.

Analyse: Die NCC Group stellt fest, dass die Nitro Systemarchitektur diese Aussage vollständig untermauert. Es gibt keinen Mechanismus, über den Mitarbeiter von Cloud-Serviceanbietern auf Kundeninhalte zugreifen können, die in Host-Instanzen oder verschlüsselten 'EBS-Volumes' gespeichert sind.

4. Es gibt keinen Mechanismus, über den Mitarbeiter von Cloud-Serviceanbietern auf verschlüsselte, über das Netzwerk übermittelte Daten zugreifen können.

Die für den Schutz von Nitrobezogenen Daten verwendete Verschlüsselung und andere von AWS verwaltete Verschlüsselungen basieren auf geeigneten Algorithmen und einer sicheren Schlüsselverwaltung. Für verschlüsselteVerbindungen wird das TLS 1.2-Protokoll verwendet. Die direkt von der Nitro-Hardware verwendeten Schlüssel werden in einem lokal verschlüsselten Speicher gespeichert, der durch einen manipulationssicheren TPM-Chip geschützt wird Die gesamte Kommunikation über administrative APIs und die gesamte von AWS verwaltete Kommunikation sind sicher verschlüsselt. AWS verwendet sichere Protokollversionen und Algorithmusvarianten und kann schnell auf neuere Versionen und Varianten umsteigen, sobald dies nötig ist.

Analyse: Die NCC Group stellt fest, dass die Nitro SystemaArchitektur diese Aussage vollständig untermauert. Es gibt keinen Mechanismus, über den Mitarbeiter von Cloud-Serviceanbietern auf Verschlüsselungsschlüssel zugreifen oder die Kommunikationsverschlüsselung deaktivieren können.

5. Zugriffe auf administrative APIs erfordern stets eine Authentifizierung und Autorisierung.

In Bezug auf Anfragen fordern die administrativen APIs einen Bearer-Token an, der Authentifizierungs- und Autorisierungsdaten bereitstellt. Dieser Token wird gemäß der Identität des entsprechenden Systemadministrators und dessen Zugriffsrechten generiert und einem autorisierten Systemadministrators zur Verfügung gestellt. Der Token gewährt lediglich Zugriff auf die Ressourcen, für die er ausgegeben wurden, und läuft nach kurzer Zeit ab. Zugriffsberechtigungen werden durch die Verknüpfung von Betreibergruppen mit bestimmten APIs und Gruppen verwalteter Ressourcen beschrieben, und auf die in einem bestimmten Zeitraum jeweils betroffenen Ressourcen begrenzt.

Die Daten für die Konfiguration von Berechtigungen können schnell überprüft werden und sind nicht übermäßig komplex, sodass Benutzer keine unangemessenen Berechtigungen besitzen. Die Daten für die Konfiguration von Zugriffsberechtigungen werden uber denToken-Anbieterservice definiert und folgen dem gleichen Peer-Review- und Änderungskontrollverfahren.

Analyse: Die NCC Group stellt fest, dass die Nitro Systemarchitektur diese Aussage vollständig untermauert. Das eingesetzte Bearer-Token-System verhindert, dass böswillige Benutzer einen vergebenen Token erneut, und anders als für den autorisierten Zweck verwenden. Die Ablaufzeiten des Tokens sind ausreichend lang, um Probleme zu vermeiden, falls der ausgebende Service unterbrochen wird, jedoch kurz genug, um einen eventuellenMissbrauch zu begrenzen. Durch die Speicherung der Konfiguration der Zugriffsberechtigungen im Code des Bearer-Token-Systems, wird gewährleistet, dass beide Systeme vor böswilligen Änderungen geschützt werden. Festgesetzte Kontingente verhindern, dass sich die missbräuchliche Verwendung autorisierter Zugriffe auf eine unangemessen hohe Anzahl von Systemen auswirkt.

6. Zugriffe auf administrative APIs werden stets erfasst und aufgezeichnet.

Alle Zugriffsereignisse (einschließlich fehlgeschlagener Authentifizierungen oder Autorisierungen von Anfragen) werden sofort in einem dedizierten CloudWatch-Protokollstream aufgezeichnet, der vom AWS-Nitro-Entwicklungsteam erstellt und verwaltet wird. Diese Ereignisse werden kontinuierlich auf wesentliche ungewöhnliche oder verdächtige Aktivitäten oder Aktivitätsmuster überwacht.

