

White Paper

Das müssen Sie zur TR-Resiscan wissen



Das müssen Sie zur TR-Resiscan wissen



Die TR-Resiscan oder ausgeschrieben „die Technische Richtlinie Ersetzendes Scannen“, ist eine Empfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI). Diese legt fest, unter welchen Bedingungen ein Originaldokument nach dem Scannen vernichtet werden darf.

Einer der Hauptgründe für die Einführung der Richtlinie sind die hohen Kosten, die durch die Aufbewahrung von Originaldokumenten entstehen, da hierfür viel physischer Speicherplatz benötigt wird. Darüber hinaus schreitet die Digitalisierung immer weiter voran, weshalb es nur konsequent ist, auch die Archivierung sensibler Dokumente in elektronischer Form zu forcieren. Hierfür existiert eine Vielzahl an Dokumentenmanagement- und Erfassungslösungen auf dem Markt. Da sich diese nur bedingt vergleichen lassen, wurde die TR-Resiscan als eine Art Leitfaden der zu erfüllenden Kriterien für die Informations- und Rechtssicherheit beim Scanvorgang eingeführt.

In diesem Whitepaper erfahren Sie, was genau die TR-Resiscan alles reguliert und wie Sie diese Vorgaben in Ihrem Erfassungsprozess einhalten.

Was genau ist die TR-Resiscan?

Werfen wir zunächst einen Blick auf die allgemeinen Inhalte der TR-Resiscan. In erster Linie soll damit die Rechtssicherheit bzw. die „Beweiswerterhaltung“ beim ersetzenden Scannen von Papierdokumenten sichergestellt werden. Dafür werden vereinheitlichte Anforderungen und Sicherheitsmaßnahmen in einem praxisorientierten Leitfaden definiert und insgesamt **neun Sicherheitsziele** aufgerufen, die es einzuhalten gilt:

1. Integrität:

Hierbei ist sicherzustellen, dass Dokumente nicht nachträglich verändert werden. Demnach soll der Inhalt in dem Zustand erhalten bleiben, wie er im Scanprozess erzeugt wurde. Vom Schutz der Integrität spricht man, wenn Dokumente nachträglich zwar geändert wurden, diese Veränderungen aber anhand technischer Sicherungsmittel erkennbar sind.

2. Authentizität:

Eindeutige Bestimmbarkeit der Quelle. Hier wird sichergestellt, dass die in der Urkunde angegebene Person mit dem tatsächlichen Aussteller der Urkunde übereinstimmt. Durch die Authentizität von dokumentierten Willens- und Wissenserklärungen können die aus ihnen abzuleitenden

Rechte und Pflichten einer konkreten Person zugeordnet werden. Die Forderung nach Authentizität leitet sich daher aus dem Rechtsstaatsprinzip ab.

3. Vollständigkeit

aller Datenobjekte. Dies bezieht sich sowohl auf die Akte als auch den Inhalt. Eine Akte ist vollständig, wenn der Bezug mehrerer, aufgrund eines inneren Zusammenhangs zu einer Sammlung oder Akte zusammengefasster Einzeldokumente sichergestellt ist. Die Vollständigkeit des Inhalts ist gewährleistet, wenn die Zusammengehörigkeit, Reihenfolge und Vollständigkeit der Einzelseiten des mehrseitigen Dokuments sich im elektronischen Dokument widerspiegeln

4. Nachvollziehbarkeit:

Aufzeichnen der Prozessschritte, sodass der dokumentierte Vorgang durch eine unabhängige Stelle unter alleiniger Zuhilfenahme der Akte rekonstruierbar ist. Der zugrundeliegende Sachverhalt der Akte muss also aus sich heraus verständlich sein, hierzu können auch alle Metadaten der Akte herangezogen werden.

