kaspersky

Sicherheit, Verfügbarkeit, Vertraulichkeit und Datenschutz in der Entwicklung und Verteilung von AV-Basen: **Management Summary zum SOC 2-Audit**

Eine der vier großen globalen Wirtschaftsprüfungsgesellschaften (Big Four) hat 2019 und erneut 2022 mit Stichtag 28. April die Prozesse von Kaspersky in der Entwicklung und Verteilung von AV-Basen gemäß SOC 2-Typ 1 nach den Richtlinien des vom American Institute of Certified Public Accountants (AICPA) entwickelten Standards (AICPA Professional Standard) auditiert.

Das Audit weist nach, dass Kaspersky die Prinzipien und Grundsätze von

(i) ***Sicherheit;***

(ii) ***Verfügbarkeit;***

(iii) ***Vertraulichkeit*** *und*

(iv) ***Datenschutz***

in der Software-Entwicklung und Software-Verteilung uneingeschränkt erfüllt. ***Kaspersky hat in allen 72 Testszenarien die Prüfkriterien ohne Ausnahme erfüllt.***

Der Auditor hat die Beschreibung und Dokumentation durch Kaspersky analysiert und bewertet. Zudem wurden die beschriebenen und umgesetzten Systemkontrollen im Produktivbetrieb überprüft.

Der Service-Auditor hat insgesamt 72 Testszenarien nach Common Criteria für die Bewertung durchgeführt (*C_ELC_01 – C_GCC_61* — siehe die Tabellen auf den Seiten 32-69 im Prüfbericht) und kommt zu dem Ergebnis, dass Kaspersky alle Prüfkriterien ohne Ausnahme erfüllt.

Neben der Prüfung der Dokumentationen und Beschreibungen umfasste das Audit:

- die Befragung der für die genannten Prozesse verantwortlichen Führungskräfte, der Kaspersky-internen Prüfteams sowie der beteiligten Mitarbeiter;
- die Betrachtung und Prüfung der Aktivitäten im laufenden Betrieb sowie
- die Einsichtnahme in alle Unterlagen, Aufzeichnungen und Dokumentationen von Kaspersky *(hierzu zählen u. a. Standardberichte, wie im System konfiguriert; Parametergesteuerte Berichte, die von Kaspersky-Systemen generiert werden; Benutzerdefinierte Berichte, die nicht zum Standard der Anwendung gehören, wie z. B. Skripte, Report Writer und Abfragen; Kalkulationstabellen, die relevante Informationen enthalten, die für die Leistung oder das Testen des Kontrollsystems verwendet werden; von Kaspersky erstellte Analysen, Zeitpläne oder andere Nachweise, die vom Unternehmen manuell erstellt und verwendet werden)*

In den Audits wurden insbesondere folgende Kriterien (CC) betrachtet:

- CC zum Systembetrieb: Kaspersky setzt modernste Erkennungs- und Kontrollverfahren ein, um Änderungen an Konfigurationen zu identifizieren, die zum versehentlichen oder bewussten Einbau von Schwachstellen führen können. Kaspersky überwacht die Systemkomponenten und den Betrieb dieser Komponenten auf Anomalien, die auf böswillige Handlungen, Systemstörungen und Fehler hinweisen, die die Fähigkeit des Unternehmens beeinträchtigen könnten, die Schutzziele zu gewährleisten.

Jede Änderung am Quellcode durchläuft ein dezidiertes Prüfverfahren, um ihre Integrität und Sicherheit zu bestätigen. An den Review-Prozessen zur Erstellung von Updates sind Kaspersky-Experten außerhalb Russlands einbezogen – einschließlich der Kaspersky-Teams in den USA und Kanada (S. 19).

- CC zur Risiko Minimierung: Kaspersky identifiziert, entwickelt und setzt alle erforderlichen Risikominimierungsmaßnahmen ein, die sich aus potenziellen Geschäftsunterbrechungen ergeben können. Das Unternehmen bewertet kontinuierlich alle möglichen Risiken mit Blick auf Zulieferer und die gesamte Supply-Chain. Der Auditor hat zudem das Verfahren zur Aktualisierung der Prozess- und Strukturbeschreibungen überprüft, um sicherzustellen, dass dort die Rollen, ihre Verantwortlichkeiten und die Reihenfolge der Aktionen im Prozess der Indexdateierstellung beschrieben sind.
- CC, die sich auf logische und physische Zugriffskontrollen beziehen: dabei geht es insbesondere um die Art und Weise, wie Kaspersky den Zugriff auf Daten, Software, Funktionen und andere geschützte Informationsbestände auf der Grundlage von Rollen, Zuständigkeiten oder des Systemdesigns autorisiert, ändert oder aufhebt. Kaspersky berücksichtigt dabei umfassend die Konzepte der geringsten Privilegien und der Aufgabentrennung, um höchste Schutzziele zu erreichen.
- CC in Bezug auf das Kontrollumfeld: einschließlich der Verpflichtung zu Integrität und ethischen Werten.
- CC in Bezug auf Kommunikation und Information: Der Auditor hat u. a. überprüft, ob und wie Kaspersky mit externen Parteien über Sachverhalte kommuniziert, die die Funktionsfähigkeit der internen Kontrolle betreffen.
- CC in Bezug auf Kontrolltätigkeiten: Der Auditor hat u. a. den Umfang überprüft, in dem Kaspersky Kontrolltätigkeiten entwickelt und umsetzt, um die Risiken auf ein den Schutzzielen entsprechendes Niveau zu senken.
- CC in Bezug auf Change Management
- CC für die Überwachung der Kontrollen
- CC für die Risikobewertung

Der Bericht enthält zudem ergänzende Informationen über die Maßnahmen von Kaspersky zur Steigerung von Transparenz und Vertrauenswürdigkeit, insbesondere über die konkreten Aktivitäten im Rahmen der **Globalen Transparenzinitiative (GTI)**.

Sie können den 74 Seiten umfassenden Audit-Bericht vom 19. April 2022 bei Ihrem Kaspersky-Ansprechpartner anfordern.

Der Bericht besteht aus folgenden fünf Abschnitten:

Abschnitt I: *Bericht des unabhängigen Service-Auditors (S. 3-6)*

Abschnitt II: *Erklärung des Managements von AO Kaspersky Lab (S. 7-8)*

Abschnitt III: *Systembeschreibung des Managements (S. 9-24)*

Abschnitt IV: *Informationen des unabhängigen Service-Auditors mit Ausnahme von Kontrollzielen und Kontrolltätigkeiten (S. 25-69)*

Abschnitt V: *Zusätzliche Informationen von Kaspersky (S. 70-73)*