



#soreisenFabriken



## MB-SPECIAL: INDUSTRIE 4.0

Mensch und Maschine:  
Technologie unterstützt  
industrielle Arbeit

16

## INDUSTRIEMAGAZIN: ZUM THEMA

Ein gutes Produktdaten-  
management ist  
entscheidend

24

## DOSSIER: MESS-, STEUER- UND REGELTECHNIK

Die Grenzen konventioneller  
Messverfahren überwinden

46

# Risiken in der Informationssicherheit erfassen und verwalten

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-Mi-

## 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

nimalstandard 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,

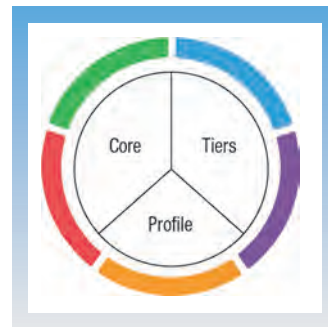


Bild 1: Das NIST Cybersecurity Framework.

welches sich ebenfalls am CSF orientiert.

## 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 si-

cherstellen. 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-

Kostenloser Download NIST Cybersecurity Framework unter [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)



IKT-Minimalstandard unter [www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt\\_minimalstandard.html](http://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html)



Anzeige

**FLEXIBEL  
LEISTUNGSSTARK  
EFFIZIENT**

MEMBER OF SWISSFACTORY GROUP

**MASCHINENBAU IM GROSSFORMAT**

Mit unserem modernen Maschinenpark bearbeiten wir Werkstücke mit 5 Achsen bis 75t und bis 18'000mm x 3'500mm x 3'000mm und Drehteile bis D 2'000 und L 6'000. (Aber es geht natürlich auch kleiner). Zudem verfügen wir über Schweiss-Kapazitäten und Lackiermöglichkeiten für Teile bis 20t.

Konstruktion  
Grossteile  
Schlosserei  
Mechanik  
Maschinenbau  
Montage  
Lackieren

**Bunorm Maschinenbau AG** | 062 919 20 40 | [www.bunorm.ch](http://www.bunorm.ch)

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
	Maintenance	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
Recover	Improvements	RS.IM
	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Bild 2: Die 23 Kategorien.

Function	Category	Subcategory	Informative References
	<b>Asset Management (ID.AM):</b> 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.	<b>ID.AM-1:</b> Physical devices and systems within the organization are inventoried.	<ul style="list-style-type: none"> <li>CIS CSC 1</li> <li>COBIT 5 BAI09.01, BAI09.02</li> <li>ISA 62443-2-1:2009 4.2.3.4</li> <li>ISA 62443-3-3:2013 SR 7.8</li> <li>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</li> <li>NIST SP 800-53 Rev. 4 CM-8, PM-5</li> </ul>

Bild 3: ID.AM-1.

setzung aussehen könnte, kann auf andere Richtlinien wie das Grundschrift-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 errei-

chen, 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.

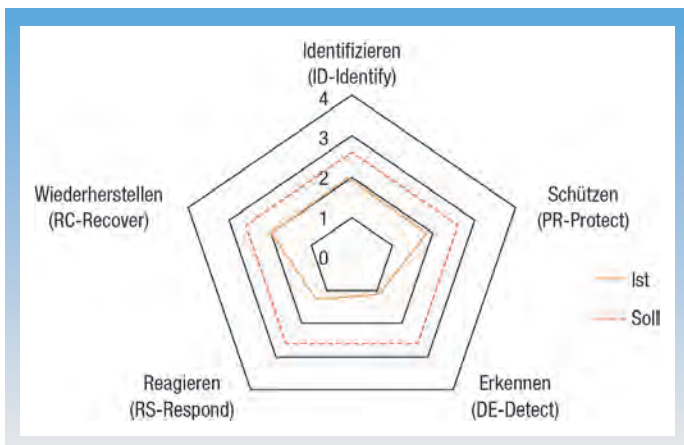


Bild 4: Overall Cyber Security Maturity Bewertung.

■ Anzeige

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.

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

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.

# Suche Stelle als Polymechaniker 100%

Ich arbeite für mein Leben gerne in der Produktion! Nichts ist mir zu streng. Auch Sonderschichten oder **das Arbeiten rund um die Uhr** gehören zu meiner Leidenschaft. Ich bin Ihr neuer Mitarbeiter!

- hohe Leistungsbereitschaft
- prozessstreu und schnell
- präzises, konzentriertes Arbeiten
- selbstständiges Arbeiten gewohnt
- loyal
- keine Abwesenheiten

Suche eine **neue Herausforderung in modernen Betrieben**. Meine Arbeit wurde einige Male ausgezeichnet, darum ergänze ich Ihr Team optimal und am richtigen Ort. **Mich kann man nicht bremsen**, mich muss man nur schnell programmieren.

Hier geht's zu meinen Bewerbungsunterlagen:

Freu mich auf Ihre Kontaktaufnahme und Jobangebote unter:

[r-c2@gressel.ch](mailto:r-c2@gressel.ch)



qrco.de/bcse7c