Ein Leitfaden für den Schutz kritischer Infrastrukturen

Die Digitalisierung bringt nicht nur Vorteile mit sich, sondern auch neue Gefahren. Der Sicherheitsbedarf in der Informations- und Kommunikationstechnologie (IKT) nimmt zu. Unternehmen und Organisationen müssen sich vor den zunehmenden Gefahren durch Cyberangriffe schützen.

Aus diesem Grund haben die Schweizer Bundesbehörden IKT-Minimalstandards festgelegt, die den Betreibern kritischer Infrastrukturen als zentrale Orientierungshilfe dienen. Diese Anforderungen dienen der systematischen Minimierung von Cyberrisiken und zur Stärkung der Widerstandsfähigkeit der betroffenen Unternehmen. Diese Standards sollten aber nicht nur durch KRITIS-Unternehmen beachtet werden. Sie helfen unabhängig davon den Unternehmen, Schwächen zu erkennen.

Die Relevanz von kritischer Infrastruktur

Kritische Infrastrukturen beziehen sich auf die elementaren Systeme, Anlagen und Dienste, die für die Funktionsweise einer Gesellschaft unverzichtbar sind. Zu diesen gehören unter anderem Kommunikationssysteme, Gesundheitswesen, Finanzwesen, öffentliche Sicherheit und Energieversorgung. Wenn diese Infrastrukturen ausfallen oder beeinträchtigt werden, würde dies bedeutende Folgen für die Bevölkerung und die Wirtschaft haben. Daher wurde der IKT-Minimalstandard an verschiedene Bereiche angepasst. Die IKT-Minimalstandards dienen dabei als Leitfaden, um die Sicherheit digitaler Systeme zu sichern und potenzielle Angriffspunkte zu reduzieren.

Ziele der IKT-Minimalstandards

Die IKT-Minimalstandards haben verschiedene Zielsetzungen, die den Schutz und die Sicherheit gewährleisten sollen. Die Hauptziele sind:

Schutz vor Cyberangriffen

Organisationen sollen durch die Einführung der IKT-Minimalstandards ihre Fähigkeit zur Abwehr von Cyberraumbedrohungen stärken. Dies beinhaltet Schritte zur Prävention, Identifizierung und Reaktion auf Cyberangriffe.

Stärkung der Widerstandsfähigkeit (Resilienz)

Ziel ist es, dass Unternehmen auch im Falle von Störungen durch Angriffe oder technischen Ausfällen weiterhin handlungsfähig sind. Dazu gehören technische Massnahmen und organisatorische Abläufe, die es ermöglichen, die Dienste schnell wiederherzustellen.

Reduzierung von Schwachstellen

Die Standards helfen dabei, bestehende Schwachstellen in IKT-Systemen zu identifizieren und zu beheben. Dies betrifft nicht nur technologische Aspekte, sondern auch menschliche und prozessuale Faktoren.

Einhaltung rechtlicher Anforderungen

Die IKT-Minimalstandards unterstützen Organisationen dabei, gesetzliche und regulatorische Vorgaben im Bereich der Cybersicherheit einzuhalten. Dies ist besonders wichtig, um Haftungsrisiken zu vermeiden und den Schutz sensibler Daten zu gewährleisten.

Aufbau und Struktur des IKT-Minimalstandards

Der ISO/IEC 27001-Standard für Informationssicherheitsmanagementsysteme sowie das NIST (National Institute of Standards and Technology)-Rahmenwerk bilden die Grundlage des IKT-Minimalstandards. Mit diesen internationalen Standards können Organisationen bewährte Methoden anwenden und diese in ihre Cybersicherheitsstrategie einbinden.

Der Minimalstandard wurde in mehrere Hauptbereiche unterteilt, in denen konkrete Massnahmen für verschiedene Aspekte der Cybersicherheit enthalten sind. Dazu zählen:

Governance und Risikomanagement

Hierbei handelt es sich um die Ausarbeitung einer ganzheitlichen Sicherheitsstrategie, die auf den spezifischen Gefahren und Erfordernissen des Unternehmens beruht. Ein zentrales Element ist die regelmässige Risikoanalyse, die potenzielle Bedrohungen identifiziert und Massnahmen zur Risikominderung definiert.

