KORAMIS

Scannen von mobilen Datenträgern

KORAMIS GmbH
Europaallee 5
66113 Saarbrücken
info@koramis.de

VORWORT

Dieses Dokument befasst sich mit der Arbeitsweise von Virenscannern im Allgemeinen und den Anforderungen an Virenscanner beim Einsatz einer Datenschleuse im Umfeld von Industrieanlagen, der Automatisierungs-, Fertigungs-, Prozess- und Netzwerk-Leittechnik. Es beleuchtet die Aspekte beim Scannen von Wechseldatenträgern und anderen mobilen Medien mit Virenscannern anhand von Beispielen aus der Praxis und zeigt Lösungen auf.

Für weitere Informationen oder eine Beratung wenden Sie sich bitte an info@koramis.de.

Inhaltsverzeichnis

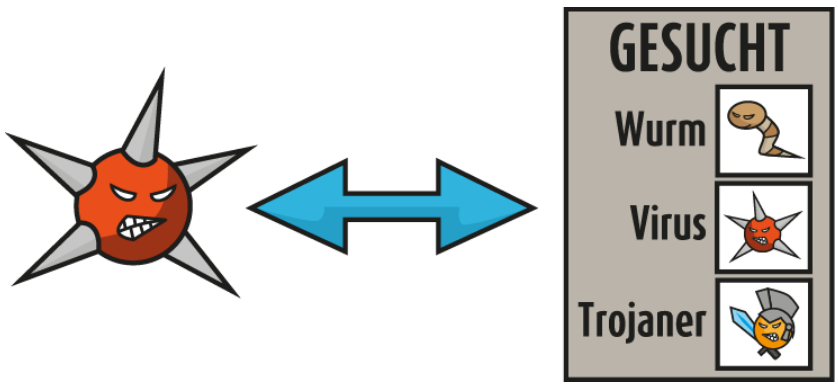
SCANNEN VON DATEN AM BÜROCOMPUTER

Auf nahezu allen Bürocomputern ist heutzutage ein Virenscanner installiert, der den Schutz der Rechner vor Infektionen mit Viren und Schadsoftware gewährleisten soll. Diese Scanner bieten in der Regel drei verschiedenen Arbeitsmodi, die auch parallel genutzt werden können:

- Regelmäßiger Scan ausgewählter oder aller Daten auf der Festplatte des Computers (z. B. täglich oder wöchentlich).
- Ständige Überwachung von Schreibaktionen auf der Festplatte und Scannen der erzeugten, kopierten oder modifizierten Dateien.
- Einmaliger „manueller“ Scan von ausgewählten bzw. allen Dateien auf einem Medium.

Die Arbeitsweise des installieren Virenscanners ist für alle drei Modi gleich:

Die einzelnen Dateien werden Stück für Stück mit den gespeicherten Virensignaturen des Virenscanners verglichen, um Gemeinsamkeiten zu finden. Dabei setzen viele Hersteller zusätzlich heuristische Untersuchungen ein, bei denen anhand von aus Schadsoftware bekannten (Code-) Mustern Rückschlüsse gezogen werden, ob es sich bei der gescannten Datei um einen Schädling handeln könnte.



Die Virenscanner der Bürocomputer haben jedoch alle ein Problem:

Sie sollen - wenn möglich - unauffällig im Hintergrund laufen, den Scanvorgang schnellstmöglich durchführen und gleichzeitig möglichst wenig Systemressourcen in Anspruch nehmen, also das System nicht verlangsamen. Zugleich sollen Sie aber auch alle Daten so gründlich wie möglich nach Schädlingen durchsuchen. Dieser Spagat führt bei nahezu allen Virenscannern dazu, dass bei Standardeinstellungen nur bestimmte Dateitypen aktiv untersucht werden, so etwa ausführbare Dateien wie .exe, .dll, .ocx, MS Office-Dateien wie beispielsweise. doc, .docx, usw. . Inhalte von Containerarchiven wie z. B. .zip oder selbstentpackende .exe Archive werden nicht weiter betrachtet.

