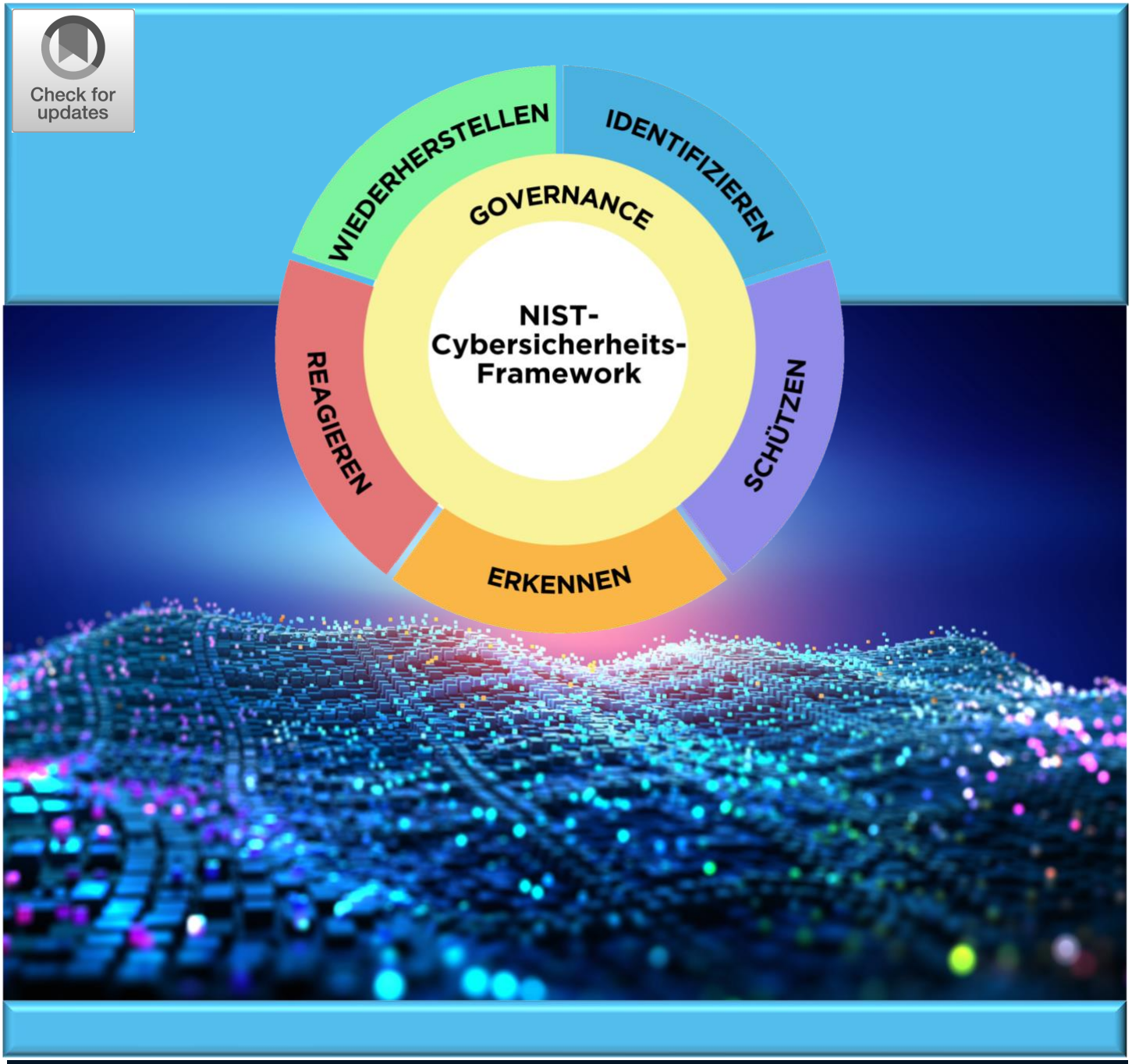

NIST-Cybersicherheits-Framework (CSF) 2.0

National Institute of Standards and Technology
Diese Veröffentlichung ist kostenlos unter https://doi.org/10.6028/NIST.CSWP.29.ger erhältlich.

26. Februar 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Abstract

Das NIST-Cybersicherheits-Framework (CSF) 2.0 ist ein Leitfaden für die Industrie, Behörden und andere Organisationen zum Management von Cybersicherheitsrisiken. Es bietet eine Taxonomie von hochrangigen Cybersicherheitsergebnissen, die von jeder Organisation – unabhängig von ihrer Größe, Branche oder ihrem Reifegrad – verwendet werden kann, um ihre Cybersicherheitsmaßnahmen besser zu verstehen, zu bewerten, zu priorisieren und zu kommunizieren. Das CSF schreibt nicht vor, wie die Ergebnisse erreicht werden sollten. Vielmehr verweist es auf Online-Ressourcen, die zusätzliche Anleitungen zu Praktiken und Kontrollen bieten, die zur Erreichung dieser Ergebnisse eingesetzt werden können. Dieses Dokument beschreibt das CSF 2.0, seine Komponenten und einige der vielen Möglichkeiten, wie es verwendet werden kann.

Keywords

Cybersicherheit; Cybersecurity Framework (CSF); Cybersecurity Risk Governance; Risikomanagement im Bereich Cybersicherheit; Risikomanagement für Unternehmen; Profile; Ebenen

Zielgruppe

Das CSF richtet sich in erster Linie an Personen, die für die Entwicklung und Leitung von Cybersicherheitsprogrammen verantwortlich sind. Das CSF kann auch von anderen am Risikomanagement beteiligten Personen verwendet werden, z. B. von Führungskräften, Vorständen, Akquisitionsfachkräften, Technologieexperten, Risikomanagern, Rechtsanwälten, Personalfachkräften und Auditoren für Cybersicherheit und Risikomanagement, um ihre Entscheidungen in Bezug auf Cybersicherheit zu treffen. Darüber hinaus kann das CSF für diejenigen nützlich sein, die politische Entscheidungen treffen und beeinflussen (z. B. Verbände, Berufsverbände, Regulierungsbehörden), die Prioritäten für das Management von Cybersicherheitsrisiken festlegen und kommunizieren.

Ergänzende Inhalte

NIST wird weiterhin zusätzliche Ressourcen erstellen und bereitstellen, um Organisationen bei der Umsetzung des CSF zu unterstützen, darunter Kurzanleitungen und Community-Profile. Alle Ressourcen werden auf der NIST-CSF-Website öffentlich zugänglich gemacht. Vorschläge für zusätzliche Ressourcen auf der NIST-CSF-Website können jederzeit mit NIST unter cyberframework@nist.gov geteilt werden.

Hinweis für die Leser

Sofern nicht anders angegeben, sind die in dieser Veröffentlichung zitierten, referenzierten oder auszugsweise wiedergegebenen Dokumente nicht vollständig in diese Veröffentlichung aufgenommen.

Vor der Version 2.0 trug das Cybersicherheits-Framework die Bezeichnung „Framework for Improving Critical Infrastructure Cybersecurity“. Dieser Titel wird für das CSF 2.0 nicht verwendet.

Danksagungen

Das CSF ist das Ergebnis einer mehrjährigen gemeinsamen Anstrengung von Industrie, Wissenschaft und von Regierungen in den Vereinigten Staaten und der ganzen Welt. Das NIST dankt all jenen, die zu diesem überarbeiteten CSF beigetragen haben, und spricht ihnen seine Anerkennung aus. Informationen über den CSF-Entwicklungsprozess finden Sie auf der NIST-CSF-Website. Erfahrungen mit der Anwendung des CSF können jederzeit mit NIST unter cyberframework@nist.gov geteilt werden.

Inhaltsverzeichnis

Liste der Abbildungen

Vorwort

Das Cybersicherheits-Framework (CSF) 2.0 soll Organisationen aller Größen und Sektoren – einschließlich Industrie, Behörden, Hochschulen und gemeinnützige Organisationen – dabei helfen, ihre Cybersicherheitsrisiken zu steuern und zu verringern. Es ist unabhängig vom Reifegrad und der technischen Ausgereiftheit der Cybersicherheitsprogramme einer Organisation nützlich. Dennoch verfolgt das CSF keinen Einheitsansatz, der für alle gilt. Jede Organisation hat sowohl gemeinsame als auch einzigartige Risiken sowie eine unterschiedliche Risikobereitschaft und -toleranz, spezifische Aufgaben und Ziele zur Erreichung dieser Aufgaben. Die Art und Weise, wie eine Organisation das CSF umsetzt, ist daher zwangsläufig unterschiedlich.

Idealerweise wird das CSF dazu verwendet, um Cybersicherheitsrisiken zusammen mit anderen Risiken des Unternehmens anzugehen, einschließlich Risiken finanzieller, datenschutzrechtlicher, lieferkettenbezogener, reputationsbezogener, technologischer oder physischer Natur.

Das CSF beschreibt die gewünschten Ergebnisse, die von einem breiten Publikum verstanden werden sollen, einschließlich Führungskräften, Managern und Praktikern, unabhängig von ihrem Fachwissen im Bereich der Cybersicherheit. Da diese Ergebnisse branchen-, länder- und technologieneutral sind, bieten sie einer Organisation die nötige Flexibilität, um ihre speziellen Risiken, Technologien und Aufgaben zu berücksichtigen. Die Ergebnisse werden direkt einer Liste potenzieller Sicherheitskontrollen zugeordnet, die sofort in Betracht gezogen werden können, um Cybersicherheitsrisiken zu mindern.

Obwohl das CSF keine Vorschriften enthält, hilft es seinen Nutzern dabei, sich über spezifische Ergebnisse zu informieren und diese auszuwählen. Vorschläge, wie bestimmte Ergebnisse erreicht werden können, finden sich in einer wachsenden Zahl von Online-Ressourcen, die das CSF ergänzen, darunter eine Reihe von Kurzanleitungen (QSGs). Außerdem bieten verschiedene Tools herunterladbare Formate, um Organisationen zu helfen, die einige ihrer Prozesse automatisieren möchten. Die QSGs schlagen erste Möglichkeiten zur Nutzung des CSF vor und laden den Leser dazu ein, das CSF und die zugehörigen Ressourcen eingehender zu erforschen. Das CSF, diese ergänzenden Ressourcen von NIST und andere Ressourcen sind über die NIST-CSF-Website verfügbar und sollten als „CSF-Portfolio“ betrachtet werden, das bei dem Management und der Reduzierung von Risiken hilft. Unabhängig davon, wie es angewendet wird, fordert das CSF seine Nutzer auf, ihre Cybersicherheitslage im Kontext zu betrachten und das CSF dann an ihre spezifischen Bedürfnisse anzupassen.