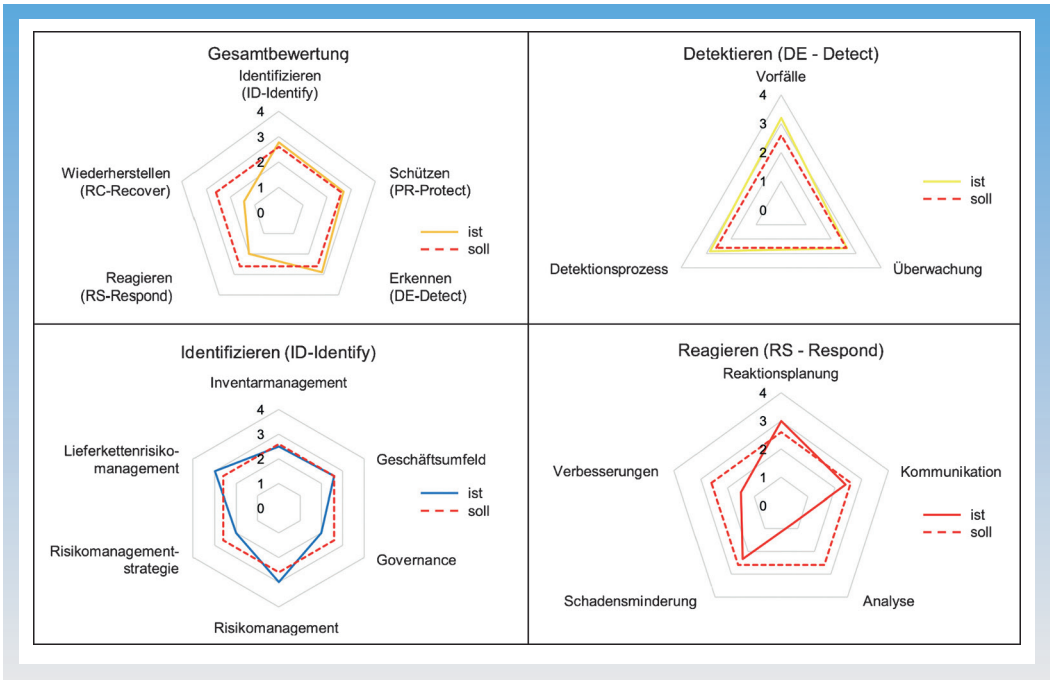

Bild: Minimalstandard zur Verbesserung der IKT-Resilienz 2018, Seite 39

Beispieldarstellung einer Assessment-Auswertung.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Technische Schutzmassnahmen
Hierunter fallen technische Sicherheitsvorkehrungen wie Firewalls, Intrusion-Detection-Systeme, Verschlüsselung und Netzwerksicherheitsprotokolle. Diese Massnahmen sollen unerlaubten Zugriff auf sensible Daten verhindern und die Systemsicherheit gewährleisten.

Sicherheitsbewusstsein und Schulung
Ein weiteres wichtiges Element des IKT-Minimalstandards ist die Schulung und Sensibilisierung der Mitarbeitenden. Cybersicherheit stellt eine menschliche und technische Herausforderung dar. Es ist das Ziel von regelmässigen Schulungen, sicherzustellen, dass Angestellte sicherheitsbewusst handeln und potenzielle Gefahren frühzeitig identifizieren.

Incident Management und Business Continuity
Ein wesentlicher Bestandteil des IKT-Minimalstandards ist die Fähigkeit, auf Sicherheitsvorfälle rasch und wirksam zu antworten. Dies beinhaltet Massnahmen, die darauf abzielen, Sicherheitsvorfälle zu identifizieren und zu analysieren sowie die Ausarbeitung von Notfallplänen, um den Betrieb auch in Notfällen zu erhalten.

(Externe) Kommunikation und Zusammenarbeit
Organisationen sollten nicht isoliert agieren, sondern mit anderen Beteiligten in Kontakt treten. Dazu gehören sowohl die Zusammenarbeit mit Behörden als auch der Austausch von Informationen über Bedrohungen und Sicherheitsvorfälle. Dies ist besonders wichtig, um frühzeitig auf neue Angriffsszenarien reagieren zu können.