Diese Archive werden nicht entpackt, um deren Inhalte zu überprüfen. Diese Vorgehensweise macht durchaus Sinn, kann das Entpacken der Archive viel Zeit in Anspruch nehmen und dabei einen Großteil der vorhandenen Systemressourcen beanspruchen. Sollte im Archiv eine Schadsoftware verborgen sein, kann sie keinen Schaden anrichten, solange sie im Archiv „eingesperrt“ ist. Erst wenn das Archiv entpackt wird, kann der Schädling aktiv werden. Ist dies der Fall, werden durch das Entpacken Schreibaktionen auf der Festplatte des Computers ausgelöst – die enthaltenen Dateien müssen ja auf die Festplatte geschrieben werden. Der Virenscanner bemerkt diese Schreibaktionen und untersucht dann den ausgepackten Inhalt. So ist der umfassende Schutz vor Schädlingen auf dem Computer gegeben.

Manche Virenscanner bieten die Option, das Entpacken und Scannen der Inhalte von Archiven zu aktivieren. Was der Scanner aber in Wirklichkeit tut, bleibt im Dunkeln. Treten beim Entpacken von Archiven Probleme auf (z. B. nicht normgerecht gepackte .zip Dateien, die der Scanner nicht entpacken kann), übergeht er dieses Problem oft und fährt mit der nächsten Datei fort. Es besteht ja kein Grund zur Beunruhigung, denn wenn irgendwann das Archiv vom Benutzer entpackt wird, ist der Scanner sofort da und erkennt den Schädling.

Diese Arbeitsweise hat sich bewährt aber funktioniert nur solange der Virenscanner aktiv ist und die zu „überwachenden“ Daten auf dem Computer bleiben. Eine konkrete Aussage, ob alle Dateien auf einem Medium zu einem bestimmten Zeitpunkt wirklich sauber sind, lässt sich allerdings nicht treffen.

SCANNEN VON DATEN AN EINER DATENSCHLEUSE

Eine Datenschleuse dient zum Untersuchen von Wechseldatenträgern auf Schadsoftware. Der Einsatz einer Datenschleuse ist in Umgebungen empfehlenswert, in denen Daten über portable Speichermedien zu Rechnersystemen transportiert werden, die keinen ausreichenden Virenschutz besitzen.

Im Gegensatz zum Einsatz von Virenscannern im Office-Umfeld ist hier nur ein Betriebsmodus notwendig:

- Einmaliger „manueller" Scan von ausgewählten bzw. allen Dateien auf dem Medium

Eine permanente Überwachung der Daten auf dem Datenträger kann nicht wie beim Office-PC gewährleistet werden, da das Medium nur kurzzeitig verbunden ist. Daher müssen **alle** Dateien des Mediums auf Schadsoftware untersucht werden, bevor es mit dem Netzwerk in Verbindung kommt. Ignoriert der Scanner des Büro-PC ein .zip Archiv und tritt erst beim Auspacken des Archivs durch den Benutzer auf den Plan, so muss der Scanner der Datenschleuse dieses komplett entpacken und seinen Inhalt untersuchen. Treten hier Probleme auf (z. B. nicht normgerecht gepackte .zip Dateien, die der Scanner nicht entpacken kann), darf dieses Vorkommnis nicht wie beim Office-Scanner ignoriert werden, weil meist keine nachfolgende Kontrolle mehr erfolgen kann. Die betroffene Datei muss als „Risiko-Datei" klassifiziert werden.

Der Anspruch bezüglich der Funktionsweise unterscheidet sich in diesem Fall also deutlich vom Einsatzszenario im Office-Umfeld.