Aufbauend auf früheren Versionen enthält das CSF 2.0 neue Funktionen, die die Bedeutung von *Governance* und *Lieferketten* hervorheben. Besonderes Augenmerk wird auf die Kurzanleitungen gelegt, um sicherzustellen, dass das CSF sowohl für kleinere als auch für größere Organisationen relevant und leicht zugänglich ist. Das NIST bietet nun Umsetzungsbeispiele und informative Referenzen, die online verfügbar sind und regelmäßig aktualisiert werden. Die Erstellung von Organisationsprofilen für den Ist- und Soll-Zustand hilft Organisationen, ihren Ist-Zustand mit dem Soll-Zustand zu vergleichen, und ermöglicht es ihnen, Sicherheitskontrollen schneller zu implementieren und zu bewerten.

Cybersicherheitsrisiken nehmen ständig zu, und das Management dieser Risiken muss ein kontinuierlicher Prozess sein. Dies gilt unabhängig davon, ob eine Organisation gerade erst beginnt, sich mit ihren Cybersicherheitsherausforderungen auseinanderzusetzen, oder ob sie bereits seit vielen Jahren aktiv ist und über ein hoch entwickeltes, gut ausgestattetes Cybersicherheitsteam verfügt. Das CSF ist so konzipiert, dass es für jede Art von Organisation von Nutzen ist, und es wird erwartet, dass es über einen langen Zeitraum hinweg eine angemessene Orientierung bietet.

1. Cybersicherheits-Framework (CSF) – Überblick

Dieses Dokument ist die Version 2.0 des NIST-Cybersicherheits-Framework (*Framework* oder *CSF*). Es umfasst die folgenden Komponenten:

- ***CSF-Kern***, die Grundlage des CSF, eine Taxonomie von hochrangigen Cybersicherheitsergebnissen, die jeder Organisation beim Management ihrer Cybersicherheitsrisiken helfen können. Die CSF-Kernkomponenten bestehen aus einer Hierarchie von Funktionen, Kategorien und Unterkategorien, die jedes Ergebnis detailliert beschreiben. Diese Ergebnisse können von einem breiten Publikum, einschließlich Führungskräften, Managern und Praktikern, unabhängig von ihrem Fachwissen im Bereich der Cybersicherheit verstanden werden. Da diese Ergebnisse branchen-, länder- und technologieneutral sind, bieten sie einer Organisation die nötige Flexibilität, um ihre speziellen Risiken, Technologien und Aufgaben zu berücksichtigen.
- ***CSF-Organisationsprofile***, die einen Mechanismus zur Beschreibung der aktuellen und/oder angestrebten Cybersicherheitslage einer Organisation in Bezug auf die Ergebnisse des CSF-Kerns darstellen.
- ***CSF-Ebenen***, die auf CSF-Organisationsprofile angewandt werden können, um die Strenge der Cybersicherheitsrisiko-Governance und -Managementpraktiken einer Organisation zu charakterisieren. Die Ebenen können auch Aufschluss darüber geben, wie eine Organisation Cybersicherheitsrisiken und die Prozesse zum Management dieser Risiken sieht.

Dieses Dokument beschreibt *welche* wünschenswerten Ergebnisse eine Organisation anstreben kann. Es schreibt keine Ergebnisse *vor* und auch nicht, *wie* sie erreicht werden können. Beschreibungen, wie eine Organisation diese Ergebnisse erreichen kann, sind in einer Reihe von Online-Ressourcen enthalten, die das CSF ergänzen und über die NIST-CSF-Website verfügbar sind. Diese Ressourcen bieten zusätzliche Anleitungen zu Praktiken und Kontrollen, die zur Erreichung der Ergebnisse eingesetzt werden können, und sollen einer Organisation helfen, das CSF zu verstehen, anzunehmen und zu nutzen. Sie umfassen:

- *Informative Referenzen* auf Quellen, die auf bestehende globale Normen, Standards, Frameworks, Vorschriften, Richtlinien usw. verweisen.
- *Umsetzungsbeispiele*, die mögliche Wege zur Erreichung der einzelnen Ergebnisse aufzeigen.
- *Kurzanleitungen* mit praktischen Anleitungen zur Nutzung des CSF und seiner Online-Ressourcen, einschließlich der Umstellung von früheren CSF-Versionen auf Version 2.0.
- *Gemeinschaftsprofile und Vorlagen für Organisationsprofile*, die einer Organisation helfen, das CSF in die Praxis umzusetzen und Prioritäten für das Management von Cybersicherheitsrisiken zu setzen.

Eine Organisation kann den CSF-Kern, die Profile und die Ebenen mit den ergänzenden Ressourcen verwenden, um Cybersicherheitsrisiken zu verstehen, zu bewerten, zu priorisieren und zu kommunizieren.

- **Verstehen und Bewerten:** Beschreiben Sie die aktuelle oder angestrebte Cybersicherheitslage eines Teils oder der gesamten Organisation, ermitteln Sie Lücken und bewerten Sie die Fortschritte bei der Behebung dieser Lücken.
- **Priorisieren:** Identifizieren, organisieren und priorisieren Sie Maßnahmen zur Bewältigung von Cybersicherheitsrisiken, die mit dem Auftrag der Organisation, den rechtlichen und regulatorischen Anforderungen sowie den Erwartungen an das Risikomanagement und die Governance übereinstimmen.
- **Kommunizieren:** Schaffen Sie eine gemeinsame Sprache für die Kommunikation innerhalb und außerhalb des Unternehmens über Risiken, Fähigkeiten, Bedürfnisse und Erwartungen im Bereich der Cybersicherheit.

Das CSF ist so konzipiert, dass es von Organisationen aller Größen und Sektoren genutzt werden kann, einschließlich Industrie, Behörden, Hochschulen und gemeinnützigen Organisationen, unabhängig vom Reifegrad ihrer Cybersicherheitsprogramme. Das CSF ist eine grundlegende Ressource, die sowohl auf freiwilliger Basis als auch durch staatliche Richtlinien und Vorschriften übernommen werden kann. Die Taxonomie des CSF und die referenzierten Standards, Richtlinien und Praktiken sind nicht länderspezifisch, und frühere Versionen des CSF wurden von vielen Regierungen und anderen Organisationen sowohl innerhalb als auch außerhalb der Vereinigten Staaten erfolgreich eingesetzt.

Das CSF sollte in Verbindung mit anderen Ressourcen (z. B. Frameworks, Standards, Richtlinien, führende Praktiken) verwendet werden, um Cybersicherheitsrisiken besser zu handhaben und das gesamte Management von Risiken der Informations- und Kommunikationstechnologie (IKT) auf Unternehmensebene zu unterstützen. Das CSF ist ein flexibles Framework, das für alle Organisationen unabhängig von ihrer Größe angepasst werden soll. Organisationen werden auch weiterhin einzigartige Risiken – einschließlich unterschiedlicher Bedrohungen und Schwachstellen – und Risikotoleranzen sowie einzigartige Organisationsziele und Anforderungen haben. Daher werden die Ansätze der Organisationen für das Risikomanagement und die Umsetzung des CSF unterschiedlich sein.

Der Rest dieses Dokuments ist wie folgt aufgebaut:

- Abschnitt 2 erläutert die Grundlagen des CSF-Kerns: Funktionen, Kategorien und Unterkategorien.
- Abschnitt 3 definiert die Konzepte der CSF-Profile und -Ebenen.
- Abschnitt 0 bietet einen Überblick über ausgewählte Komponenten der Online-Ressourcen des CSF: Informative Referenzen, Umsetzungsbeispiele und Kurzanleitungen.
- Abschnitt 5 erörtert, wie eine Organisation das CSF in andere Risikomanagementprogramme integrieren kann.

- Anhang A ist der Kern des CSF.
- Anhang B enthält eine fiktive Illustration der CSF-Ebenen.
- Anhang C ist ein Glossar der CSF-Terminologie.

2. Vorstellung des CSF-Kerns

Anhang A ist der CSF-Kern – eine Reihe von Cybersicherheitsergebnissen, geordnet nach Funktion, dann Kategorie und schließlich Unterkategorie, wie in Abb. 1 dargestellt. Diese Ergebnisse sind keine Checkliste der durchzuführenden Maßnahmen. Spezifische Maßnahmen, die zur Erreichung eines Ergebnisses ergriffen werden, variieren je nach Organisation und Anwendungsfall, ebenso wie die Personen, die für diese Maßnahmen verantwortlich sind. Die Reihenfolge und der Umfang der Funktionen, Kategorien und Unterkategorien im Kernbereich sagt nichts über die Reihenfolge oder die Wichtigkeit ihrer Erreichung aus. Die Struktur des Kerns soll vor allem diejenigen ansprechen, die mit der Umsetzung des Risikomanagements innerhalb einer Organisation betraut sind.

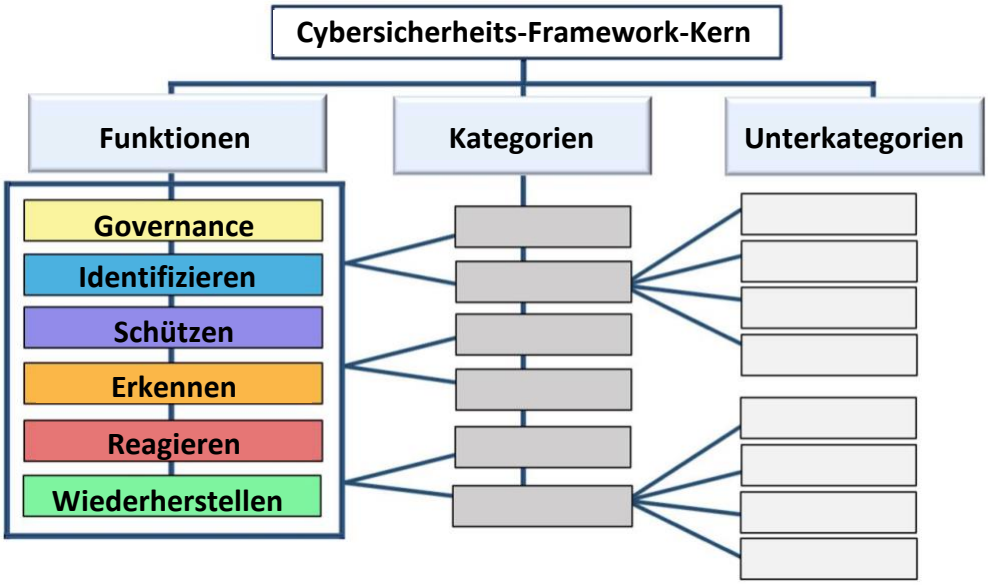

Abb. 1: CSF-Kernstruktur

Die CSF-Kernfunktionen – GOVERNANCE, IDENTIFIZIEREN, SCHÜTZEN, ERKENNEN, REAGIEREN und WIEDERHERSTELLEN – organisieren die Ergebnisse der Cybersicherheit auf ihrem höchsten Niveau.