5. Lesbarkeit:

Erkennbarkeit aller Datenobjekte. Erst die Lesbarkeit eines Dokuments macht dessen Informationen verwertbar. Die Lesbarkeit des Scanprodukts setzt daher voraus, dass eine geeignete Hard- und Software vorhanden ist, um die auf dem Datenträger gespeicherten Informationen für den Betrachter sichtbar zu machen.

6. Vertraulichkeit:

Dient dem Schutz vor unbefugter Herausgabe von Informationen. Zum grundrechtlichen Schutz der Persönlichkeit gehört auch der Schutz personenbezogener Daten. Dies gilt vor allem in Anbetracht stetiger Nutzung informationstechnischer Systeme, mit deren Hilfe Daten erhoben und gespeichert werden können, die durch Auswertung weitreichende Rückschlüsse auf die Person ermöglichen. Die Wahrung der Vertraulichkeit setzt in der Regel voraus, dass der Zugang zu Daten nur einem bestimmten Kreis von Berechtigten gewährt wird und die Daten vor unberechtigtem Verbreiten geschützt werden.

7. Verkehrsfähigkeit:

Bezeichnet bei Originaldokumenten die jederzeitige Verfügbarkeit des Inhalts ohne technische Hilfsmittel. Die Verkehrsfähigkeit eines elektronischen Dokuments ist dann erreicht, wenn es in den Rechtsverkehr gebracht, insbesondere einem Gericht als Beweismittel vorgelegt werden kann. Dabei muss sichergestellt sein, dass durch entsprechende Sicherungsmittel kein Qualitätsverlust eintritt.

8. Lösbarkeit:

Wird von Löschpflichten (z. B. Bundesdatenschutzgesetz u. v. m.) gefordert und unterstützt das Erreichen der Grundsätze Datenvermeidung, Datensparsamkeit sowie Datenminimierung. Personenbezogene Daten sind nur für zuvor definierte Zwecke zu erheben und nur in dem Maße, wie diese zur Erfüllung des

Zwecks erforderlich sind. Unter der Löschung versteht man das Unkenntlichmachen gespeicherter personenbezogener Daten. Es soll unabhängig von einem bestimmten Verfahren bewirkt werden, dass aus den gespeicherten Daten keine Informationen und Erkenntnisse mehr gewonnen werden können.

9. Verfügbarkeit

aller IT-Systeme. Diese ist dann gegeben, wenn Anwendungen und Informationen zu jeder Zeit durch den Anwender abgerufen werden können. Sie stellt damit eine Grundanforderung der Dokumentationspflicht dar, denn eine Dokumentation kann ihren Zweck, z. B. als Gedächtnisstütze oder zur Beweiserleichterung, nur erfüllen, wenn auf die Informationen zugegriffen werden kann.

9 Sicherheitsziele von TR-Resiscan:



Um diese Ziele zu erreichen, ist die Richtlinie in zwei große Bereiche aufgeteilt, der administrative und der technische Teil.

Im administrativen Teil wird der generische Scanprozess mit der Dokumentenvorbereitung, dem Scannen, der Nachbereitung und schließlich der Integrationssicherung beschrieben.

Der technische Teil widmet sich der Auswahl, Nutzung und Einrichtung von Hard- und Softwarekomponenten, der korrekten Entwicklung, Installation und regelmäßigen Prüfung des Prozesses bis hin zur Dokumentation des fehlerfreien Ablaufs.

Damit die TR-Resiscan nachvollziehbar und leicht anzuwenden ist, wurde sie in drei Schritte aufgeteilt:

1. Strukturanalyse

Im ersten Schritt müssen Sie als Anwender der TR-Resiscan eine Strukturanalyse für ihr Scansystem durchführen und hierbei die für seinen Scanprozess relevanten IT-Systeme, Netze, Anwendungen und Datenobjekte identifizieren und einen bereinigten Netzplan erstellen. Ein Netzplan ist eine grafische Übersicht über die im betrachteten Bereich der Informations- und Kommunikationstechnik eingesetzten Komponenten und deren Vernetzung.

