Risiken in der Informationssicherheit erfassen und verwalten

Kostenloser Download NIST Cybersecurity Framework unter www.nist.gov/ cyberframework

IKT-Minimalstandard unter www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Das Cybersecurity Framework (CSF) des NIST (National Institute of Standards and Technology) ist ein Leitfaden, der Unternehmen hilft, die Risiken in der Informationssicherheit zu erfassen und zu verwalten. Bestehende Standards, Richtlinien und Praktiken werden darin referenziert.

Die Schweiz hat das Framework übernommen und als IKT-Minimalstandard veröffentlicht. Es richtet sich vor allem an kritische Infrastrukturen, ist aber auch für Unternehmen ein sinnvoller Leitfaden.

Auch die eidgenössischen Finanzmarktaufsicht FINMA hat im Rundschreiben 2008/21 explizite Anforderung an ein Risikomanagement-Konzept für den Umgang mit Cyberrisiken definiert, welches sich ebenfalls am CSF orientiert.

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

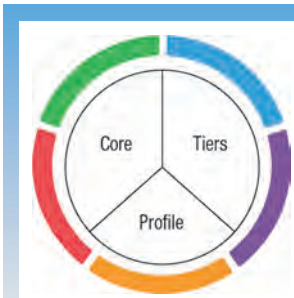

Bild 1: Das NIST Cybersecurity Framework.

Auf weitere Normen referenziert

Das Framework selbst ist in drei Teile unterteilt: Core, Profile und Tiers (Bild 1). Der Hauptteil (Core) definiert eine Reihe von Cybersicherheitsaktivitäten und -ergebnissen. Diese sind in Kategorien unterteilt und auf weitere Normen referenziert. Es soll ebenfalls die Kommunikation zwischen verschiedenen Teams sicherstellen. Dazu besteht der Hauptteil aus drei Teilen: Funktionen, Kategorien und Unterkategorien. Die Funktionen sind in die fünf Teile Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen unterteilt. In diesen Funktionen sind 23 Kategorien enthalten. Diese teilen sich wie in Bild 2 folgt.

Mit den 23 Kategorien decken alle Cybersicherheitsziele eines Unternehmens ab, ohne sich dabei zu tief in die Details zu verlieren. Der Schwerpunkt liegt immer auf den Geschäftsergebnissen.

Eine Ebene tiefer sind 108 Unterkategorien, welche eine ergebnisorientierte Aussage zur Erstellung und Verbesserung der Cybersicherheit enthalten. Da das Framework ergebnisorientiert ist, schreibt es nicht vor, wie ein Unternehmen seine Ergebnisse erreichen muss, sondern ermöglicht damit eine risikobasierte Umsetzung. Ist unklar, wie eine Um-

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes and Procedures	PR.IP
	Maintenence	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Bild 2: Die 23 Kategorien.

Function	Category	Subcategory	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5

Bild 3: ID.AM-1.

setzung aussehen könnte, kann auf andere Richtlinien wie das Grundschutz-Kompendium des BSI (Deutsches Bundesamt für Sicherheit in der Informationstechnik) zurückgegriffen werden.

Als Beispiel an dieser Stelle das ID.AM-1 (Bild 3).

- Die Kategorie fordert, dass die Daten, Mitarbeiter, Geräte, Systeme und Einrichtungen, die es der Organisation ermöglichen, ihre Geschäftsziele zu erreichen, entsprechend ihrer relativen Bedeutung für die Unternehmensziele und die Risikostrategie der Organisation identifiziert und verwaltet werden.
- Die Unterkategorie verlangt, dass physische Geräte und Systeme innerhalb der Organisation inventarisiert sind.
- Die letzte Spalte referenziert auf weitere Normen, wie CIS, COBIT, ISA, ISO oder NIST.

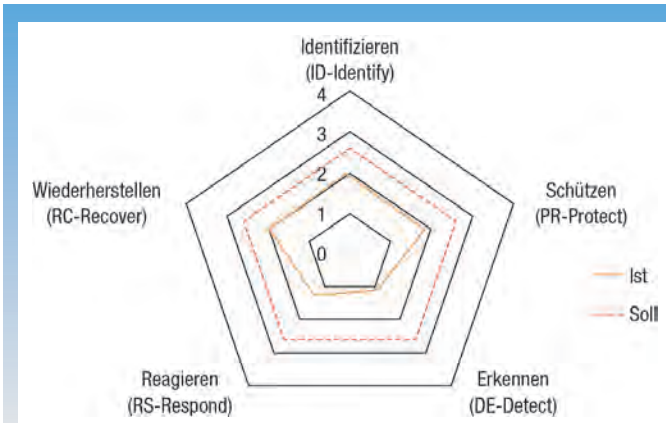

Bild 4: Overall Cyber Security Maturity Bewertung.

Die Stufen (Tiers) zeigen den Stand der Umsetzung an. Sie reichen von «Teilweise» (Stufe 1) bis «Angepasst» (Stufe 4) und zeigen damit wie gut die Cyberrisiken im Unternehmen integriert sind. Entgegen anderen Bewertungen wie dem CMMI (Capability Maturity Model Integration) stellen diese Stufen nicht unbedingt Reifegrade dar.

Das Unternehmen definiert selber, welche Stufe es erreichen möchte und legt damit das akzeptierte Risiko-Niveau fest, in Anbetracht der technischen und finanziellen Möglichkeiten.

Lücken erkennen und schliessen

Dieser Umstand wird auch in den Profilen (Profile) wiedergegeben. Die Anforderungen und Ziele, die Risikobereitschaft und die Ressourcen des Unternehmens werden mit den gewünschten Ergebnissen verglichen und abgestimmt. Profile ermöglichen einen Vergleich zwischen Ist und Soll und damit eine Möglichkeit zur Verbesserung. Da das Framework freiwillig ist, gibt es auch keinen richtigen oder falschen Weg. Jedes Unternehmen definiert sein Soll selber, arbeitet die 108 Unterkategorien durch und ermittelt damit sein Ist. Punkte, die noch nicht erreicht wurden, können erfasst und priorisiert werden. Damit können Lücken erkannt und geschlossen werden.

Wie in der Einleitung erwähnt, hat die Schweiz das NIST CSF übernommen und in den IKT-Minimalstandard überführt. Anhand der Empfehlungen kann die ICT-Resilienz verbessert werden. Es richtet sich zwar an kritische Infrastrukturen, kann aber in jedem Unternehmen genutzt werden. Bei der in Deutsch übersetzten Excel-Tabelle wurden weitere Normen, wie der BSI-Standard verlinkt. Das Self Assessment zeigt am Ende grafisch, wo noch Handlungsbedarf vorhanden ist (Bild 4).

Das NIST Cybersecurity Framework richtet sich an alle Firmen, die einen umfassenden Überblick über ihre Informationssicherheit haben möchten. 108 Massnahmen in die 5 Kapitel Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen unterteilt, zeigen den aktuellen Stand des Unternehmens und ermöglichen damit eine stetige Verbesserung.