Toad® von Quest®: Updates als wichtiger Beitrag zur Sicherheit

Ein technischer Überblick über die in Toad for Oracle integrierten Software-Sicherheitsstandards

Von Julie Hyman, Senior Product Manager, und Ryan Crochet, Sr. Product Marketing Manager, Quest Software

Angesichts der zunehmenden Bedrohungen für die Cybersicherheit ist es für IT-Administratoren von entscheidender Bedeutung, bei der Software, die sie auf ihren Computern und in ihrem Netzwerk zulassen, klare Grenzen zu setzen – unabhängig von bestehenden Sicherheitsprotokollen oder der vorhandenen Architektur. Ausgefeilte Ransomware-Angriffe und andere schädliche Aktivitäten treten immer häufiger auf. Allerdings müssen Unternehmen zur Erreichung ihrer geschäftlichen Ziele eine breitere Palette von Software und Anwendungen einsetzen. Deshalb ist proaktives, robustes Engagement bei der Softwareverwaltung unerlässlich. Beim Schutz der digitalen Assets Ihres Unternehmens gelten die folgenden Mindestanforderungen:

1. Es darf nur sichere Software installiert werden
2. Die Software muss stets auf dem neuesten Stand sein, um die Sicherheit der Systeme zu gewährleisten

In diesem technischen Überblick finden Sie Unterstützung für beide Anforderungen, um die Sicherheit Ihrer Software-Lieferkette zu gewährleisten.

Auf den nächsten Seiten erhalten Sie Antworten auf folgende Fragen:

- **Was ist mit „Sicherheit der Software-Lieferkette“ gemeint und warum ist diese so wichtig?**
- **Wie wichtig ist es, Software auf dem neuesten Stand zu halten?**
- **Welche wichtigen Sicherheitskontrollen unterstützen Toad dabei, optimalen Schutz zu bieten?**

SICHERHEIT DER SOFTWARE-LIEFERKETTE

Sicherheit der Software-Lieferkette bezeichnet die Integrität, Vertraulichkeit und Verfügbarkeit von Softwarekomponenten und deren Abhängigkeiten während des gesamten Lebenszyklus der Softwareentwicklung, von der Konzeption bis zur Bereitstellung. Sie ist von hoher Bedeutung, denn kompromittierte Softwarekomponenten können Unternehmen und ihren Kunden schaden. Effektive Sicherheitsmaßnahmen in der Software-Lieferkette tragen dazu bei, diese Risiken zu minimieren, indem sie für Transparenz, Kontrolle und Sicherheit während des gesamten Prozesses sorgen.

DATENSICHERHEIT UND TOAD

Toad von Quest ist eine IDE (Integrated Development Environment; integrierte Entwicklungsumgebung), mit der Entwickler und Datenbankadministratoren Datenbanken, einschließlich Rollen und Benutzern erstellen, verwalten und pflegen können. Wenn ein Angreifer Zugriff auf die Toad-Sitzung eines Benutzers erhält, kann er möglicherweise nicht autorisierte Datenbankbefehle ausführen, sensible Daten stehlen oder sogar die gesamte Datenbank zum Absturz bringen. Daher müssen Sie unbedingt sicherstellen, dass Toad und die zugehörigen Komponenten regelmäßig aktualisiert, ordnungsgemäß konfiguriert und durch geeignete Sicherheitskontrollen geschützt werden, um diese Risiken zu mindern. Hinweis: Unabhängig von der Architektur und den Sicherheitsprotokollen sind Betriebssysteme und die Datenbankplattformen selbst die wichtigsten Komponenten, die auf dem neuesten Stand gehalten werden müssen. Dies gilt auch für Datenbank-IDEs, da jede Sicherheitslücke in einer IDE oder den zugehörigen Komponenten die Sicherheit der gesamten Datenbankumgebung gefährden kann.

ANWENDUNGSSICHERHEIT UND UPDATES VON TOAD

Eine weitere wichtige Aufgabe ist die Gewährleistung der Sicherheit des Netzwerks durch kontinuierliche Softwareupdates. Die Ransomware-Angriffe, die durch die WannaCry/Petya-Schwachstelle ermöglicht wurden, haben gezeigt, dass auf Hunderttausenden von Computern weltweit veraltete Software installiert war. (Auf vielen von ihnen ist das wahrscheinlich immer noch so.) Obwohl die Beseitigung von WannaCry als Teil eines normalen Updates für Windows durchgeführt wurde, haben zu viele Unternehmen dieses Update nicht angewendet. Trotz monatelanger Warnungen handelte es sich bei dem Petya-Angriff um eine zweite Angriffswelle auf dieselbe Sicherheitslücke, die Computer betraf, die noch nicht aktualisiert worden waren.