2. Schutzbedarfsanalyse

Im nächsten Schritt ist für die konkret zu verarbeiteten Dokumente eine fachliche Schutzbedarfsanalyse zu erstellen. Dabei werden Geschäftsprozesse, mitsamt der darin verarbeiteten Informationen, in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ eingestuft. Grundlage für diese Klassifizierung ist der zu erwartende Schaden, der bei einer Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit entstehen könnte. Auch mögliche Folgeschäden sollten dabei realistisch eingeschätzt werden. Grundsätzlich lassen sich folgende Schadensauswirkungen auf die Kategorien wie folgt verteilen:

Schutzbedarf: Normal

Schadensauswirkung: „begrenzt, überschaubar“

Definition: Die Schadensauswirkungen sind in der Regel begrenzt und überschaubar. Ein solcher Schaden induziert im Regelfall keine nennenswerten Konsequenzen für die am Geschäftsvorfall beteiligten Personen und Institutionen.

Schutzbedarf: Hoch

Schadensauswirkung: „beträchtliche Konsequenzen“

Definition: Die Schadensauswirkungen sind in der Regel beträchtlich. Ein solcher Schaden führt im Regelfall zu beträchtlichen Konsequenzen für die am Geschäftsvorfall beteiligten Personen und Institutionen.

Schutzbedarf: Sehr hoch

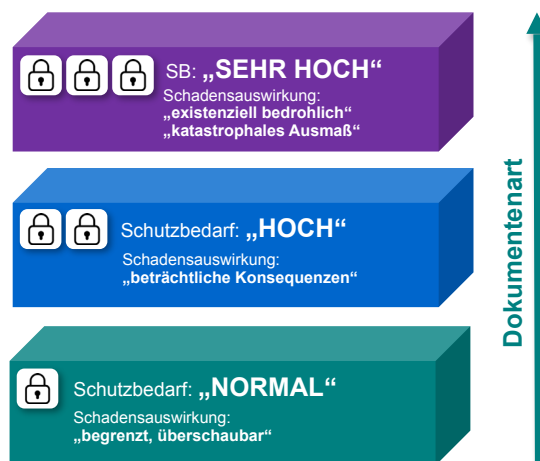
Schadensauswirkung: „existenziell bedrohlich“ oder „katastrophales Ausmaß“

Definition: Die Schadensauswirkungen können ein existenziell bedrohliches oder sogar katastrophales Ausmaß erreichen. Ein solcher Schaden kann zu existenziell bedrohlichen oder sogar katastrophalen Konsequenzen für die am Geschäftsvorfall beteiligten Personen und Institutionen führen.

Die Schutzbedarfsfeststellung ist ein iterativer Prozess. Bereits ganz am Anfang, bei der ersten Diskussion darüber, welche Geschäftsprozesse und Informationen welche Bedeutung für Ihre Institution haben, wird eine erste grobe Schutzbedarfsfeststellung durchgeführt. Auch nach Durchführung von Risikoanalysen sollte die Schutzbedarfsfeststellung erneut dahingehend geprüft werden, ob sie angepasst werden muss, da sich während der Risikoanalyse und der Auswahl von Maßnahmen neue Erkenntnisse für den Schutzbedarf von Assets ergeben können.

Die Schutzbedarfskategorie

... wird pro **Dokumententyp** ermittelt und festgestellt.



Neben der Schutzbedarfsanalyse muss eine Verfahrensdokumentation und -anweisung angefertigt werden, um einen geordneten Ablauf beim ersetzenden Scannen zu ermöglichen. So sind beispielsweise für Originale, die für den automatischen Einzug des Scanners ungeeignet sind (z. B. Reisepass oder geöste Dokumente), passende Prozesse in der Verfahrensdokumentation zu beschreiben.