Analyse: Die NCC Group stellt fest, dass die Nitro Systemarchitektur diese Aussage vollständig untermauert. Der Überwachungsprozess ist auf die Identifizierung von Anfragen ausgelegt, die auf eine missbräuchliche Verwendung der administrativen APIs durch böswillige Akteure oder eine anderweitig unangemessene Verwendung hinweisen könnten.

7. Hosts können ausschließlich eine getestete und signierte Software ausführen, die über einen authentifizierten und autorisierten Service verteilt wird. Mitarbeiter von Cloud-Serviceanbieternkönnen Code nicht direkt auf den Hosts einsetzen.

Der Integritätsschutz der Software und die Mechanismen für die Selbstaktualisierung der Nitro-Umgebung sind direkt in das System integriert. Das Verfahren, über das Systeme gestartet, Identitäten erfasst und übergeordnete Funktionen zum Laden und Verwalten der Software ausgeführt werden, ist von Anfang angesichert. Nitro-Komponenten können funktionell in den ursprünglich sicheren Zustand zurückversetzt werden. Dadurch kann eine Identität in Produktions- oder Nicht-Produktionsumgebungen festgesetzt werden. Aufgrund der Steuerelemente innerhalb der Nitro-Komponenten und der Umgebungen können Komponenten nicht in andere Umgebungen verschoben werden.

Analyse: Die NCC Group stellt fest, dass die Nitro Systemarchitektur diese Aussage vollständig untermauert. Die für die Entwicklung und Autorisierung der Software verwendeten Verfahren bieten böswilligen Akteuren keine Möglichkeit, nicht autorisierte Funktionen in das System einzuschleusen, auch nicht in dem sie als AWS-Systemadministrator oder Nitro-Entwickler agieren, und auf das System zugreifen. Die Anreize, die allen autorisierten Personen geboten werden, sind darauf ausgerichtet, genau dies zu verhindern.

4 Überprüfte Dokumente

Die folgenden Dokumente wurden während dieser Bewertung überprüft.

Öffentliche AWS-Dokumentation

Diese Dokumente sind öffentlich verfügbar. Sie sind empfehlenswert für ein umfassenderes Verständnis des Nitro Systems.

- Sicherheitsdesign des AWS Nitro Systems.
  https://docs.aws.amazon.com/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.html
- Modellprüfungs-Startcode in AWS-Rechenzentren.
  https://link.springer.com/chapter/10.1007/978-3-319-96142-2_28
- AWS re:Inforce 2019: Sicherheitsvorteile der Nitro-Architektur (SEP401-R).
  https://www.youtube.com/watch?v=kN9XcFp5vUM

Interne AWS-Dokumentation

Diese internen AWS-Dokumente wurden der NCC Group auf einem AWS-System zur Lektüre bereitgestellt. Es wurden keine Kopien gemacht,

- **Nitro-Kontrollen:** Detaillierte Dokumentation des Nitro Systemdesigns mit einer Beschreibung der Kontrollen, die einen Betreiberzugriff auf Kundeninhalte verhindern. Dieses Dokument enthält eine detaillierte Übersicht über das Nitro System und dessen Komponenten, die Beschreibung der Trusted Computing Base (TCB), die Beschreibung der Funktion der Nitro-APIs, Bedrohungsmodelle und mehr.
- **Nitro-Sicherheitsdesign:** Ein frühes Designdokument, das die Ziele und Einschränkungen des Nitro Systems beschreibt.
- **Infrastruktur für öffentliche EC2-Schlüssel:** Dokumentation der Infrastruktur für öffentliche Schlüssel, die die Vertrauensgrundlage zwischen internen EC2-Komponenten bildet.
- **Inhalt von Bearer-Token:** Spezifische Dokumentation der Struktur des vom Nitro System verwendeten Bearer-Tokens.
- **Nitro Pipeline:** Dokumentation des für Nitro-Softwareverteilung verwendeten Orchestrierungsagenten. Die Nitro Pipeline ist die Brücke zwischen Standard-Tools von Amazon, Testsuite-Services und weiteren EC2-Services und Tools. Teile dieses Dokuments waren geschwärzt.