Manche IT-Teams verzögern absichtlich Updates, die einen Neustart des Systems erfordern und die Produktivität unterbrechen. Einige machen sich Sorgen darüber, wie sich Updates auf Anwendungen auswirken, von denen Tausende von Benutzern abhängig sind. Andere räumen nur notwendigen Aktualisierungen Priorität ein – und legen selbst fest, was „notwendig“ bedeutet. Wieder andere behandeln die Aktualisierung von Toad und anderer Entwicklungssoftware getreu dem Motto „Was nicht kaputt ist, muss auch nicht repariert werden“.

Identifizierte Schwachstellen

Nachfolgend finden Sie ein Beispiel dafür, warum Benutzer darauf achten sollten, die neueste unterstützte Version zu verwenden. Vor einigen Jahren hat Quest im Rahmen regelmäßiger Überprüfungen während des Build-/Release-Prozesses eine Sicherheitslücke in Toad for Oracle v13.1.1 identifiziert und behoben, zusammen mit der folgenden Meldung:

„Quest hat vor kurzem einen Patch für eine dieser [Drittanbieter-]Bibliotheken erstellt, die eine kritische Sicherheitslücke (CVSS 9.3) enthielt. Die Sicherheitslücke betrifft die Microsoft Visual C++-Bibliothek und könnte zu einer Ausweitung der Rechte führen. Diese Sicherheitslücke wurde mit unserer neuesten Version von Toad behoben.“

Wenn Sie das hier lesen und denken: „Es funktioniert doch noch alles mit der Version von Oracle, die ich verwende … wo ist das Problem?“ – dann lesen Sie unbedingt weiter.

„Es funktioniert doch noch alles mit der Version von Oracle, die ich verwende … wo ist das Problem?“

Erstens: Ist es nicht großartig, dass eine Software, die vor zehn Jahren herauskam, mit einer Datenbank kompatibel ist, die neun Jahre später veröffentlicht wurde? Aufwärtskompatibilität ist heute selten.

Zweitens ist dies jedoch aus Sicht der Cybersicherheit keine optimale Vorgehensweise, unabhängig davon, welche Architektur verwendet wird oder welche Sicherheitsprotokolle oder Firewalls vorhanden sind. Die Verwendung von Software, deren Support eingestellt wurde, kann dazu führen, dass die Software ohne Updates oder Patches anfällig für Sicherheitsbedrohungen ist, was die Integrität und Vertraulichkeit der Daten, mit denen sie interagiert, gefährden kann. Mit der zunehmenden Verwendung von Open-Source-Bibliotheken in proprietärer Software gibt es auch immer mehr Quellen für Cyberbedrohungen.

Eine Studie von Fossa aus dem Jahr 2018 ergab, dass 92 % der Softwareprojekte Open-Source-Komponenten verwenden und dass die durchschnittliche Anwendung 57 % Open-Source-Code enthält. In ähnlicher Weise stellte Synopsys 2019 fest, dass Open-Source-Code im Durchschnitt 70 % des Codes in den analysierten proprietären Anwendungen ausmachte.

Hinzu kommt dann noch die Log4j-Krise von 2021. Die Log4j-Bedrohung resultierte aus einer Sicherheitslücke in der Apache Log4j-Bibliothek, einem weit verbreiteten Open-Source-Protokollierungswerkzeug für Java-Anwendungen. Diese Sicherheitslücke ermöglichte es Angreifern, aus der Ferne bösartigen Code auf den betroffenen Systemen auszuführen – was wiederum Datendiebstahl, Ransomware-Angriffe und andere Sicherheitsverletzungen ermöglichen kann.

Die log4j-Schwachstelle betraf eine große Anzahl von Unternehmen weltweit. Die Geschwindigkeit und das Ausmaß der Ausnutzung dieser Schwachstelle

haben Bedenken hinsichtlich der Sicherheit von Open-Source-Software und der Notwendigkeit robusterer Cybersicherheitsmaßnahmen aufkommen lassen.

Kurz gesagt: Ohne Software-Materialliste können Sie nie wirklich wissen, welche Abhängigkeiten die Software hat und woher die nächste Bedrohung kommt. Ihre einzige mögliche Sicherheitsmaßnahme ist die Verwendung unterstützter Software mit Patches, die verfügbar sind, wenn die nächste Bedrohung auftritt.

Um die Frage zu wiederholen: Wissen Sie, welche Version von Toad Sie verwenden und ob sie unterstützt wird? Quest veröffentlicht fortlaufend neuere, sicherere Versionen. Ein Beispiel: In Tabelle 1 ist ein Teil der Versionsgeschichte von Toad for Oracle aufgeführt. Für alle Versionen unterhalb von 15.0 wurde der Support eingestellt.