Bewertung des Scanergebnisses

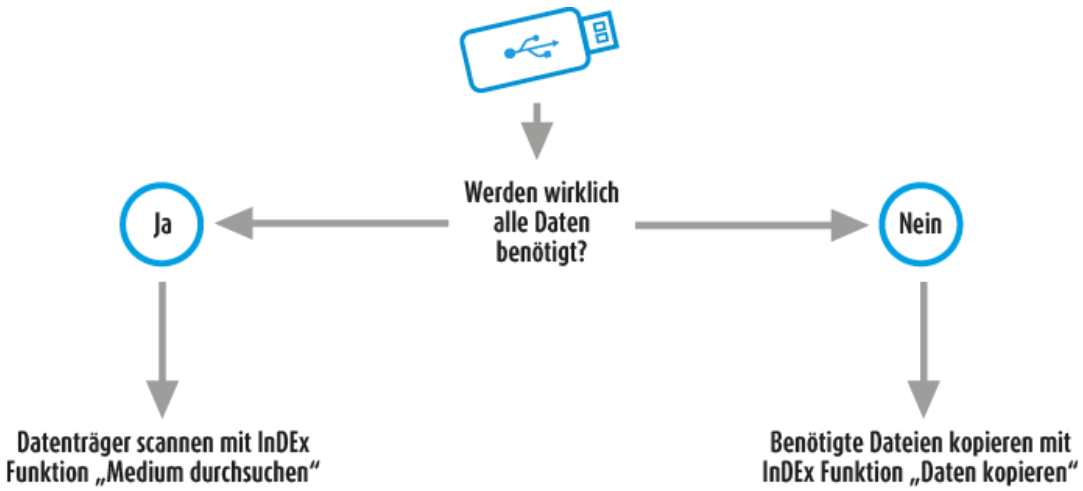
- **Das Medium wird von der Datenschleuse zugelassen:**
  Der Scanner hat alle auf dem Medium vorhandenen Dateien (incl. der in Archiven vorhandenen) auf Schadsoftware untersucht und hat keine Schadsoftware gefunden.
  Man kann davon ausgehen, dass auf dem Medium keine bekannten Schädlinge vorhanden sind.
- **Das Medium wird von der Datenschleuse zurückgewiesen, ein Risiko wird gemeldet:**
  Der Scanner hat alle auf dem Medium vorhandenen Dateien (incl. der in Archiven vorhandenen) auf Schadsoftware untersucht. Schadsoftware wurde zwar nicht gefunden, allerdings konnte mindestens eine Datei nicht oder nicht vollständig gescannt werden (z. B. nicht normgerecht gepackte oder verschlüsselte .zip Dateien, die der Scanner nicht entpacken kann). In diesem Fall muss ein festgelegter Prozess starten, der vorschreibt, was zu tun ist. Dieser Prozess kann nur vom Betreiber der Datenschleuse an Hand seiner Security Policy festgelegt werden. Möglichkeiten sind z. B.:
  - Das Medium darf grundsätzlich nicht verwendet werden.
  - Das Medium darf verwendet werden, wenn ein Entscheidungsträger dies genehmigt. Dieser Genehmigungsprozess sollte dokumentiert werden (z. B. mit unterschriebenem Scan-Protokoll).

- Wurden nicht benötigte Dateien beanstandet, die aktuell benötigten Dateien jedoch als „sauber“ klassifiziert, können die „sauberen“ Dateien mit Hilfe der Datenschleuse auf ein leeres sauberes Medium kopiert werden, das dann zugelassen wird.

- **Das Medium wird von der Datenschleuse zurückgewiesen, ein Virus wird gemeldet:**
  Der Scanner hat alle auf dem Medium vorhandenen Dateien (incl. der in Archiven vorhandenen) auf Schadsoftware untersucht und hat Schadsoftware gefunden. Auch hier muss ein festgelegter Prozess starten, der vorschreibt, was zu tun ist. Dieser Prozess kann nur vom Betreiber der Datenschleuse an Hand seiner Security Policy festgelegt werden. Möglichkeiten sind z. B.:
  - Das Medium darf grundsätzlich nicht verwendet werden.
  - Die infizierten Dateien werden mit Hilfe der Datenschleuse gelöscht, danach muss das Scanergebnis nochmals bewertet werden.
  - Wurden nicht benötigte Dateien als infiziert gemeldet, die aktuell benötigten Dateien jedoch als „sauber“ klassifiziert, können die „sauberen“ Dateien mit Hilfe der Datenschleuse auf ein leeres sauberes Medium kopiert werden, das dann zugelassen wird.

Empfehlungen

- Das Risiko eines Vorfalls sinkt, wenn die Datenmenge auf dem Wechselmedium gering gehalten wird. Im Idealfall befinden sich auf dem Medium nur die aktuell benötigten Daten. Dadurch sinkt auch die Dauer des Scanvorgangs.



- Der Betreiber der Datenschleuse sollte im Vorfeld einen Prozess festlegen, wie mit einem „riskanten“ oder infizierten Medium umgegangen wird.

Version	3.1
Dokumenttitel	DatentraegerScannen
Ersteller	KORAMIS GmbH
Email	info@koramis.de
Erstelldatum	21.09.2017