Das zur Verfügung gestellte Excel-Dokument unterstützt bei der Selbstbewertung. Zu jedem Themengebiet gibt es mehrere Fragen. Als Umsetzungsstand (Reifegrad) kann ein Wert von 0 bis 4 eingegeben werden. Dabei stehen die Werte für:
- 0 = nicht umgesetzt
- 1 = partiell umgesetzt, nicht vollständig definiert und abgenommen
- 2 = partiell umgesetzt, vollständig definiert und abgenommen
- 3 = umgesetzt, vollständig oder grösstenteils umgesetzt, statisch
- 4 = dynamisch, umgesetzt, kontinuierlich überprüft, verbessert

Vordefiniert ist ein Mittelwert von 2,6 pro Themengebiet. Dieser kann, und sollte auch, an das eigene Unternehmen und die Anforderungen angepasst werden. Am Ende kann dies beispielsweise wie in der Grafik aussehen.

Umsetzung der IKT-Minimalstandards

Um die IKT-Minimalstandards einzuführen, müssen Unternehmen und Organisationen eine gründliche Planung und Ressourcenverteilung durchführen. Es genügt nicht, bloss technische Massnahmen umzusetzen. Es ist wichtig, dass auch die Organisationsstrukturen angepasst und fortlaufende Überprüfungen und Verbesserungen durchgeführt werden. Die Durchführung kann durch verschiedene Schritte erfolgen:

Bestandsaufnahme
Unternehmen sollten zunächst ihre vorhandenen IKT-Systeme und Sicherheitsvorkehrungen untersuchen. Dabei werden Schwachstellen identifiziert und die aktuelle Risikolage bewertet.

Risikobewertung
Die Bestandsaufnahme dient als Grundlage für eine ausführliche Risikobewertung. Welche Risiken stellen für das Unternehmen eine besondere Bedeutung dar? Welche Mängel stellen ein hohes Risiko für Angriffe dar? Die Prioritäten für die Umsetzung der Minimalstandards lassen sich anhand dieser Analyse festlegen.

Massnahmenplanung und Durchführung
Dieser Schritt beinhaltet die Festlegung und Durchführung konkreter Massnahmen zur Steigerung der Sicherheit. Dazu gehören möglicherweise die Anschaffung neuer Technologien, die Anpassung von Abläufen oder die Schulung von Angestellten.

Überwachung und kontinuierliche Verbesserung
Die Cybersicherheit ist ein fortlaufender Prozess. Es ist von Bedeutung, die Massnahmen nach der Umsetzung ständig zu überwachen und gegebenenfalls anzupassen. In die Sicherheitsstrategie sollten auch regelmässige Schulungen und Sensibilisierungskampagnen für Mitarbeiter integriert sein.

Herausforderungen in der Umsetzung

Trotz der klaren Vorteile gibt es auch Herausforderungen bei der Implementierung der IKT-Minimalstandards. Der Aufwand an Ressourcen, der vor allem für kleine Unternehmen eine Belastung darstellen kann, stellt eine der grössten Herausforderungen dar. Für die Realisierung der Massnahmen sind finanzielle Mittel, technisches Fachwissen und Personalressourcen erforderlich. Ein zusätzliches Problem stellt die Dynamik der Gefährdungslage dar. Aufgrund der fortwährenden Weiterentwicklung von Cyberangriffen müssen Unternehmen ihre Sicherheitsstrategien ständig anpassen. Es ist hier von Bedeutung, eine Sicherheitsstrategie zu konzipieren, die flexibel und anpassungsfähig ist und in der Lage ist, den sich wandelnden Bedrohungen standzuhalten.

Fazit

Der IKT-Minimalstandard bietet eine solide Grundlage für den Schutz kritischer Infrastrukturen in der Schweiz. Er unterstützt Firmen bei der Stärkung ihrer Cybersicherheit und der Abwehr zunehmender Bedrohungen aus dem digitalen Raum. Für eine gelungene Realisierung sind allerdings nicht nur technologische Massnahmen erforderlich, sondern auch eine Anpassung der Organisation beziehungsweise der Prozesse und fortlaufende Überwachung. Der IKT-Minimalstandard ist ein unverzichtbares Werkzeug, um die Sicherheit und Stabilität der digitalen Infrastruktur auf lange Sicht sicherzustellen, besonders (aber nicht nur) für Unternehmen, die eine Schlüsselrolle in der Gesellschaft spielen.

Der IKT-Minimalstandard kann mittels untenstehendem QR-Code kostenlos bezogen werden. Dazu gehört auch ein Self Assessment Tool im Excel-Format.

Download