Neuere Versionen von Toad-Produkten, wie Toad for Oracle, gehen weit über den funktionalen Bereich hinaus und umfassen auch erhebliche Sicherheitsverbesserungen.

Die Entwicklung von Toad im Rahmen unseres Release-Prozesses folgt der sich ständig verändernden Landschaft von Schwachstellen und Bedrohungen in der Datenbankentwicklung. Dies schließt Folgendes ein:

- Unsichere (unverschlüsselte) Verbindungen zu einer Datenbank
- Unbeabsichtigte Rechteausweitung (Beispiel: Benutzer mit geringen Berechtigungen wird zum Superuser)
- Zu niedrige Hürden für den Zugriff auf personenbezogene und sensible Daten, die in der Cloud gespeichert sind
- Personenbezogene Daten, die in Nicht-Produktionskopien von Datenbanken gespeichert (und vergessen) werden

Mindestens zweimal pro Jahr haben die Kunden von Quest die Möglichkeit, Toad auf die aktuelle Version zu aktualisieren und Sicherheitsverbesserungen hinzuzufügen, die derartige Bedrohungen abschwächen.

Toad for Oracle – Versionen und Support

Version	Support	Datum der allgemeinen Verfügbarkeit
16.3	**Umfassender Support**	07. Apr. 2023
16.2	**Umfassender Support**	30. Sep. 2022
16.1	**Eingeschränkter Support**	29. Jun. 2022
16.0	**Eingeschränkter Support**	26. Apr. 2022
15.1	**Eingeschränkter Support**	27. Jan. 2022
15.0	**Eingeschränkter Support**	18. Okt. 2021
14.2	**Support eingestellt**	13. Jul. 2021
14.1	**Support eingestellt**	30. März 2021
14.0	**Support eingestellt**	23. Okt. 2020

Tabelle 1. Frühere nicht aufgeführte Produktversionen wurden eingestellt. Die aktuellsten Informationen finden Sie in der Versionsunterstützungstabelle von Toad for Oracle (HIER).

SICHERHEITSKONTROLLEN ZUR VERHINDERUNG VON ANGRIFFEN AUF DIE LIEFERKETTE

In der komplexen Softwareumgebung von heute müssen IT-Administratoren eine Reihe von Sicherheitsherausforderungen bewältigen, darunter die Notwendigkeit, Schwachstellen in verschiedenen Anwendungen und Plattformen zu beseitigen. Mit der zunehmenden Verbreitung von Open-Source-Bibliotheken in der Softwareentwicklung wird es immer wichtiger, Abhängigkeiten innerhalb der Software-Lieferkette zu identifizieren und zu verwalten.

Die effektive Verwaltung von Softwareabhängigkeiten ist jedoch entscheidend für die Gewährleistung der Systemsicherheit und die Minderung des Risikos von Cyberangriffen oder rechtlichen Komplikationen im Zusammenhang mit Lizenzierungsfragen. Um dies zu erreichen, müssen Unternehmen der Sicherheit in der Lieferkette Priorität einräumen und Strategien zur Verwaltung und Überwachung von Abhängigkeiten während des gesamten Lebenszyklus der Softwareentwicklung implementieren.

Die Entwicklung von Toad folgt der sich ständig verändernden Landschaft von Schwachstellen und Bedrohungen in der Datenbankentwicklung.

Quest erkennt wachsende Besorgnis über Angriffe in der Lieferkette, bei denen Malware eingeschleust wird, bevor die Produkte an Kunden ausgeliefert werden. Es gibt eine Reihe von Scan-Kontrollen, um im Erstellungsprozess der Toad-Produkte von Quest, einschließlich Toad for Oracle, die Einhaltung von Software-Sicherheitsstandards zur Identifizierung und Beseitigung von Malware sicherzustellen. Die Kontrollen stellen sicher, dass die Produkte frei von Schwachstellen und Malware sind, keine versteckten Hintertüren enthalten und von Mitarbeitern und Auftragnehmern entwickelt werden, die sicher handeln. Tabelle 2 zeigt die Sicherheitskontrollen, die jede Version von Toad durchläuft.

