Informationssicherheit

ISI kompakt – Update

Erweiterter Funktionsumfang und Umsetzung aufsichtsrechtlicher Anforderungen: Neu ist die Darstellung der Recovery Time Objective, des Schutzniveaus, einer möglichen Unterdeckung und die Wiedervorlage.

Die Corona-Zeit wurde intensiv genutzt, um weitere Funktionen und Ansichten zu ergänzen, aber auch die aufsichtsrechtlichen Anforderungen bestmöglich umzusetzen. So ist ISI kompakt eines der ersten Tools, das auch die seitens der BAIT in den Erläuterungen Tz. 46 geforderte Bewertung des maximal tolerierbaren Datenverlusts (RPO) bietet.

RPO – RTO

Die Recovery Point Objective (RPO) ist Bestandteil der Business-Impact-Analyse (BIA) zur Bewertung der Verfügbarkeit eines Geschäftsprozesses. Die RPO betrachtet für ein IT-System oder eine IT-Infrastruktur den Zeitraum, der maximal zwischen zwei Datensicherungen liegen darf. Im Prinzip geht es hier also um die Frage, wie viele Daten oder Transaktionen zwischen der letzten Sicherung und einem Systemausfall höchstens verloren gehen dürfen.

Andererseits gilt es in der Business-Impact-Analyse, die maximal tolerierbare Ausfallzeit (RTO) zu berücksichtigen.

Die Recovery Time Objective (RTO) beschreibt die benötigte Zeit für den Wiederanlauf eines Geschäftsprozesses im Rahmen eines Notfalls. Also: Wie viel Zeit darf vergehen, bis nach einem Ausfall eines Geschäftsprozesses wieder der Normalbetrieb hergestellt ist und auf die Daten zugegriffen werden kann?

Die Darstellung in ISI kompakt erfolgt über die doppelte Anzeige der Verfügbarkeit („A“ = Availability) bei der Darstellung des Schutzbedarfs sowie des Schutzniveaus. Die übrigen Buchstaben stellen die weiteren Bestandteile der Schutzbedarfseinstufungen dar für die Schutzziele Vertraulichkeit (C = Confidentiality), Integrität (I = Integrity) und Authentizität/Verbindlichkeit (N = Non repudiation).

Im Beispiel (Tabelle 1) wird die Verfügbarkeit mit A1:3 bewertet. Dies ist wie folgt zu interpretieren:

- Der erste Teil vor dem Doppelpunkt stellt – wie bisher in ISI kompakt ausgewiesen – die RTO dar, hier A1 = 1 Woche maximal tolerierbare Ausfallzeit.
- Der zweite Teil nach dem Doppelpunkt stellt – und dies ist neu – die RPO dar, hier 3 = 1-4 Stunden darf der Zugriff auf die Daten maximal ausfallen.

Erreichtes Schutzniveau

Ein weiteres Novum ist die Darstellung des Umsetzungsstands der relevanten Sicherheitsmaßnahmen bei den einzelnen Objekten in ISI kompakt. Aus den zugeordneten Maßnahmen wird unter Berücksichtigung der vollständig umgesetzten Maßnahmen eine entsprechende Umsetzungsquote ermittelt. Aus dieser Quote kann direkt abgelesen werden, bei welchen Objekten noch Bedarf hinsichtlich der Bearbeitung bzw. Umsetzung der relevanten Sicherheitsmaßnahmen besteht.

Im Rahmen des Abgleichs des erforderlichen Schutzniveaus mit dem Schutzbedarf, also den geforderten Sicherheitsmaßnahmen, wurde bislang in einigen Fällen eine Differenz ausgewiesen: Die umgesetzten Maßnahmen reichten nicht aus, um den Bedarf an Sicherheit, den die Bank in dem Schutzniveau darstellt, zu decken.

TABELLE 1

Schutzbedarf	Schutzniveau	Unterdeckung	Schutzniveau (E)	Quote
A1:3 C3 I2 N2	A3:4 C3 I3 N3	–	A3:4 C3 I3 N3	100 % 31/31

TABELLE 2

Schutzbedarf	Schutzniveau	Unterdeckung	Schutzniveau (E)	Quote
A1:3 C3 I2 N2	A3:4 C3 I3 N3	–	A3:4 C3 I3 N3	100 % 31/31
A1:3 C3 I2 N2	A3:4 C2 I2 N2	C3 I3 N3	A3:4 C3 I3 N3	81 % 25/31

Unklar war dabei häufig,

- ob einfach nur offene Maßnahmen nicht in der Bank umgesetzt wurden, oder
- ob die zugeordneten Maßnahmen nicht ausreichen, um das Schutzniveau mit dem Schutzbedarf in Einklang zu bringen.

Mit der Darstellung des erwarteten Schutzniveaus („Schutzniveau (E)“) bietet ISI kompakt nun die Möglichkeit, bereits anhand der noch zu bearbeitenden Maßnahmen zu erkennen,

- ob eine Unterdeckung beseitigt werden kann, oder
- ob noch weitere Maßnahmen getroffen werden müssen.