- **GOVERNANCE (GV)** – *Die Strategie, Erwartungen und Richtlinien der Organisation für das Management von Cybersecurity-Risiken werden festgelegt, kommuniziert und überwacht.* Die GOVERNANCE-Funktion liefert Ergebnisse, die Aufschluss darüber geben, was eine Organisation tun kann, um die Ergebnisse der anderen fünf Funktionen im Kontext ihres Zwecks und der Erwartungen der Interessengruppen zu erreichen und zu priorisieren. Governance-Aktivitäten sind entscheidend für die Einbindung der Cybersicherheit in die umfassendere Risikomanagement-Strategie (ERM) einer Organisation. GOVERNANCE befasst sich mit dem Verständnis des organisatorischen Kontexts, der Festlegung der Cybersicherheitsstrategie und des Risikomanagements in der Cybersicherheits-Lieferkette, den Rollen, Verantwortlichkeiten und Befugnissen, den Richtlinien und der Überwachung der Cybersicherheitsstrategie.
- **IDENTIFIZIEREN (ID)** – *Die aktuellen Cybersicherheitsrisiken der Organisation sind bekannt.* Die Kenntnis der Vermögenswerte der Organisation (z. B. Daten, Hardware, Software,

Systeme, Einrichtungen, Dienstleistungen, Mitarbeiter), der Zulieferer und der damit verbundenen Cybersicherheitsrisiken ermöglicht es der Organisation, ihre Bemühungen im Einklang mit ihrer Risikomanagementstrategie und den unter GOVERNANCE ermittelten Missionsanforderungen zu priorisieren. Diese Funktion umfasst auch die Identifizierung von Verbesserungsmöglichkeiten für die Richtlinien, Pläne, Prozesse, Verfahren und Praktiken der Organisation, die das Cybersicherheits-Risikomanagement unterstützen, um die Bemühungen in allen sechs Funktionen zu unterstützen.

- **SCHÜTZEN (PR)** – *Schutzmaßnahmen zur Verwaltung der Cybersicherheitsrisiken der Organisation werden eingesetzt.* Sobald Vermögenswerte und Risiken identifiziert und priorisiert sind, unterstützt die Funktion SCHÜTZEN die Fähigkeit, diese Vermögenswerte zu sichern, um die Wahrscheinlichkeit und die Auswirkungen negativer Cybersicherheits-Ereignisse zu verhindern oder zu verringern sowie die Wahrscheinlichkeit und die Auswirkungen der Nutzung von Chancen zu erhöhen. Zu den von dieser Funktion abgedeckten Ergebnissen gehören Identitätsmanagement, Authentifizierung und Zugangskontrolle, Sensibilisierung und Schulung, Datensicherheit, Plattformsicherheit (d. h. Sicherung der Hardware, Software und Dienste physischer und virtueller Plattformen) und die Widerstandsfähigkeit der technologischen Infrastruktur.
- **ERKENNEN (DE)** – *Mögliche Cybersicherheitsangriffe und -kompromittierungen werden erkannt und analysiert.* Die Funktion ERKENNEN ermöglicht das rechtzeitige Entdecken und die Analyse von Anomalien, Indikatoren für eine Kompromittierung und anderen potenziell schädlichen Ereignissen, die auf Cybersicherheits-Angriffe und -Vorfälle hindeuten können. Diese Funktion unterstützt eine erfolgreiche Reaktion auf Vorfälle und Wiederherstellungsaktivitäten.
- **REAGIEREN (RS)** – *Es werden Maßnahmen in Bezug auf einen erkannten Cybersicherheitsvorfall ergriffen.* Die Funktion REAGIEREN unterstützt die Fähigkeit, die Auswirkungen von Cybersicherheitsvorfällen einzudämmen. Die Ergebnisse in dieser Funktion umfassen Vorfallsmanagement, Analyse, Schadensbegrenzung, Berichterstattung und Kommunikation.
- **WIEDERHERSTELLEN (RC)** – *Von einem Cybersicherheitsvorfall betroffene Anlagen und Abläufe werden wiederhergestellt.* Die Funktion WIEDERHERSTELLEN unterstützt die rechtzeitige Wiederherstellung des normalen Betriebs, um die Auswirkungen von Cybersicherheitsvorfällen zu verringern und eine angemessene Kommunikation während der Wiederherstellungsmaßnahmen zu ermöglichen.

Viele Aktivitäten im Rahmen des Managements von Cybersicherheitsrisiken konzentrieren sich zwar auf die Verhinderung negativer Ereignisse, können aber auch die Nutzung positiver Chancen unterstützen. Maßnahmen zur Verringerung des Cybersicherheitsrisikos können einer Organisation auch auf andere Weise zugutekommen, etwa durch die Steigerung der Einnahmen (z. B., indem zunächst einem kommerziellen Hosting-Anbieter überschüssige Räumlichkeiten für das Hosting der eigenen Rechenzentren und der Rechenzentren anderer Organisationen zur Verfügung gestellt werden und dann ein wichtiges Finanzsystem vom unternehmenseigenen Rechenzentrum zum Hosting-Anbieter verlagert wird, um die Cybersicherheitsrisiken zu verringern).

Abb. 2 zeigt die CSF-Funktionen als ein Rad, da alle Funktionen miteinander in Beziehung stehen. So wird eine Organisation beispielsweise Vermögenswerte unter IDENTIFIZIEREN kategorisieren und Schritte zur Sicherung dieser Vermögenswerte unter SCHÜTZEN unternehmen. Investitionen in die Planung und das Testen in den Funktionen GOVERNANCE und IDENTIFIZIEREN unterstützen die rechtzeitige Erkennung von unerwarteten Ereignissen in der Funktion ERKENNEN und ermöglichen die Reaktion auf Vorfälle und Wiederherstellungsmaßnahmen für Cybersicherheitsvorfälle in den Funktionen REAGIEREN und WIEDERHERSTELLEN. GOVERNANCE steht in der Mitte des Rades, weil es darüber informiert, wie eine Organisation die anderen fünf Funktionen implementiert.

Abb. 2: CSF-Funktionen

Die Funktionen sollten gleichzeitig bearbeitet werden. Die Maßnahmen zur Unterstützung von GOVERNANCE, IDENTIFIZIEREN, SCHÜTZEN und ERKENNEN sollten kontinuierlich durchgeführt werden, und die Maßnahmen zur Unterstützung von REAGIEREN und WIEDERHERSTELLEN sollten jederzeit bereit sein und bei Cybersicherheits-Vorfällen durchgeführt werden. Alle Funktionen haben wichtige Aufgaben im Zusammenhang mit Cybersicherheits-Vorfällen. Die Ergebnisse von GOVERNANCE, IDENTIFIZIEREN und SCHÜTZEN helfen bei der Vorbeugung und Vorbereitung auf

Vorfälle, während die Ergebnisse von GOVERNANCE, ERKENNEN, REAGIEREN und WIEDERHERSTELLEN bei der Entdeckung und Bewältigung von Vorfällen helfen.

Jede Funktion ist nach einem Verb benannt, das ihren Inhalt zusammenfasst. Jede Funktion ist in *Kategorien* unterteilt, bei denen es sich um verwandte Ergebnisse der Cybersicherheit handelt, die zusammen die Funktion ausmachen. *Unterkategorien* unterteilen jede Kategorie weiter in spezifischere Ergebnisse technischer und Managementaktivitäten. Die Unterkategorien sind nicht erschöpfend, aber sie beschreiben detaillierte Ergebnisse, die jede Kategorie unterstützen.

Die Funktionen, Kategorien und Unterkategorien gelten für alle von einer Organisation verwendeten IKT, einschließlich Informationstechnologie (IT), Internet der Dinge (IoT) und Betriebstechnologie (OT). Sie gelten auch für alle Arten von Technologieumgebungen, einschließlich Cloud, mobile und künstliche Intelligenzsysteme. Der CSF-Kern ist zukunftsorientiert und soll auch für künftige Veränderungen bei Technologien und Umgebungen gelten.

3. Einführung in CSF-Profile und -Ebenen

Dieser Abschnitt definiert die Konzepte der CSF-Profile und -Ebenen.

3.1. CSF-Profile

Ein *CSF-Organisationsprofil* beschreibt die aktuelle und/oder angestrebte Cybersicherheitslage einer Organisation in Bezug auf die Ergebnisse des Kerns. Organisationsprofile werden verwendet, um die Ergebnisse des Kerns zu verstehen, anzupassen, zu bewerten, zu priorisieren und zu kommunizieren, indem die Auftragsziele einer Organisation, die Erwartungen der Stakeholder, die Bedrohungslandschaft und die Anforderungen berücksichtigt werden. Eine Organisation kann dann ihre Maßnahmen priorisieren, um bestimmte Ergebnisse zu erreichen, und diese Informationen an die Stakeholder weitergeben.

Jedes Organisationsprofil enthält eines oder beide der folgenden Elemente:

1. Ein *aktuelles Profil*, das die Kernergebnisse, die eine Organisation derzeit erreicht (oder zu erreichen versucht), spezifiziert und beschreibt, wie oder in welchem Ausmaß die einzelnen Ergebnisse erreicht werden.
2. Ein *Zielprofil*, das die gewünschten Ergebnisse angibt, die eine Organisation ausgewählt und priorisiert hat, um ihre Ziele im Bereich des Cybersicherheits-Risikomanagements zu erreichen. Ein Zielprofil berücksichtigt voraussichtliche Änderungen an der Cybersicherheitslage der Organisation, wie z. B. neue Anforderungen, die Einführung neuer Technologien und Bedrohungsanalyse-Trends.