Sicherheitskontrolle	Beschreibung
1. Sicherheitsschulung	Entwickler, Manager und Führungskräfte müssen an einer zweieinhalbstündigen Sicherheitsschulung teilnehmen.
2. Sicherer Softwareentwicklungs-Lebenszyklus	Der Entwicklungslebenszyklus basiert auf den Best Practices des Geschäftsbereichs Information and Systems Management (ISM) von Quest.
3. Drittanbieter-Software	Gebündelte Drittanbieter-Software wird mittels eines Standardprozesses vor Anwendungs-Release auf Schwachstellen überprüft.
4. Schwachstellenscans	Die gesamte Software wird mithilfe eines branchentypischen SAST-/DAST-Produkts auf Schwachstellen hin untersucht.
5. Penetrationstests (Drittanbieter)	Produkte werden jährlich einem Penetrationstest durch eine dritte Instanz unterzogen.
6. Malware-Scans	Alle Produkte werden vor dem Release mit zwei unabhängigen branchentypischen Anti-Malware-Scannern auf Malware untersucht.
7. Codesignierung	Die für Kunden bereitgestellte Software wird mithilfe eines offiziellen Signierschlüssels von Quest zur Bestätigung der Authentizität kryptologisch signiert.
8. Softwareintegrität	Für Kunden werden Prüfsummen für Softwareinstallationsprogramme veröffentlicht, um die Integrität der verteilten Software sicherzustellen.
9. FIPS-Compliance	Durch die Anwendung FIPS-geprüfter kryptographischer Algorithmen werden sensible Daten im Ruhezustand und bei der Übertragung geschützt.

Tabelle 2: Toad-Sicherheitskontrollen gegen Angriffe in der Lieferkette

- Software-Sicherheitsbedrohungen
- Sicheres Software-Design
- Sicheres Coding
- Sicherheitstests
- Sicherheits- und Risikoübersicht
- Code-Probleme bei der Webclient-Server-Interaktion
- Probleme bei der Interaktion von Thick App und Client Server
- Probleme durch Missbrauch von Krypto- und Sicherheitsmaßnahmen
- Sicherheit im Softwareentwicklungs-Lebenszyklus

Nachfolgend finden Sie Einzelheiten dazu, wie Quest Software die einzelnen Kontrollen für Toad-Produkte implementiert:

1. SICHERHEITSSCHULUNG

Ziele der Schulung sind die Entwicklung von Grundkenntnissen im Bereich Sicherheit, die Verbesserung sicherer Coding-Praktiken und eine höhere Einhaltung des sicheren Softwareentwicklungs-Lebenszyklus von Quest (siehe unten). Zu den aktuellen Schulungsthemen gehören:

- Allgemeines zur Softwaresicherheit
- Software-Sicherheitsbedrohungen
- Sicheres Software-Design
- Sicheres Coding
- Sicherheitstests
- Sicherheits- und Risikoübersicht
- Code-Probleme bei der Webclient-Server-Interaktion
- Probleme bei der Interaktion von Thick App und Client Server
- Probleme durch Missbrauch von Krypto- und Sicherheitsmaßnahmen
- Sicherheit im Softwareentwicklungs-Lebenszyklus

Quest überprüft den Abschluss jedes Kurses und bewahrt Aufzeichnungen zur Verwendung bei Kundenaudits auf. Die Aufzeichnungen belegen, dass die Quest Engineering-Teams in sicheren Entwicklungspraktiken geschult werden.

2. SICHERER SOFTWAREENTWICKLUNGS-LEBENSZYKLUS (SECURE SOFTWARE DEVELOPMENT LIFECYCLE; SSDLC)

Der SSDLC für Toad-Produkte führt Überlegungen zu Sicherheit und Datenschutz in den eigentlichen Prozess der Produktentwicklung ein. Der SSDLC wurde entwickelt, um Toad-Engineers zu helfen, sichere Software zu schreiben, Software-Sicherheitsstandards einzuhalten und die Entwicklungskosten niedrig zu halten. Zu den Komponenten und Phasen des SSDLC gehören:

- Definition von Sicherheitsanforderungen
- Definition von Metriken und Compliance-Berichterstellung
- Ausführung von Bedrohungsmodellierung
- Definition und Verwendung von Kryptografiestandards
- Kontrollieren des Risikos bei der Verwendung von Drittanbieterkomponenten
- Erstellung eines Standardprozesses für Vorfallsreaktionen

3. PATCHING VON DRITTANBIETER-SOFTWARE UND -KOMPONENTEN

Wie viele Anbieter von Unternehmenssoftware integriert Quest häufig Code, der von anderen Unternehmen („Drittanbietern“) geschrieben wurde, damit Quest diesen nicht von Grund auf neu erstellen muss. Mit der Zeit tauchen jedoch in einigen Komponenten von Drittanbietern Schwachstellen auf, die gepatcht werden müssen. Quest stützt sich nicht nur auf die NIST CVE-Datenbank, um Informationen über aktuelle Schwachstellen zu erhalten, sondern verwendet auch Tools zur Identifizierung von Drittanbieter-DLLs und allen Schwachstellen, die in diesen DLLs identifiziert wurden. Quest hat außerdem ein Verfahren entwickelt, um die Wahrscheinlichkeit zu verringern, dass Software mit anfälligen Drittanbieter-Komponenten veröffentlicht wird. Dieses Verfahren:

- spezifiziert Kriterien für Schwachstellen, die eine Auslieferung verhindern.
- erfordert eine Bestandsaufnahme aller Komponenten, Softwareprogramme und DLLs von Drittanbietern, die in Produkten gebündelt sind.
- schreibt regelmäßige Prüfungen auf Sicherheitslücken in Drittanbieter-Komponenten vor.
- legt Fristen (30/60/180 Tage) für Drittanbieter fest, um anfällige Komponenten zu patchen.
- schreibt eine Benachrichtigung an Kunden vor, wenn Produkte gepatcht werden und eine neue Version herausgegeben wird.

4. SCHWACHSTELLENSCANS (SAST UND DAST)

Quest hat Prozesse für SAST(Static Application Security Testing)- und DAST(Dynamic Application Security Testing)-Scans mithilfe externer Tools definiert.

SAST ist eine Form des White-Box-Tests. Ein Tester, der SAST einsetzt, untersucht die Anwendung von innen heraus, indem er den Quellcode nach Bedingungen durchsucht, die auf potenzielle Sicherheitsschwachstellen hinweisen. DAST ist eine Form von Blackbox-Tests von außen – so wie ein Angreifer die Anwendung sehen würde. Ein Tester, der DAST verwendet, untersucht eine laufende Webanwendung und versucht, sie wie ein Angreifer zu hacken.

SAST-Tools helfen bei der Identifizierung von häufig auftretenden Schwachstellen mithilfe einer Liste, der sogenannten Common Weakness Enumeration (CWE). Die Tools sind in Bezug auf Logikfluss, Authentifizierung und Autorisierung beschränkt. Hierfür eignen sich Penetrationstests (siehe unten) oder manuelle Quellcodeüberprüfungen besser. DAST-Scanner, die mit einer Webanwendung von außen interagieren, basieren auf HTTP und sind technologieunabhängig.

Für Toad-Produkte umfasst das Verfahren Folgendes:

- Vollständige Scans des Produkts/der Webanwendung werden, wenn möglich, mindestens zweimal pro Jahr und vor allen Releases automatisch mit dem aktuell vorgesehenen SAST/DAST-Tool durchgeführt.
- Der gesamte von Quest entwickelte Produktcode wird mit dem SAST/DAST-Tool gescannt.
- Der Toad Security Advocate überprüft die Ergebnisse jedes Scans und arbeitet bei Bedarf mit dem InfoSec Principal Engineer zusammen, um den Schweregrad der gefundenen Probleme zu bestimmen.
- Es werden keine Produkte mit kritischen oder hohen Sicherheitslücken veröffentlicht.
- Bei mittleren und geringen Schwachstellen arbeitet der Security Advocate mit dem Produktarchitekten zusammen.
- Der Security Advocate und der Produktarchitekt bestimmen die beste Lösung für alle durch die Scans aufgedeckten Schwachstellen.

SAST untersucht die Anwendung von innen heraus und durchsucht den Quellcode nach potenziellen Sicherheitsschwachstellen. DAST ist eine Form von Blackbox-Tests von außen, so wie ein Angreifer die Webanwendung sehen würde.

5. PENETRATIONSTESTS (DRITTANBIETER)

Penetrationstests zeigen die realen Auswirkungen, wenn eine Schwachstelle oder eine Prozessschwäche ausgenutzt wird. Sie sind darauf ausgelegt, die Sicherheit zu bewerten, bevor ein Angreifer zuschlägt. Ein Penetrationstest ist kein automatischer Scan einer Anwendung oder ihres Quellcodes, sondern ein nächster Schritt nach einem automatischen Schwachstellen-Scan (siehe oben).

Bei Toad-Produkten werden jährlich Penetrationstests durchgeführt. Die Tests – eine Kombination aus manuellen und automatisierten Tests – sind so konzipiert, dass sie die Software-Sicherheitsstandards in den folgenden Bereichen des Produkts einhalten:

- Anwendungslogik
- Code-Einschleusung
- Lokaler Speicher
- Ausnutzung von Binärdateien und Reverse Engineering
- Überflüssige Berechtigungen
- Unverschlüsselte Speicherung sensibler Informationen
- Unverschlüsselte Übertragung sensibler Informationen
- Schwache Verschlüsselungsimplementierungen
- Schwache Assembly-Kontrollen
- Schwache GUI-Steuerung
- Schwache oder voreingestellte Passwörter

In den meisten Fällen folgt ein Penetrationstest einem bestimmten Rahmen, der von der Zielanwendung oder -infrastruktur abhängt. Dabei variiert die Taktik je nach dem Angreifer, der imitiert werden soll.