Das erwartete Schutzniveau ermittelt sich aus den für das jeweilige Objekt relevanten Maßnahmen und zeigt das Schutzniveau an, das erreicht werden kann, wenn sämtliche für das Objekt relevanten Maßnahmen in der Bank umgesetzt werden. Im Beispiel (Tabelle 2) wurden bei einer Erfüllungsquote von 100 % sämtliche 31 von 31 relevanten Maßnahmen in der Bank umgesetzt (Zeile 1).

Im zweiten Fall wurden bisher nur 25 Maßnahmen von 31 Maßnahmen in der Bank umgesetzt. Dies entspricht einer Erfüllungsquote von ca. 81 % (Zeile 2). Es ist aber durch das erwartete Schutzniveau („Schutzniveau (E)“) erkennbar, dass die derzeit ausgewiesene Unterdeckung durch die weitere Umsetzung der noch offenen bzw. nicht vollständig erfüllten Maßnahmen geschlossen werden kann.

Unterdeckung

Nicht immer können sämtliche Maßnahmen in der Bank tatsächlich umgesetzt werden. Auch Kosten-Nutzen-Aspekte spielen häufig eine Rolle.

In einer neu gestalteten Ansicht sehen Sie nun, bei welchen Objekten das aufgrund der Maßnahmenumsetzung im Haus erreichte Schutzniveau nicht für den Schutzbedarf ausreichend ist, also eine Unterdeckung besteht (siehe Tabelle 3, Zeile 2).

Wenn Sicherheitsmaßnahmen eine Unterdeckung nicht abwenden können, ist dies regelmäßig entsprechend zu kommentieren bzw. zu dokumentieren. Das gilt insbesondere dann, wenn die hinterlegten Maßnahmen auch bei einer vollständigen Bearbeitung bzw. Umsetzung nicht ausreichen, um die Unterdeckung zu beheben. Damit wird die Unterdeckung zwar nicht aufgehoben. Aber über eine Begründung kann und muss dokumentiert werden, weshalb trotz der bestehenden (theoretischen) Unterdeckung das Schutzobjekt weiterhin eingesetzt wird. >

TABELLE 3

Schutzbedarf	Schutzniveau	Unterdeckung	Schutzniveau (E)	Quote
A1:3 C3 I2 N2	A3:4 C3 I3 N3	–	A3:4 C3 I3 N3	100 % 31/31
A1:3 C3 I2 N2	A3:4 C2 I2 N2	C3 I3 N3	A3:4 C3 I3 N3	81 % 25/31

Sollte aufgrund neuer Maßnahmenumsetzungen die Unterdeckung entfallen, so wird der Kommentar automatisch archiviert und zukünftig nicht mehr in der Ansicht angezeigt.

Wiedervorlage

Unabhängig von dem in der Bank für das Informationssicherheitsmanagement genutzten Standard ist eine regelmäßige Überprüfung des Informationssicherheitsmanagementsystems erforderlich. Sowohl der SOIT als auch das BSI oder die ISO 27001 fordern einen entsprechenden Regelkreislauf.

Mit ISI kompakt ist die technische Möglichkeit für die Abbildung eines Regelkreislaufs gegeben.

In den Vorgaben kann festgelegt werden, wie die Wiedervorlage mandantenindividuell ausgestaltet wird. Sowohl der Wiedervorlageturnus für Prozesse, Objekte und Objektmaßnahmen als auch die Frequenz der Erinnerungen an den Prozesseigentümer bzw. Verantwortlichen kann individuell eingestellt werden.

Damit sich der Aufwand zur Bearbeitung der Wiedervorlagen im Rahmen hält, gibt es in ISI kompakt jetzt auch die Möglichkeit, mit Hilfe des Buttons „Bestätigen“ die Richtigkeit eines Prozesses, eines Objektes bzw. einer Maßnahmen zu bestätigen. Dies kann im Rahmen der Wiedervorlagen auch über mehrere Objekte, Maßnahmen und Prozesse hinweg erfolgen: schnell und unkompliziert mit einem Klick.

AUTOREN UND ANSPRECHPARTNER

Michael Switalla
Leiter Informationssicherheit & Datenschutz,
E-Mail: michael.switalla@dz-cp.de

Marc Hübner
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: marc.huebner@dz-cp.de

Ausblick

Die Arbeiten an ISI kompakt sind bei weitem noch nicht abgeschlossen. Informationssicherheit lebt und erfährt stetig Änderungen. Entsprechend wird ISI kompakt weiterentwickelt: Einerseits bedingt durch die regelmäßige Aktualisierung des Standards für Ordnungsmäßigkeit der IT-Verfahren der Fiducia & GAD (SOIT) oder der Einführung des Sicherheitsmaßnahmenkatalogs der Fiducia & GAD (SiMaKat). Andererseits veranlasst durch Anregungen, die uns von Anwendern oder Prüfern erreichen. ▬