Ein *Gemeinschaftsprofil* ist eine Basis von CSF-Ergebnissen, das erstellt und veröffentlicht wird, um gemeinsame Interessen und Ziele einer Reihe von Organisationen zu berücksichtigen. Ein Gemeinschaftsprofil wird in der Regel für einen bestimmten Sektor, Teilsektor, eine bestimmte Technologie, eine bestimmte Bedrohungsart oder einen anderen Anwendungsfall entwickelt. Eine Organisation kann ein Gemeinschaftsprofil als Grundlage für ihr eigenes Zielprofil verwenden. Beispiele für Gemeinschaftsprofile sind auf der NIST-CSF-Website zu finden.

Die in Abb. 3 dargestellten und im Folgenden zusammengefassten Schritte veranschaulichen eine Möglichkeit, wie eine Organisation ein Organisationsprofil nutzen kann, um die kontinuierliche Verbesserung ihrer Cybersicherheit zu unterstützen.

Abb. 3: Schritte zur Erstellung und Verwendung eines CSF-Organisationsprofils

1. **Umfang des Organisationsprofils.** Dokumentieren Sie die wichtigsten Fakten und Annahmen, auf denen das Profil basieren wird, um seinen Umfang zu definieren. Eine Organisation kann beliebig viele Organisationsprofile erstellen, die jeweils einen unterschiedlichen Umfang haben. Ein Profil kann sich beispielsweise auf die gesamte Organisation beziehen oder auf die Finanzsysteme einer Organisation oder auf die Abwehr von Ransomware-Bedrohungen und den Umgang mit Ransomware-Vorfällen, die diese Finanzsysteme betreffen, beschränkt sein.
2. **Sammeln der für die Erstellung des Organisationsprofils erforderlichen Informationen.** Beispiele für Informationen können Organisationsrichtlinien, Prioritäten und Ressourcen für das Risikomanagement, Risikoprofile des Unternehmens, Register für die Analyse der Auswirkungen auf das Geschäft (BIA), von der Organisation befolgte Cybersicherheitsanforderungen und -standards, Praktiken und Instrumente (z. B. Verfahren und Schutzmaßnahmen) sowie Arbeitsrollen sein.
3. **Erstellen des Organisationsprofils.** Bestimmen Sie, welche Arten von Informationen das Profil für die ausgewählten CSF-Ergebnisse enthalten soll, und dokumentieren Sie die benötigten Informationen. Berücksichtigen Sie die Risikoimplikationen des aktuellen Profils für die Planung und Priorisierung des Zielprofils. Erwägen Sie auch, ein Gemeinschaftsprofil als Grundlage für das Zielprofil zu verwenden.
4. **Analysieren der Lücken zwischen dem aktuellem und dem Zielprofil und erstellen eines Aktionsplans.** Führen Sie eine Lückenanalyse durch, um die Unterschiede zwischen dem aktuellem und dem Zielprofil zu identifizieren und zu analysieren, und entwickeln Sie einen nach Prioritäten geordneten Aktionsplan (z. B. Risikoregister, Risikodetailbericht, Aktions- und Meilensteinplan [POA&M]), um diese Lücken zu schließen.
5. **Umsetzen des Aktionsplans und Aktualisieren des Organisationsprofils.** Befolgen Sie den Aktionsplan, um die Lücken zu schließen und die Organisation in Richtung des Zielprofils zu bewegen. Ein Aktionsplan kann eine allgemeine Frist haben oder fortlaufend sein.

Angesichts der Bedeutung der kontinuierlichen Verbesserung kann eine Organisation diese Schritte so oft wie nötig wiederholen.

Es gibt weitere Verwendungsmöglichkeiten für Organisationsprofile. Ein aktuelles Profil kann beispielsweise dazu verwendet werden, die Cybersicherheitsfähigkeiten der Organisation und bekannte Verbesserungsmöglichkeiten zu dokumentieren und mit externen Interessengruppen wie Geschäftspartnern oder potenziellen Kunden zu kommunizieren. Außerdem kann ein Zielprofil dabei helfen, die Anforderungen und Erwartungen der Organisation an das Cybersicherheits-Risikomanagement gegenüber Lieferanten, Partnern und anderen Dritten als Zielvorgabe zu formulieren, die diese Parteien erreichen müssen.

3.2. CSF-Ebenen

Eine Organisation kann die Ebenen als Grundlage für ihr aktuelles Profil und ihr Zielprofil verwenden. Die Ebenen charakterisieren die Strenge der Governance- und Managementpraktiken für Cybersicherheitsrisiken einer Organisation und geben Aufschluss darüber, wie eine Organisation Cybersicherheitsrisiken und die zur Verwaltung dieser Risiken eingesetzten Prozesse sieht. Die Ebenen, wie in Abb. 4 und fiktiv in Anhang B veranschaulicht dargestellt, spiegeln die Praktiken einer Organisation für das Management von Cybersicherheitsrisiken als teilweise (Ebene 1), risikoinformiert (Ebene 2), wiederholbar (Ebene 3) und anpassungsfähig (Ebene 4) wider. Die Ebenen beschreiben eine Entwicklung von informellen Ad-hoc-Reaktionen hin zu agilen, risikoinformierten und kontinuierlich verbesserten Ansätzen. Die Auswahl der Ebenen hilft dabei, den Grundtenor für die Art und Weise festzulegen, wie eine Organisation ihre Cybersicherheitsrisiken handhaben wird.

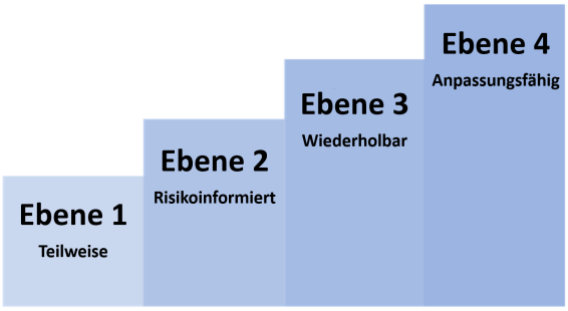

Abb. 4: CSF-Ebenen für Governance und Management von Cybersicherheitsrisiken

Die Ebenen sollten die Methodik eines Unternehmens für das Management von Cybersicherheitsrisiken ergänzen und nicht ersetzen. Beispielsweise kann eine Organisation die Ebenen zur internen Kommunikation als Maßstab für einen organisationsweiten[1] Ansatz zum Management von Cybersicherheitsrisiken verwenden. Ein Aufstieg in höhere Ebenen wird empfohlen, wenn die Risiken oder Anforderungen größer sind oder wenn eine Kosten-Nutzen-Analyse eine machbare und kosteneffiziente Reduzierung negativer Cybersicherheitsrisiken ergibt

[1] Für die Zwecke dieses Dokuments haben die Begriffe „organisationsweit“ und „Unternehmen“ die gleiche Bedeutung.

Die NIST-CSF-Website bietet zusätzliche Informationen zur Verwendung von Profilen und Ebenen. Sie enthält Verweise auf von NIST gehosteten Vorlagen für Organisationsprofile und eine Sammlung von Gemeinschaftsprofilen in einer Vielzahl von maschinenlesbaren und für den Menschen nutzbaren Formaten.

4. Einführung in Online-Ressourcen, die das CSF ergänzen

Das NIST und andere Organisationen haben eine Reihe von Online-Ressourcen erstellt, die Organisationen helfen, das CSF zu verstehen, zu übernehmen und zu verwenden. Da sie online gehostet werden, können diese zusätzlichen Ressourcen häufiger aktualisiert werden als dieses Dokument, das nur selten aktualisiert wird, um seinen Benutzern Stabilität zu bieten, und in maschinenlesbaren Formaten verfügbar sein. In diesem Abschnitt wird ein Überblick über drei Arten von Online-Ressourcen gegeben: Informative Referenzen, Umsetzungsbeispiele und Kurzanleitungen.

Informative Referenzen sind Zuordnungen, die Beziehungen zwischen dem Kern und verschiedenen Standards, Richtlinien, Vorschriften und anderen Inhalten aufzeigen. Informative Referenzen geben Auskunft darüber, wie eine Organisation die Ergebnisse des Kerns erreichen kann. Informative Referenzen können sektor- oder technologiespezifisch sein. Sie können vom NIST oder einer anderen Organisation erstellt werden. Manche informativen Referenzen sind enger gefasst als eine Unterkategorie. Zum Beispiel kann eine bestimmte Kontrolle aus SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, eine von vielen Referenzen sein, die benötigt werden, um das in einer Unterkategorie beschriebene Ergebnis zu erreichen. Andere informative Referenzen können übergeordneter Natur sein, wie z. B. eine Anforderung aus einer Richtlinie, die teilweise zahlreiche Unterkategorien anspricht. Bei der Verwendung des CSF kann eine Organisation die wichtigsten informativen Referenzen identifizieren.

Beispiele für die Umsetzung bieten fiktive Beispiele für prägnante, handlungsorientierte Schritte, die helfen, die Ergebnisse der Unterkategorien zu erreichen. Zu den Verben, mit denen die Beispiele ausgedrückt werden, gehören teilen, dokumentieren, entwickeln, durchführen, überwachen, analysieren, bewerten und üben. Die Beispiele sind keine umfassende Liste aller Maßnahmen, die von einer Organisation ergriffen werden könnten, um ein Ergebnis zu erreichen, noch stellen sie eine Grundlinie der erforderlichen Maßnahmen zur Bewältigung von Cybersicherheitsrisiken dar.

Kurzanleitungen (QSGs) sind kurze Dokumente zu bestimmten CSF-bezogenen Themen und sind oft auf bestimmte Zielgruppen zugeschnitten. Kurzanleitungen können einer Organisation bei der Umsetzung des CSF helfen, da sie spezifische Teile des CSF in umsetzbare „erste Schritte“ destillieren, die eine Organisation auf dem Weg zur Verbesserung ihrer Cybersicherheitslage und des Managements der damit verbundenen Risiken in Betracht ziehen kann. Die Anleitungen werden in ihrem eigenen Zeitrahmen überarbeitet, und neue Anleitungen werden nach Bedarf hinzugefügt.

Vorschläge für neue informative Referenzen für das CSF 2.0 können jederzeit an NIST unter olir@nist.gov weitergeleitet werden. Vorschläge für andere Ressourcen, die auf der NIST-CSF-Website aufgeführt werden sollen, einschließlich zusätzlicher QSG-Themen, sollten an cyberframework@nist.gov gerichtet werden.