Argumente für ein Toad-Update

Als Ergebnis der Penetrationstests hat Quest eine Schwachstelle in Toad for Oracle v13.3 identifiziert und behoben und seine Kunden wie folgt informiert: „Während eines kürzlich durchgeführten Penetrationstests wurde ein Problem entdeckt, bei dem ein Benutzer nicht benachrichtigt wurde, wenn er eine unsichere Verbindung zu einer Datenbank herstellte. Wenn ein Benutzer unwissentlich über einen unverschlüsselten Link eine Verbindung zu einem System herstellt, kann ein Angreifer die Anmeldeinformationen des Benutzers oder alle über die Verbindung übertragenen Daten abfangen. Quest hat diese Schwachstelle behoben."

6. MALWARE-SCANS VON SOFTWARE-BUILDS

Wenn Toad-Produkt-Builds für die Veröffentlichung gepackt werden, werden sie zunächst nach einem konsistenten Prozess auf Malware gescannt, der folgende Schritte umfasst:

- Installationspakete werden vor dem Scannen mit dem SHA-256-Algorithmus gehasht, und der Hash muss mit dem endgültigen, veröffentlichten Hash des Pakets übereinstimmen.

Alle Software-Builds werden auf Malware gescannt, bevor sie zur Installation freigegeben werden.

- Alle Dateien, die in ein Installationsprogramm gepackt werden, werden zunächst auf Malware gescannt.
- Das Scannen von Malware erfolgt automatisch (Befehlszeilenprozess oder Skript).
- Es werden unabhängige Malware-Scanner (zwei für Windows und zwei für Linux) verwendet, die vor dem Scan mit den neuesten Signaturen/Definitionen aktualisiert werden.
- Für jeden Scan wird ein Nachweisprotokoll mit Zeit, Datum und Ergebnissen erstellt und dauerhaft aufbewahrt.
- Verantwortliche für Sicherheit und Engineering müssen Ausnahmen für alle Dateien im Paket genehmigen.

Der Prozess berücksichtigt mehrere Software-Sicherheitsstandards:

Installationspakete werden vor dem Scannen mit dem SHA-256-Algorithmus gehasht, und der Hash muss mit dem endgültigen, veröffentlichten Hash des Pakets übereinstimmen.

- Alle Software-Builds werden auf Malware gescannt, bevor sie zur Installation freigegeben werden.
- Alle Dateien, die in ein Installationsprogramm gepackt werden, werden zunächst auf Malware gescannt.
- Das Scannen von Malware erfolgt automatisch (Befehlszeilenprozess oder Skript).
- Es werden unabhängige Malware-Scanner (zwei für Windows und zwei für Linux) verwendet, die vor dem Scan mit den neuesten Signaturen/Definitionen aktualisiert werden.
- Für jeden Scan wird ein Nachweisprotokoll mit Zeit, Datum und Ergebnissen erstellt und dauerhaft aufbewahrt.
- Verantwortliche für Sicherheit und Engineering müssen Ausnahmen für alle Dateien im Paket genehmigen.

7. und 8. CODESIGNIERUNG UND SOFTWARE-INTEGRITÄT

Eine Anwendung mit dem Codesignierungszertifikat von Quest gibt Kunden die Gewissheit, dass Quest die Anwendung erstellt hat und dass die Software vertrauenswürdig ist. Codesignierung dient dem Ziel, die Authentizität sicherzustellen, indem der Autor der Software verifiziert wird. Außerdem stellt sie die Integrität der Software sicher, indem nachgewiesen wird, dass der Code seit seiner Signierung nicht verändert wurde. Codesignierung spielt auch bei der Veröffentlichung von

Updates und Patches eine Rolle. Wenn Quest ein Update für ein Toad-Produkt mit demselben Schlüssel signiert, der in der ursprünglichen Anwendung verwendet wurde, bedeutet dies, dass das Update vertrauenswürdig ist – es kann von keiner anderen Quelle als Quest stammen. Die bei der Codesignierung erzeugten Prüfsummen geben dem Benutzer die Gewissheit, dass er die richtige Datei erhalten hat und keine, die mit einem gestohlenen Schlüssel signiert wurde. Alle wichtigen Betriebssysteme und Webbrowser unterstützen Codesignierung, um die Verbreitung von Schadcode zu verhindern.

Quest signiert jede im Installationsprogramm enthaltene .exe- und .dll-Datei sowie die mit der Anwendung verpackten Binärdateien und die Installationsdateien selbst.