Die Dokumentation muss grundsätzlich folgende Aspekte umfassen:

- Art der verarbeiteten Dokumente und Festlegung nicht verarbeitbarer Dokumente
- Rollen & Verantwortlichkeiten
- Abläufe, Aufgaben im Scanprozess
- Festlegung von Maßnahmen zur Qualifizierung und Sensibilisierung der Mitarbeiter
- Organisatorische und technische Anforderungen an die relevanten Räume, IT-Systeme, Anwendungen und Sicherungsmittel
- Regelungen für Administration und Wartung der IT-Systeme und Anwendungen
- Festlegung von Sicherheitsanforderungen an IT-Systeme, Netze und Anwendungen

Die Verfahrensdokumentation umfasst insbesondere eine Verfahrensanweisung, die sich an die im Scanprozess eingebundenen Personen richtet. Sie kann auf mitgeltende Unterlagen, wie z. B. Handbücher oder Arbeitsanweisungen verweisen. Eine beispielhafte Verfahrensanweisung findet sich in BSI-TR03138-V (Ersetzendes Scannen -Anwendungshinweis V: Exemplarische Gliederung einer Verfahrensanweisung).

3. Sicherheitsmaßnahmen

Nach der Schutzbedarfsanalyse müssen nun entsprechende Sicherheitsmaßnahmen festgelegt werden, die ein angemessenes Schutzniveau garantieren. Hilfestellung geben hierbei IT-Grundschutzkataloge. Bei der praktischen

Umsetzung empfiehlt es sich, pragmatische Lösungen orientiert am Schutzbedarf der vorab festgelegten Klassifizierung durchzuführen. Würde man jeden Dokumententyp einzeln differenzieren würde der Prozess unnötig komplex und kostspielig werden.

Die gewählten Scanner und Scanlösungen sollten dabei grundsätzlich in der Lage sein, eingescannte Dokumente perfekt lesbar zu digitalisieren. Intelligente Bildtechnologien passen u. a. Helligkeit und Kontrast so an, dass genaueste Ergebnisse erzielt werden. Um den Verlust oder die Beschädigung von Originalen zu verhindern, empfehlen sich Funktionen wie Metallklammererkennung und intelligenter Dokumentenschutz mit Ultraschalltechnologie. Das stellt sicher, dass Doppeleinzüge vermieden bzw. angezeigt werden, um tatsächlich jedes einzelne Dokument zu erfassen. Mikrofone am Einzug des Scanners bemerken verdächtige Knittergeräusche und stoppen den Scanprozess sofort, um das Papieroriginal nicht zu beschädigen. Achten Sie bei der Wahl der Scanlösung zudem auf intelligente Funktionen, um die Richtigkeit der Daten sicherzustellen. So kann die Vollständigkeit der eingescannten Dokumente gewährleistet werden und falls es unvollständig oder nicht lesbar ist, wird automatisch ein manueller Prozess angestoßen. Die Unterstützung von Patch- und Barcodes sorgt für eine zuverlässige Trennung sowie sichere Übergabe von Meta-Informationen im Scanprozess. Für Dokumente, die nicht für den automatischen Einzug geeignet sind, wie ein Reisepass, kann nach Möglichkeit z. B. ein Flachbett benutzt werden, das an den Scanner angedockt wird.

Voraussetzungen an eine TR-Resiscan konforme Belegerfassung mit Kodak Caputre Pro Software:

geeignete Doppeleinzugsmechanismen	geeignete Bildkompressionsverfahren	Sichere Schnittstellen Schutz vor Veränderung und Manipulation	Protokollierungen Erfassung von Metainformation Statistikinformationen Konfigurationsänderungen
Gebundene Belege Überlängen			Integritätsschutz durch geeignete Authentifizierungs- Massnahmen Zugriffs- u. Zutrittschutz Benutzerverwaltung Rollen & Rechte Gesicherter Zugang
Intelligente Dokumenten- und Metallklammererkennung	sicheres Löschen von Zwischenspeichern	Automatisierte Qualitätssicherung PERFECT PAGE	Schulung Wartung sicheres + sinnvolles Konzept
			Profile nicht veränderbare Scanner- und Jobeinstellungen