5. Verbesserung der Kommunikation und Integration von Cybersicherheitsrisiken

Die Anwendung des CSF hängt von den spezifischen Aufgaben und Risiken einer Organisation ab. Wenn eine Organisation die Erwartungen der Stakeholder sowie die Risikobereitschaft und -toleranz (wie in GOVERNANCE beschrieben) kennt, kann sie Prioritäten für Cybersicherheits-Aktivitäten setzen und fundierte Entscheidungen über Cybersicherheits-Ausgaben und -Maßnahmen treffen. Je nach den potenziellen Auswirkungen und Wahrscheinlichkeiten kann eine Organisation eine oder mehrere Arten des Umgangs mit Risiken wählen – einschließlich der Abschwächung, Übertragung, Vermeidung oder Akzeptanz negativer Risiken und der Realisierung, Weitergabe, Verbesserung oder Akzeptanz positiver Risiken. Wichtig ist, dass eine Organisation das CSF sowohl intern zur Verwaltung ihrer Cybersicherheitskapazitäten als auch extern zur Überwachung oder Kommunikation mit Dritten verwenden kann.

Unabhängig von der Verwendung des CSF kann eine Organisation davon profitieren, wenn sie den CSF als Leitfaden verwendet, um Cybersicherheitsrisiken und die Maßnahmen zur Bewältigung dieser Risiken zu verstehen, zu bewerten, zu priorisieren und zu kommunizieren. Die ausgewählten Ergebnisse können genutzt werden, um sich auf strategische Entscheidungen zu konzentrieren und diese umzusetzen, um die Cybersicherheitslage zu verbessern und die Kontinuität der missionswichtigen Funktionen aufrechtzuerhalten, wobei die Prioritäten und die verfügbaren Ressourcen berücksichtigt werden.

5.1. Verbesserung der Risikomanagement-Kommunikation

Das CSF bietet eine Grundlage für eine verbesserte Kommunikation in Bezug auf Erwartungen, Planung und Ressourcen im Bereich der Cybersicherheit. Das CSF fördert den bidirektionalen Informationsfluss (wie in der oberen Hälfte von Abb. 5 gezeigt) zwischen den Führungskräften, die sich auf die Prioritäten und die strategische Ausrichtung des Unternehmens konzentrieren, und den Managern, die sich um spezifische Cybersicherheitsrisiken kümmern, die das Erreichen dieser Prioritäten beeinträchtigen könnten. Das CSF unterstützt auch einen ähnlichen Informationsfluss (wie in der unteren Hälfte von Abb. 5 gezeigt) zwischen den Managern und den Praktikern, die die Technologien implementieren und betreiben. Die linke Seite der Abbildung zeigt, wie wichtig es ist, dass die Praktiker ihre Aktualisierungen, Erkenntnisse und Bedenken mit den Managern und Führungskräften teilen.

Abb. 5: Verwendung des CSF zur Verbesserung der Risikomanagementkommunikation

Zur Vorbereitung auf die Erstellung und Verwendung von Organisationsprofilen gehört das Sammeln von Informationen über die Prioritäten der Organisation, die Ressourcen und die Risikoausrichtung von Führungskräften. Manager arbeiten dann mit Praktikern zusammen, um Geschäftsanforderungen zu kommunizieren und risikobezogene Organisationsprofile zu erstellen. Maßnahmen zur Schließung etwaiger Lücken zwischen dem aktuellem und dem Zielprofil werden von Managern und Praktikern umgesetzt und liefern wichtige Beiträge zu Plänen auf Systemebene. Sobald der Soll-Zustand in der gesamten Organisation erreicht ist – auch durch Kontrollen und Überwachung auf Systemebene – können die aktualisierten Ergebnisse über Risikoregister und Fortschrittsberichte weitergegeben werden. Im Rahmen der fortlaufenden Bewertung gewinnen die Manager Erkenntnisse, um Anpassungen vorzunehmen, die die potenziellen Schäden weiter verringern und den potenziellen Nutzen erhöhen.

Die GOVERNANCE-Funktion unterstützt die Risikokommunikation der Organisation mit den **Führungskräften**. Bei den Gesprächen mit den Führungskräften geht es um die Strategie, insbesondere darum, wie sich Unwägbarkeiten im Zusammenhang mit der Cybersicherheit auf das Erreichen der Unternehmensziele auswirken könnten. Diese Governance-Diskussionen unterstützen den Dialog und die Einigung über Risikomanagement-Strategien (einschließlich Risiken in der Cybersicherheits-Lieferkette), Rollen, Verantwortlichkeiten und Befugnisse, Richtlinien und Aufsicht. Während die Führungskräfte auf der Grundlage dieser Bedürfnisse Prioritäten und Ziele für die Cybersicherheit festlegen, kommunizieren sie die Erwartungen hinsichtlich Risikobereitschaft, Verantwortlichkeit und Ressourcen. Führungskräfte sind auch für die Integration des Cybersicherheits-Risikomanagements in ERM-Programme und Risikomanagementprogramme auf niedrigerer Ebene verantwortlich (siehe Abschnitt 5.2). Die Kommunikation, die in der oberen Hälfte von Abb. 5 dargestellt ist, kann Überlegungen zum ERM und zu den untergeordneten Programmen enthalten und somit Manager und Praktiker anleiten.

Die von den Führungskräften festgelegten Gesamtziele für die Cybersicherheit werden von den **Managern** mitgeteilt und an diese weitergegeben. In einem Wirtschaftsunternehmen können diese Ziele für einen Geschäftsbereich oder eine Betriebsabteilung gelten. Bei staatlichen Einrichtungen können diese Ziele auf Abteilungs- oder Zweigstellenebene gelten. Bei der Umsetzung des CSF konzentrieren sich die Manager darauf, wie die Risikoziele durch gemeinsame Dienste, Kontrollen und Zusammenarbeit erreicht werden können, wie sie im Zielprofil ausgedrückt und durch die im Aktionsplan verfolgten Maßnahmen (z. B. Risikoregister, Risikodetailbericht, Aktions- und Meilensteinplan) verbessert werden.

Praktiker konzentrieren sich auf die Umsetzung des Zielzustands und die Messung von Änderungen des operativen Risikos, um die Planung, Durchführung und Überwachung spezifischer Cybersicherheitsaktivitäten zu unterstützen. Während die Kontrollen implementiert werden, um das Risiko auf einem akzeptablen Niveau zu halten, stellen die Praktiker Managern und Führungskräften die Informationen zur Verfügung (z. B. wichtige Leistungsindikatoren, wichtige Risikoindikatoren), die sie benötigen, um die Cybersicherheitslage des Unternehmens zu verstehen, fundierte Entscheidungen zu treffen und die Risikostrategie entsprechend beizubehalten oder anzupassen. Führungskräfte können diese Cybersicherheits-Risikodaten auch mit Informationen über andere Risikotypen aus dem gesamten Unternehmen kombinieren. Aktualisierungen der Erwartungen und Prioritäten werden in die aktualisierten Organisationsprofile aufgenommen, wenn sich der Zyklus wiederholt.

5.2. Verbesserung der Integration mit anderen Programmen des Risikomanagements

Jede Organisation ist mit zahlreichen Arten von IKT-Risiken konfrontiert (z. B. Datenschutz, Lieferkette, künstliche Intelligenz) und kann Frameworks und Managementinstrumente verwenden, die für jedes Risiko spezifisch sind. Einige Unternehmen integrieren die IKT und alle anderen Risikomanagementmaßnahmen auf hohem Niveau, indem sie ERM einsetzen, während andere die Maßnahmen getrennt halten, um sicherzustellen, dass jedem einzelnen Risiko angemessene Aufmerksamkeit gewidmet wird. Kleine Organisationen überwachen die Risiken naturgemäß auf Unternehmensebene, während größere Unternehmen ein separates, in das ERM integriertes Risikomanagement betreiben können.

Unternehmen können einen ERM-Ansatz anwenden, um ein Portfolio von Risikoüberlegungen, einschließlich Cybersicherheit, abzuwägen und fundierte Entscheidungen zu treffen. Führungskräfte erhalten wichtige Informationen über aktuelle und geplante Risikoaktivitäten, da sie Governance- und Risikostrategien mit den Ergebnissen aus früheren Anwendungen des CSF integrieren. Das CSF hilft Organisationen, ihre Terminologie für Cybersicherheit und Cybersicherheits-Risikomanagement in eine allgemeine Risikomanagement-Sprache zu übersetzen, die von Führungskräften verstanden wird.

Zu den NIST-Ressourcen, die die gegenseitige Beziehung zwischen Cybersicherheits-Risikomanagement und ERM beschreiben, gehören:

- *NIST Cybersecurity Framework 2.0 – Enterprise Risk Management Quick-Start Guide*

- NIST Interagency Report (IR) 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*
- IR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management*
- IR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management*
- IR 8286C, *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight*
- IR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*
- SP 800-221, *Enterprise Impact of Information and Communications Technology Risk: Governing and Managing ICT Risk Programs Within an Enterprise Risk Portfolio*
- SP 800-221A, *Information and Communications Technology (ICT) Risk Outcomes: Integrating ICT Risk Management Programs with the Enterprise Risk Portfolio*

Eine Organisation kann das CSF auch für die Integration des Cybersicherheits-Risikomanagements in individuelle IKT-Risikomanagementprogramme als nützlich erachten, wie z. B.:

- **Cybersicherheits-Risikomanagement und -Bewertung:** Das CSF kann in etablierte Cybersicherheits-Risikomanagement- und -Bewertungsprogramme integriert werden, wie SP 800-37, *Risk Management Framework for Information Systems and Organizations*, und SP 800-30, *Guide for Conducting Risk Assessments* des NIST Risk Management Framework (RMF). Für eine Organisation, die das NIST RMF und die dazugehörigen Publikationen verwendet, kann das CSF verwendet werden, um den Ansatz des RMF zur Auswahl und Priorisierung von Kontrollen aus SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* zu ergänzen.
- **Datenschutzrisiken:** Obwohl Cybersicherheit und Datenschutz unabhängige Disziplinen sind, überschneiden sich ihre Ziele unter bestimmten Umständen, wie in Abb. 6 illustriert.