9. SCHUTZ SENSIBLER DATEN DURCH FIPS-KONFORMITÄT

Wenn Ihre Anwendungen und Datenbanken sensible Daten enthalten, ist ein höherer Schutz erforderlich. Sensible Daten sind fast alle Daten, von denen Sie verhindern möchten, dass sie in die falschen Hände geraten, darunter:

- Netzwerk-Anmeldeinformationen
- Kennwörter
- Sozialversicherungsnummern
- Kreditkarteninformationen
- Personenbezogene Daten wie Namen, Adressen und Telefonnummern
- Personenbezogene Gesundheitsdaten
- Finanzinformationen
- Interne Aufzeichnungen
- Geistiges Eigentum

Die Toad-Produktfamilie schützt sensible Daten durch kryptografische Algorithmen, die die Federal Information Processing Standards (FIPS) der US-Regierung einhalten. Außerdem wird dieser Schutz auf sensible Daten sowohl bei der Übertragung als auch im Ruhezustand angewandt.

Die FIPS-Standards spezifizieren die Best Practices und Anforderungen für kryptografiebasierte Sicherheitssysteme, einschließlich Methoden zur Verschlüsselung und zur Erzeugung von Verschlüsselungscodes. Die FIPS-Konformität ist für alle Computer vorgeschrieben, die für behördliche Arbeit in den USA verwendet werden, und erstreckt sich auch auf das Testen externer Anwendungen (wie Toad), die auf Behördenrechnern ausgeführt werden sollen.

Alle Quest-Produkte entsprechen den FIPS-geprüften Algorithmen für Verschlüsselung und Hashing. Der aktuelle Status der FIPS-Konformität (derzeit FIPS 140-2) wird vor jeder Veröffentlichung validiert.

Toad-Produkte werden mit einem oder mehreren der folgenden Kryptographie-Serviceanbieter und Bibliotheken/Klassen erstellt:

- SHA-256 (.NET)
- DSA (.NET)
- RSA (.NET)
- ECDSA (.NET)
- AES (.NET)
- Java-Kryptographieklasse

Alle Quest-Produkte entsprechen den FIPS-geprüften Algorithmen für Verschlüsselung und Hashing. Der aktuelle Status der FIPS-Konformität (derzeit FIPS 140-2) wird vor jeder Veröffentlichung validiert.

Argumente für ein Toad-Update

Als Ergebnis eines FIPS 140-2-Konformitätstests hat Quest eine Sicherheitslücke in Toad for Oracle v13.2 identifiziert und behoben und seine Kunden wie folgt informiert:

„Quest wurde auf eine aktive Sicherheitslücke aufmerksam gemacht, die es einem Angreifer ermöglicht, im Toad-Produkt gespeicherte Zugangsdaten zu entschlüsseln. Der Exploit, der die Art und Weise ausnutzt, wie Toad Passwörter verschlüsselt, könnte dazu verwendet werden, Zugangsdaten zu entschlüsseln und damit betroffene Datenbanken, FTP-Server oder SSH-Server zu kompromittieren. Quest hat inzwischen eine starke Verschlüsselung implementiert, diese Sicherheitslücke gepatcht und eine nicht angreifbare Version der Software veröffentlicht."

BERÜCKSICHTIGUNG VON SOFTWARE-SICHERHEITSSTANDARDS

	Sicherheits-schulung	Patching von Drittanbieter-Software und -Komponenten	Schwachstellen-scans	Malware-Scans von Software-Builds	Codesignierung und Software-Integrität
NIST SP 800-53 R4	✓	✓	✓	✓	✓
ISO 27001	✓	✓	✓	✓	
PCI DSS v3.0	✓	✓	✓		
PCI 1.4				✓	
AICPA TSC 2014		✓	✓		
AICPA TSC (SOC-2)				✓	
HIPAA 45 C.F.R.		✓	✓	✓	

FAZIT

Die oben beschriebenen Sicherheitskontrollen sind darauf ausgelegt und werden dazu angewandt, Risiken für die Lieferkettensicherheit bei Toad-Produkten zu minimieren. Abbildung 2 veranschaulicht ihren Ablauf.

Die Produkte von Toad sind renommiert und vertrauenswürdig und haben Datenbankexperten bereits Millionen von Stunden an Produktivitätssteigerungen ermöglicht. Indem Sie Updates Ihrer Toad-Produkte anwenden, stellen Sie sicher, dass Sie ständig neue Funktionen erhalten und Software-Sicherheitsstandards einhalten. Außerdem erhalten Sie umfassenden technischen Support und gewährleisten ein robustes Sicherheitsprofil in Ihrem Unternehmen.