Eher bezogen auf: **Scanner Hardware** • **Hardware + Software** • **Software**

Kodak alaris

Digitale Signatur und elektronisches Siegel

Des Weiteren sollten Zugriffsberechtigungen erstellt werden, die Daten vor unbefugten Zugriffen und Manipulation schützen. Darüber hinaus müssen Sie die Echtheit, Herkunft, Unversehrtheit sowie Authentizität des Digitalisats sicherstellen. Dies lässt sich mithilfe von digitalen Signaturen für natürliche Personen und elektronischen Siegeln für juristische Personen ideal protokollieren:

Digitale Signatur:

- Ersetzt handschriftliche Unterschrift von natürlichen Personen
- Prüfung von Echtheit, Herkunft, Unversehrtheit
- Rechtsverbindliches Signieren elektronischer Dokumente
- Einfache-, Fortgeschrittene-, Qualifizierte Signaturen
- eIDAS Verordnung („electronic Identification, Authentication and trust Services“)

Elektronische Siegel:

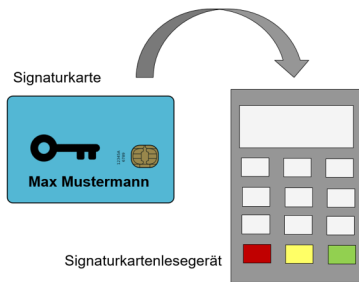
- EU-weite Signatur für juristische Personen
- Herkunftsnachweis, als Absender dauerhaft erkennbar
- Ursprung (Authentizität) und Unversehrtheit (Integrität)
- „elektronischer Unternehmensstempel“
- Fortgeschrittene und qualifizierte Siegel
- Siegelkarte

Fazit

Die TR-Resiscan bietet einen praxisorientierten Handlungsleitfaden zur sicheren Gestaltung der Prozesse für das ersetzende Scannen. Sie definiert die Anforderungen für einen sicheren Scanprozess sowie die notwendigen organisatorischen und technischen Rahmenbedingungen. Um die Digitalisierung der Papierdokumente „nach dem Stand der Technik“ umsetzen zu können, achten Sie bei der Wahl von Hard- und Software auf intelligente Funktionen, die die Einhaltung der Anforderungen an das ersetzende Scannen erleichtern. Bei der Auswahl der Scanlösung sollten Sie außerdem darauf achten, dass viele Erfassungslösungen am Markt nicht weiterentwickelt wurden, weshalb sie mit Scannern der neuesten Generation oft nicht mehr mithalten können.


Digitale Signatur vs. Elektronisches Siegel

Die elektronische Signatur



- Ersetzt handschriftliche Unterschrift von **natürlichen Personen**
- Prüfung von **Echtheit, Herkunft, Unversehrtheit**
- rechtsverbindliches Signieren elektronischer Dokumente
- Einfache-, Fortgeschrittene-, Qualifizierte Signaturen
- eIDAS Verordnung („electronic Identification, Authentication and trust Services“)
- Signaturkarte

Das elektronische Siegel



- EU weite Signatur für **juristische Personen** (Unternehmen)
- **Herkunftsnachweis**, als Absender dauerhaft erkennbar
- **Ursprung** (Authentizität) und **Unversehrtheit** (Integrität)
- „elektronischer Unternehmensstempel“
- fortgeschrittene und qualifizierte Siegel
- **Siegelkarte**

Kodak alaris

Kontaktieren Sie uns:
AlarisWorld.com/go/contactus

Services from
Kodak alaris

**PERFECT
PAGE** 

Alle Marken und Markennamen sind
Eigentum ihrer jeweiligen Inhaber.

Die Marke Kodak und das Logo von
Kodak werden unter Lizenz von der
Eastman Kodak Company verwendet.

© 2021 Kodak Alaris Inc.
TM/MC/MR: Alaris
10/21