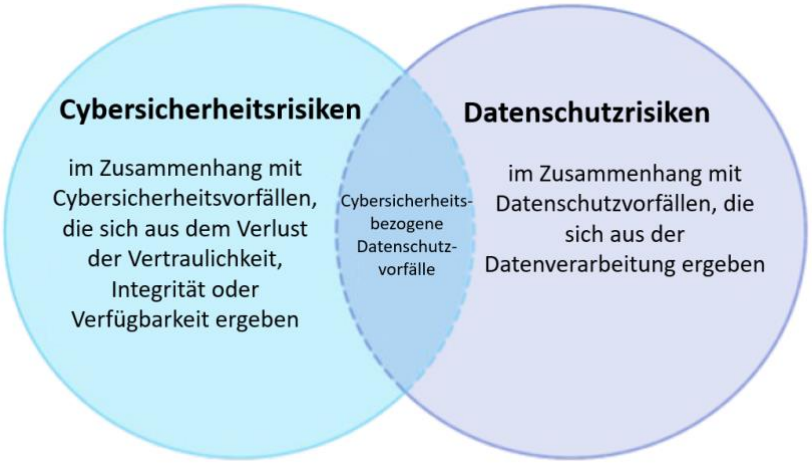

Abb. 6: Beziehung zwischen Cybersicherheit und Datenschutzrisiko

Das Risikomanagement im Bereich der Cybersicherheit ist von entscheidender Bedeutung, wenn es darum geht, Risiken für den Schutz der Privatsphäre im Zusammenhang mit dem Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit der Daten des Einzelnen zu begegnen. So können Datenverletzungen beispielsweise zu Identitätsdiebstahl führen. Risiken für den Schutz der Privatsphäre können jedoch auch durch Mittel entstehen, die nichts mit Vorfällen im Bereich der Cybersicherheit zu tun haben.

Eine Organisation verarbeitet Daten, um Aufgaben oder Geschäftszwecke zu erfüllen, was manchmal zu Ereignissen in Bezug auf den Datenschutz führen kann, bei denen Einzelpersonen als Folge der Datenverarbeitung Probleme erfahren können. Diese Probleme können sich auf unterschiedliche Weise äußern, aber NIST beschreibt sie als Auswirkungen, die von der Würde (z. B. Verlegenheit oder Stigmatisierung) bis zu konkreteren Schäden (z. B. Diskriminierung, wirtschaftlicher Verlust oder körperlicher Schaden) reichen. Das NIST-Datenschutz-Framework und das Cybersicherheits-Framework können zusammen verwendet werden, um die verschiedenen Aspekte von Cybersicherheits- und Datenschutzrisiken zu behandeln. Darüber hinaus enthält die NIST-Methodik zur Bewertung von Datenschutzrisiken (Privacy Risk Assessment Methodology, PRAM) einen Katalog von Beispielproblemen, die bei der Bewertung von Datenschutzrisiken verwendet werden können.

- **Risiken in der Lieferkette:** Eine Organisation kann das CSF nutzen, um die Aufsicht über Cybersicherheits-Risiken und die Kommunikation mit den Beteiligten in der Lieferkette zu fördern. Alle Arten von Technologien stützen sich auf ein komplexes, weltweit verteiltes, umfangreiches und miteinander verbundenes Lieferketten-Ökosystem mit geografisch unterschiedlichen Routen und mehreren Outsourcing-Ebenen. Dieses Ökosystem besteht aus öffentlichen und privaten Einrichtungen (z. B. Beschaffern, Lieferanten, Entwicklern, Systemintegratoren, externen Systemdienstleistern und anderen technologiebezogenen Dienstleistern), die zusammenarbeiten, um Technologieprodukte und -dienste zu erforschen, zu entwickeln, zu entwerfen, herzustellen, zu erwerben, zu liefern, zu integrieren, zu betreiben, zu warten, zu entsorgen und anderweitig zu nutzen oder zu verwalten. Diese Interaktionen werden durch Technologien, Gesetze, Richtlinien, Verfahren und Praktiken geprägt und beeinflusst.

  Angesichts der komplexen und vernetzten Beziehungen in diesem Ökosystem ist das Risikomanagement in der Lieferkette (SCRM) für Unternehmen von entscheidender Bedeutung. Cybersecurity SCRM (C-SCRM) ist ein systematischer Prozess zum Management von Cybersicherheits-Risiken in der gesamten Lieferkette und zur Entwicklung geeigneter Reaktionsstrategien, Richtlinien, Prozesse und Verfahren. Die Unterkategorien innerhalb der CSF-Kategorie C-SCRM [GV.SC] stellen eine Verbindung zwischen Ergebnissen her, die sich rein auf die Cybersicherheit konzentrieren, und solchen, die sich auf C-SCRM konzentrieren. SP 800-161r1 (Revision 1) *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* enthält ausführliche Informationen zu C-SCRM.

- **Risiken durch neue Technologien:** In dem Maße, wie neue Technologien und neue Technologieanwendungen verfügbar werden, treten neue Risiken zutage. Ein aktuelles Beispiel ist die künstliche Intelligenz (KI), die Risiken für die Cybersicherheit und den Datenschutz sowie viele andere Arten von Risiken birgt. Das NIST Artificial Intelligence Risk Management Framework (AI RMF) wurde entwickelt, um diesen Risiken zu begegnen. Die Behandlung von KI-Risiken zusammen mit anderen Unternehmensrisiken (z. B. Finanz-, Cybersicherheits-, Reputations- und Datenschutzrisiken) führt zu einem integrierteren Ergebnis und zu organisatorischen Effizienzsteigerungen. Überlegungen und Ansätze zum Cybersicherheits- und Datenschutz-Risikomanagement sind auf die Konzeption, Entwicklung, Einführung, Bewertung und Nutzung von KI-Systemen anwendbar. Der KI-RMF-Kern verwendet Funktionen, Kategorien und Unterkategorien, um KI-Ergebnisse zu beschreiben und das Management von Risiken im Zusammenhang mit KI zu unterstützen.

Anhang A. CSF-Kern

In diesem Anhang werden die Funktionen, Kategorien und Unterkategorien des CSF-Kerns beschrieben. Tabelle 1 listet die Namen der CSF 2.0-Kernfunktionen und -kategorien sowie die eindeutigen alphabetischen Bezeichnungen auf. Jeder Funktionsname in der Tabelle ist mit dem entsprechenden Abschnitt des Anhangs verknüpft. Die Reihenfolge der Funktionen, Kategorien und Unterkategorien des Kerns ist nicht alphabetisch. Sie soll vor allem für diejenigen von Nutzen sein, die mit der Operationalisierung des Risikomanagements in einer Organisation betraut sind. Die Nummerierung der Unterkategorien ist absichtlich nicht fortlaufend; Lücken in der Nummerierung weisen auf Unterkategorien des CSF 1.1 hin, die in den CSF 2.0 verlagert wurden.

Tabelle 1. Namen und Bezeichnungen der Kernfunktionen und Kategorien des CSF 2.0

Funktion	Kategorie	Kategorienbezeichnung
Governance (GV)	Organisatorischer Kontext	GV.OC
	Strategie für das Risikomanagement	GV.RM
	Rollen, Zuständigkeiten und Befugnisse	GV.RR
	Richtlinie	GV.PO
	Aufsicht	GV.OV
	Cybersicherheits-Risikomanagement in der Lieferkette	GV.SC
Identifizieren (ID)	Vermögensverwaltung	ID.AM
	Risikobewertung	ID.RA
	Verbesserung	ID.IM
Schützen (PR)	Identitätsmanagement, Authentifizierung und Zugangskontrolle	PR.AA
	Sensibilisierung und Schulung	PR.AT
	Datensicherheit	PR.DS
	Plattformsicherheit	PR.PS
	Widerstandsfähigkeit der Technologieinfrastruktur	PR.IR
Erkennen (DE)	Kontinuierliche Überwachung	DE.CM
	Analyse unerwünschter Ereignisse	DE.AE
Reagieren (RS)	Management von Vorfällen	RS.MA
	Analyse von Vorfällen	RS.AN
	Berichterstattung und Kommunikation bei Vorfällen	RS.CO
	Entschärfung von Vorfällen	RS.MI
Wiederherstellen (RC)	Ausführung des Vorfall-Wiederherstellungsplans	RC.RP
	Kommunikation zur Vorfall-Wiederherstellung	RC.CO

Der CSF-Kern, die informativen Referenzen und die Umsetzungsbeispiele sind auf der CSF 2.0 Website und über das CSF 2.0 Reference Tool verfügbar, das es den Benutzern ermöglicht, sie zu erkunden und in menschen- und maschinenlesbare Formate zu exportieren. Der Kern des CSF 2.0 ist auch in einem Legacy-Format verfügbar, das dem des CSF 1.1 ähnelt.

GOVERNANCE (GV): Die Strategie, Erwartungen und Richtlinien der Organisation für das Management von Cybersicherheits-Risiken werden festgelegt, kommuniziert und überwacht.

- **Organisatorischer Kontext (GV.OC):** Die Umstände – Auftrag, Erwartungen der Stakeholder, Abhängigkeiten sowie rechtliche, regulatorische und vertragliche Anforderungen – im Zusammenhang mit den Entscheidungen der Organisation zum Cybersicherheits-Risikomanagement sind bekannt.
  - **GV.OC-01:** Der Zweck der Organisation wird verstanden und fließt in das Cybersicherheits-Risikomanagement ein.
  - **GV.OC-02:** Interne und externe Stakeholder werden verstanden und ihre Bedürfnisse und Erwartungen an das Cybersicherheits-Risikomanagement werden verstanden und berücksichtigt.
  - **GV.OC-03:** Die rechtlichen, regulatorischen und vertraglichen Anforderungen an die Cybersicherheit – einschließlich der Verpflichtungen in Bezug auf den Datenschutz und die bürgerlichen Freiheiten – werden verstanden und gehandhabt.
  - **GV.OC-04:** Wesentliche Ziele, Fähigkeiten und Dienstleistungen, von denen externe Stakeholder abhängen oder die sie von der Organisation erwarten, werden verstanden und kommuniziert.
  - **GV.OC-05:** Ergebnisse, Fähigkeiten und Dienstleistungen, von denen die Organisation abhängt, werden verstanden und kommuniziert.
- **Strategie für das Risikomanagement (GV.RM):** Die Prioritäten, Einschränkungen, Risikotoleranz und -bereitschaft sowie Annahmen der Organisation werden festgelegt, kommuniziert und zur Unterstützung von Entscheidungen über operationelle Risiken verwendet.
  - **GV.RM-01:** Die Risikomanagementziele sind festgelegt und von den Interessengruppen der Organisation gebilligt.
  - **GV.RM-02:** Erklärungen zur Risikobereitschaft und Risikotoleranz werden erstellt, kommuniziert und aufrechterhalten.
  - **GV.RM-03:** Aktivitäten und Ergebnisse des Cybersicherheits-Risikomanagements sind in die Risikomanagementprozesse des Unternehmens integriert.
  - **GV.RM-04:** Die strategische Ausrichtung, die geeignete Optionen für die Risikobewältigung beschreibt, ist festgelegt und kommuniziert.
  - **GV.RM-05:** Innerhalb der Organisation sind Kommunikationswege für Cybersicherheitsrisiken, einschließlich Risiken von Lieferanten und anderen Dritten, eingerichtet.
  - **GV.RM-06:** Eine standardisierte Methode zur Berechnung, Dokumentation, Kategorisierung und Priorisierung von Cybersicherheitsrisiken ist etabliert und kommuniziert.