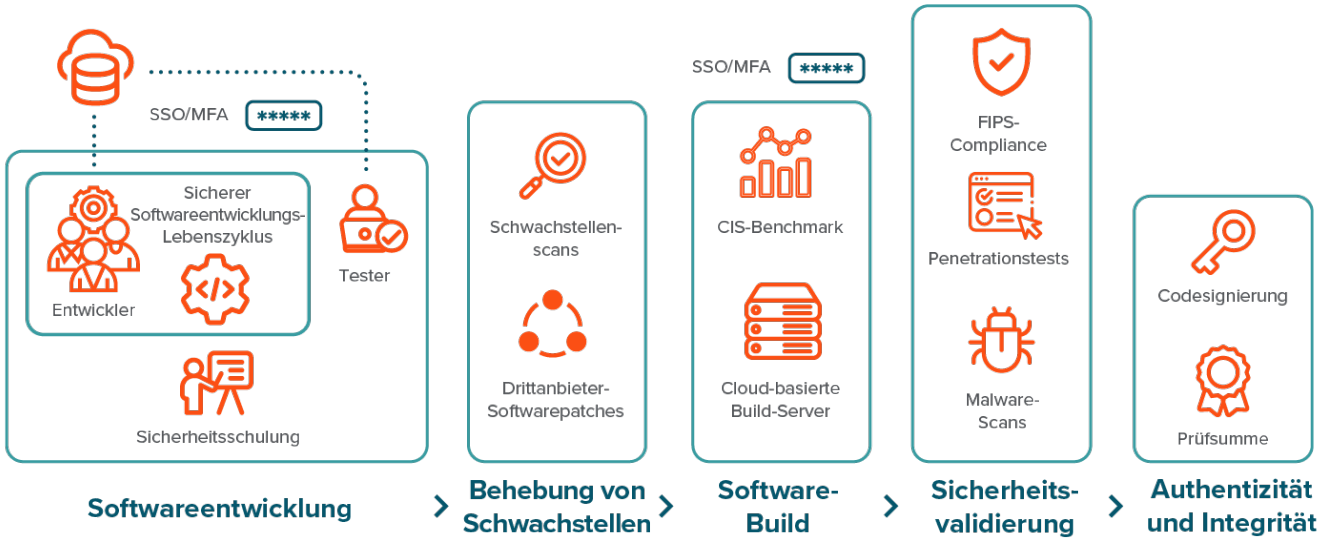

Abbildung 2: Ablauf der Sicherheitskontrollen bei der Entwicklung von Toad-Produkten

INFORMATIONEN ZU DEN AUTOREN

Julie Hyman ist Senior Product Manager für das Datenbanktool-Portfolio bei Quest Software. Sie ist eine erfahrene Softwareproduktmanagerin, die bereits 25 Jahre lang Softwareprodukte in Start-ups und Fortune 500-Unternehmen erstellt und optimiert hat. Julie hat jahrelang eng mit DBAs, Entwicklern und Analysten aus sämtlichen Branchen und vielen führenden Unternehmen zusammengearbeitet, um sicherzustellen, dass Quest nach wie vor erstklassige Lösungen bereitstellt.

Ryan Crochet ist Senior Product Marketing Manager in der Abteilung Information and Systems Management bei Quest Software. Ryan beschäftigt sich leidenschaftlich mit dem Markt, den er bedient, und den Problemen, mit denen dieser regelmäßig konfrontiert ist. Er sucht ständig nach Wegen, diese Probleme zu lösen und gleichzeitig die Macht der datengesteuerten Entscheidungsfindung zu demonstrieren und zu propagieren, um technisches Know-how und Geschäftsergebnisse miteinander in Einklang zu bringen.

Über Quest

Quest stellt Softwarelösungen bereit, mit denen das volle Potenzial neuer Technologien in einer zunehmend komplexen IT-Landschaft ausgeschöpft werden kann. Von der Datenbank- und Systemverwaltung über die Migration zu und Verwaltung von Active Directory und Microsoft 365 bis hin zur Cyber Resilience: Quest hilft Kunden, bereits heute ihre IT-Herausforderungen von morgen zu bewältigen. Weltweit vertrauen mehr als 130.000 Unternehmen und 95 % der Fortune 500 Quest die proaktive Verwaltung und Überwachung der nächsten Unternehmensinitiative an. Quest soll außerdem die nächste Lösung für komplexe Microsoft-Herausforderungen finden, um für die nächste Bedrohung gewappnet zu sein. Quest Software. Where Next Meets Now. Weitere Informationen finden Sie auf www.quest.com.

Sollten Sie Fragen hinsichtlich der potenziellen Nutzung des Materials haben, wenden Sie sich bitte an:

www.quest.com/de-de/company/contact-us.aspx