- **GV.RM-07:** Strategische Chancen (d. h. positive Risiken) sind charakterisiert und werden in Diskussionen über Cybersicherheitsrisiken im Unternehmen einbezogen.

- **Rollen, Zuständigkeiten und Befugnisse (GV.RR):** Rollen, Zuständigkeiten und Befugnisse im Bereich der Cybersicherheit zur Förderung der Rechenschaftspflicht, Leistungsbewertung und kontinuierlichen Verbesserung sind festgelegt und kommuniziert.
  - **GV.RR-01:** Die Unternehmensführung ist für Cybersicherheits-Risiken verantwortlich und rechenschaftspflichtig und fördert eine risikobewusste, ethische und sich ständig verbessernde Kultur.
  - **GV.RR-02:** Rollen, Verantwortlichkeiten und Befugnisse im Zusammenhang mit dem Management von Cybersicherheits-Risiken sind festgelegt, kommuniziert, verstanden und durchgesetzt.
  - **GV.RR-03:** Angemessene Ressourcen werden entsprechend der Strategie für Cybersicherheits-Risiken, den Rollen, Verantwortlichkeiten und Richtlinien zugewiesen.
  - **GV.RR-04:** Cybersicherheit ist Bestandteil der Personalpraxis.

- **Richtlinie (GV.PO):** Organisatorische Cybersicherheitsrichtlinien werden festgelegt, kommuniziert und durchgesetzt.
  - **GV.PO-01:** Richtlinien für das Management von Cybersicherheitsrisiken werden auf der Grundlage des organisatorischen Kontexts, der Cybersicherheits-Strategie und der Prioritäten festgelegt, kommuniziert und durchgesetzt.
  - **GV.PO-02:** Die Richtlinien für das Management von Cybersicherheitsrisiken werden überprüft, aktualisiert, kommuniziert und durchgesetzt, um Änderungen der Anforderungen, Bedrohungen, Technologien und des Organisationszwecks zu berücksichtigen.

- **Aufsicht (GV.OV):** Die Ergebnisse der organisationsweiten Cybersicherheits-Risikomanagement-Aktivitäten und -Leistungen werden zur Information, Verbesserung und Anpassung der Risikomanagement-Strategie genutzt.
  - **GV.OV-01:** Die Ergebnisse der Strategie für das Cybersicherheits-Risikomanagement werden überprüft, um die Strategie und Ausrichtung anzuleiten und anzupassen.
  - **GV.OV-02:** Die Strategie für das Cybersicherheits-Risikomanagement wird überprüft und angepasst, um sicherzustellen, dass die organisatorischen Anforderungen und Risiken abgedeckt sind.
  - **GV.OV-03:** Die Leistung des organisatorischen Cybersicherheits-Risikomanagements wird bewertet und auf erforderliche Anpassungen hin überprüft.

- **Cybersicherheits-Risikomanagement in der Lieferkette (GV.SC):** Die Prozesse für das Cybersicherheits-Risikomanagement in der Lieferkette werden von organisatorischen Stakeholdern identifiziert, eingerichtet, verwaltet, überwacht und verbessert.

- **GV.SC-01:** Ein Programm zum Cybersicherheits-Risikomanagement in der Lieferkette, eine diesbezügliche Strategie, Ziele, Richtlinien und Prozesse sind etabliert und von den organisatorischen Stakeholdern akzeptiert.
- **GV.SC-02:** Cybersicherheits-Rollen und -Verantwortlichkeiten für Lieferanten, Kunden und Partner werden intern und extern festgelegt, kommuniziert und koordiniert.
- **GV.SC-03:** Das Cybersicherheits-Risikomanagement in der Lieferkette ist in die Prozesse für Cybersicherheit und Unternehmensrisikomanagement, Risikobewertung und -verbesserung integriert.
- **GV.SC-04:** Die Lieferanten sind bekannt und werden nach Kritikalität priorisiert.
- **GV.SC-05:** Anforderungen zur Bewältigung von Cybersicherheitsrisiken in Lieferketten werden festgelegt, priorisiert und in Verträge und andere Arten von Vereinbarungen mit Lieferanten und anderen relevanten Dritten integriert.
- **GV.SC-06:** Planung und Due-Diligence-Prüfung werden durchgeführt, um Risiken zu reduzieren, bevor formelle Beziehungen zu Lieferanten oder anderen Dritten eingegangen werden.
- **GV.SC-07:** Die Risiken, die von einem Lieferanten, seinen Produkten und Dienstleistungen sowie von anderen Dritten ausgehen, werden verstanden, aufgezeichnet, nach Prioritäten geordnet, bewertet, beantwortet und im Laufe der Geschäftsbeziehung überwacht.
- **GV.SC-08:** Relevante Lieferanten und andere Dritte werden in die Planung, Reaktion und Wiederherstellung von Vorfällen einbezogen.
- **GV.SC-09:** Sicherheitspraktiken in der Lieferkette sind in Programme zur Cybersicherheit und zum Risikomanagement im Unternehmen integriert, und ihre Leistung wird während des gesamten Lebenszyklus von Technologieprodukten und -dienstleistungen überwacht.
- **GV.SC-10:** Risikomanagementpläne für die Cybersicherheit in der Lieferkette enthalten Bestimmungen für Aktivitäten, die nach Abschluss einer Partnerschaft oder eines Dienstleistungsvertrags stattfinden.

IDENTIFIZIEREN (ID): Die aktuellen Cybersicherheitsrisiken der Organisation sind bekannt.

- **Vermögensverwaltung (ID.AM):** Vermögenswerte (z. B. Daten, Hardware, Software, Systeme, Einrichtungen, Dienstleistungen, Mitarbeiter), die es der Organisation ermöglichen, ihre Geschäftsziele zu erreichen, werden entsprechend ihrer relativen Bedeutung für die Organisationsziele und die Risikostrategie der Organisation identifiziert und verwaltet.
  - **ID.AM-01:** Inventare der von der Organisation verwalteten Hardware werden geführt.
  - **ID.AM-02:** Inventare der von der Organisation verwalteten Software, Dienste und Systeme werden geführt.

- **ID.AM-03:** Darstellungen der autorisierten Netzwerkkommunikation der Organisation sowie der internen und externen Netzwerkdatenflüsse werden gepflegt.
- **ID.AM-04:** Inventare der von Lieferanten erbrachten Dienstleistungen werden geführt.
- **ID.AM-05:** Priorisierung von Vermögenswerten auf der Grundlage von Klassifizierung, Kritikalität, Ressourcen und Auswirkungen auf den Organisationszweck.
- **ID.AM-07:** Inventare von Daten und entsprechenden Metadaten für bestimmte Datentypen werden gepflegt.
- **ID.AM-08:** Systeme, Hardware, Software, Dienste und Daten werden während ihres gesamten Lebenszyklus verwaltet.

- **Risikobewertung (ID.RA):** Die Organisation kennt das Cybersicherheitsrisiko für die Organisation, Vermögenswerte und Personen.
  - **ID.RA-01:** Schwachstellen in Anlagen werden identifiziert, validiert und aufgezeichnet.
  - **ID.RA-02:** Cyberbedrohungsinformationen werden von Foren und Quellen für den Informationsaustausch erhalten.
  - **ID.RA-03:** Interne und externe Bedrohungen für die Organisation sind identifiziert und erfasst.
  - **ID.RA-04:** Mögliche Auswirkungen und Wahrscheinlichkeiten von Bedrohungen, die Schwachstellen ausnutzen, werden ermittelt und aufgezeichnet.
  - **ID.RA-05:** Bedrohungen, Schwachstellen, Wahrscheinlichkeiten und Auswirkungen werden genutzt, um das inhärente Risiko zu verstehen und eine Priorisierung der Risikobewältigung vorzunehmen.
  - **ID.RA-06:** Risikobewältigungsmaßnahmen werden ausgewählt, nach Prioritäten geordnet, geplant, nachverfolgt und kommuniziert.
  - **ID.RA-07:** Änderungen und Ausnahmen werden verwaltet, auf Risikoauswirkungen geprüft, aufgezeichnet und nachverfolgt.
  - **ID.RA-08:** Prozesse für den Empfang, die Analyse und die Reaktion auf die Offenlegung von Schwachstellen sind eingerichtet.
  - **ID.RA-09:** Die Authentizität und Integrität von Hardware und Software wird vor dem Erwerb und der Nutzung geprüft.
  - **ID.RA-10:** Wesentliche Lieferanten werden vor dem Erwerb bewertet.

- **Verbesserung (ID.IM):** Verbesserungen der organisatorischen Prozesse, Verfahren und Aktivitäten des Cybersicherheitsrisikomanagements werden in allen CSF-Funktionen identifiziert.
  - **ID.IM-01:** Verbesserungen werden anhand von Bewertungen ermittelt.
  - **ID.IM-02:** Aus Sicherheitstests und -übungen, auch in Abstimmung mit Lieferanten und relevanten Dritten, werden Verbesserungen ermittelt.

- **ID.IM-03:** Bei der Durchführung von betrieblichen Prozessen, Verfahren und Aktivitäten werden Verbesserungen festgestellt.
- **ID.IM-04:** Pläne zur Reaktion auf Vorfälle und andere Cybersicherheitspläne, die sich auf den Betrieb auswirken, werden erstellt, kommuniziert, gepflegt und verbessert.

SCHÜTZEN (PR): Schutzmaßnahmen zum Management der Cybersicherheitsrisiken der Organisation werden eingesetzt.

- **Identitätsmanagement, Authentifizierung und Zugangskontrolle (PR.AA):** Der Zugang zu physischen und logischen Ressourcen ist auf autorisierte Benutzer, Dienste und Hardware beschränkt und wird entsprechend dem bewerteten Risiko eines unbefugten Zugangs verwaltet.
  - **PR.AA-01:** Identitäten und Berechtigungsnachweise für autorisierte Benutzer, Dienste und Hardware werden von der Organisation verwaltet.
  - **PR.AA-02:** Identitäten werden geprüft und an Berechtigungsnachweise gebunden, basierend auf dem Kontext der Interaktionen.
  - **PR.AA-03:** Benutzer, Dienste und Hardware sind authentifiziert.
  - **PR.AA-04:** Identitätsbestätigungen werden geschützt, übermittelt und überprüft.
  - **PR.AA-05:** Zugriffsberechtigungen, Berechtigungen und Autorisierungen werden in einer Richtlinie definiert, verwaltet, durchgesetzt und überprüft und berücksichtigen die Prinzipien der geringsten Rechte und der Aufgabentrennung.
  - **PR.AA-06:** Der physische Zugang zu Vermögenswerten wird risikoadäquat verwaltet, überwacht und durchgesetzt.
- **Sensibilisierung und Schulung (PR.AT):** Die Mitarbeiter der Organisation werden für die Cybersicherheit sensibilisiert und geschult, damit sie ihre Aufgaben im Bereich der Cybersicherheit wahrnehmen können.
  - **PR.AT-01:** Die Mitarbeiter werden sensibilisiert und geschult, so dass sie über die Kenntnisse und Fähigkeiten verfügen, um allgemeine Aufgaben unter Berücksichtigung von Cybersicherheitsrisiken auszuführen.
  - **PR.AT-02:** Personen in speziellen Funktionen werden sensibilisiert und geschult, so dass sie über das Wissen und die Fähigkeiten verfügen, relevante Aufgaben unter Berücksichtigung von Cybersicherheitsrisiken auszuführen.
- **Datensicherheit (PR.DS):** Daten werden im Einklang mit der Risikostrategie der Organisation verwaltet, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen.
  - **PR.DS-01:** Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten im Ruhezustand sind geschützt.

- **PR.DS-02:** Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bei der Übermittlung sind geschützt.
- **PR.DS-10:** Die Vertraulichkeit, Integrität und Verfügbarkeit von Daten bei der Verwendung sind geschützt.
- **PR.DS-11:** Backups von Daten werden erstellt, geschützt, gepflegt und getestet.

- **Plattformsicherheit (PR.PS):** Software (z. B. Firmware, Betriebssysteme, Anwendungen) und Dienste physischer und virtueller Plattformen werden im Einklang mit der Risikostrategie der Organisation verwaltet, um ihre Vertraulichkeit, Integrität und Verfügbarkeit zu schützen.
  - **PR.PS-01:** Praktiken des Konfigurationsmanagements sind eingeführt und werden angewendet.
  - **PR.PS-02:** Die Software wird entsprechend dem Risiko gewartet, ersetzt und entfernt.
  - **PR.PS-03:** Hardware wird entsprechend dem Risiko gewartet, ersetzt und entfernt.
  - **PR.PS-04:** Log-Protokolle werden erstellt und für die kontinuierliche Überwachung zur Verfügung gestellt.
  - **PR.PS-05:** Installation und Ausführung nicht autorisierter Software wird verhindert.
  - **PR.PS-06:** Sichere Softwareentwicklungspraktiken sind integriert, und ihre Leistung wird während des gesamten Softwareentwicklungszyklus überwacht.

- **Widerstandsfähigkeit der Technologie-Infrastruktur (PR.IR):** Daten werden im Einklang mit der Risikostrategie der Organisation verwaltet, um die Vertraulichkeit, Integrität und Verfügbarkeit von Vermögenswerten sowie die Widerstandsfähigkeit der Organisation zu schützen.
  - **PR.IR-01:** Netzwerke und Umgebungen sind vor unbefugtem logischen Zugriff und unbefugter Nutzung geschützt.
  - **PR.IR-02:** Die technischen Anlagen der Organisation sind vor Umweltbedrohungen geschützt.
  - **PR.IR-03:** Es sind Mechanismen implementiert, um die Anforderungen an die Widerstandsfähigkeit in normalen und ungünstigen Situationen zu erfüllen.
  - **PR.IR-04:** Eine angemessene Ressourcenkapazität zur Gewährleistung der Verfügbarkeit wird aufrechterhalten.

ERKENNEN (DE): Mögliche Cybersicherheitsangriffe und -kompromittierungen werden erkannt und analysiert.

- **Kontinuierliche Überwachung (DE.CM):** Vermögenswerte werden überwacht, um Anomalien, Indikatoren für Kompromittierung und andere potenziell unerwünschte Ereignisse zu finden.

- **DE.CM-01:** Netzwerke und Netzwerkdienste werden überwacht, um potenziell unerwünschte Ereignisse zu erkennen.
- **DE.CM-02:** Die physische Umgebung wird überwacht, um potenziell unerwünschte Ereignisse zu finden.
- **DE.CM-03:** Die Aktivitäten des Personals und die Nutzung der Technologie werden überwacht, um potenziell unerwünschte Ereignisse zu erkennen.
- **DE.CM-06:** Aktivitäten und Dienstleistungen externer Dienstleister werden überwacht, um potenziell unerwünschte Ereignisse zu erkennen.
- **DE.CM-09:** Computerhardware und -software, Laufzeitumgebungen und deren Daten werden überwacht, um potenziell unerwünschte Ereignisse zu finden.

- **Analyse unerwünschter Ereignisse (DE.AE):** Anomalien, Indikatoren für eine Kompromittierung und andere potenziell unerwünschte Ereignisse werden analysiert, um die Ereignisse zu charakterisieren und Cybersicherheitsvorfälle zu erkennen.
  - **DE.AE-02:** Potenziell unerwünschte Ereignisse werden analysiert, um die damit verbundenen Aktivitäten besser zu verstehen.
  - **DE.AE-03:** Informationen aus verschiedenen Quellen werden miteinander in Beziehung gesetzt.
  - **DE.AE-04:** Die geschätzten Auswirkungen und das Ausmaß von unerwünschten Ereignissen sind bekannt.
  - **DE.AE-06:** Informationen über unerwünschte Ereignisse werden dem befugten Personal und den Hilfsmitteln zur Verfügung gestellt.
  - **DE.AE-07:** Cyber-Bedrohungsdaten und andere kontextbezogene Informationen werden in die Analyse integriert.
  - **DE.AE-08:** Zwischenfälle werden gemeldet, wenn unerwünschte Ereignisse die definierten Kriterien für Zwischenfälle erfüllen.

REAGIEREN (RS): Es werden Maßnahmen in Bezug auf einen erkannten Cybersicherheitsvorfall ergriffen.

- **Management von Vorfällen (RS.MA):** Reaktionen auf erkannte Cybersicherheitsvorfälle werden verwaltet.
  - **RS.MA-01:** Der Plan für die Reaktion auf einen Vorfall wird in Abstimmung mit den relevanten Dritten ausgeführt, sobald ein Vorfall gemeldet wird.
  - **RS.MA-02:** Berichte über Vorfälle werden sortiert und validiert.
  - **RS.MA-03:** Vorfälle werden kategorisiert und nach Prioritäten geordnet.
  - **RS.MA-04:** Vorfälle werden je nach Bedarf eskaliert oder ausgeweitet.

- **RS.MA-05:** Die Kriterien für die Einleitung der Wiederherstellung eines Vorfalls werden angewendet.

- **Analyse von Vorfällen (RS.AN):** Untersuchungen werden durchgeführt, um eine wirksame Reaktion zu gewährleisten und Forensik- und Wiederherstellungsaktivitäten zu unterstützen.
  - **RS.AN-03:** Es wird eine Analyse durchgeführt, um festzustellen, was während eines Vorfalls geschehen ist und was die Ursache für den Vorfall war.
  - **RS.AN-06:** Die während einer Untersuchung durchgeführten Maßnahmen werden aufgezeichnet, und die Integrität und Herkunft der Aufzeichnungen wird gewahrt.
  - **RS.AN-07:** Daten und Metadaten von Vorfällen werden gesammelt und ihre Integrität und Herkunft wird bewahrt.
  - **RS.AN-08:** Das Ausmaß eines Vorfalls wird geschätzt und validiert.

- **Berichterstattung und Kommunikation bei Vorfällen (RS.CO):** Reaktionsmaßnahmen werden mit internen und externen Stakeholdern koordiniert, wie es die Gesetze, Vorschriften oder Richtlinien vorschreiben.
  - **RS.CO-02:** Interne und externe Stakeholdern werden über Vorfälle informiert.
  - **RS.CO-03:** Informationen werden mit bestimmten internen und externen Stakeholdern geteilt.

- **Entschärfung von Vorfällen (RS.MI):** Aktivitäten werden durchgeführt, um die Ausbreitung eines Vorfalls zu verhindern und seine Auswirkungen abzuschwächen.
  - **RS.MI-01:** Vorfälle werden eingedämmt.
  - **RS.MI-02:** Vorfälle werden ausgemerzt.

WIEDERHERSTELLEN (RC): Von einem Cybersicherheitvorfall betroffene Anlagen und Abläufe werden wiederhergestellt.

- **Ausführung des Vorfall-Wiederherstellungsplans (RC.RP):** Es werden Wiederherstellungsmaßnahmen durchgeführt, um die betriebliche Verfügbarkeit von Systemen und Diensten zu gewährleisten, die von Cybersicherheitsvorfällen betroffen sind.
  - **RC.RP-01:** Der Wiederherstellungsteil des Vorfallsreaktionsplans wird ausgeführt, sobald er vom Vorfallsreaktionsprozess initiiert wurde.
  - **RC.RP-02:** Wiederherstellungsmaßnahmen werden ausgewählt, eingegrenzt, nach Prioritäten geordnet und durchgeführt.
  - **RC.RP-03:** Die Integrität von Backups und anderen Wiederherstellungs-Assets wird überprüft, bevor sie für die Wiederherstellung verwendet werden.

- **RC.RP-04:** Für den Organisationszweck wesentliche Funktionen und Cybersicherheitsrisikomanagement werden bei der Festlegung von Betriebsnormen für die Zeit nach einem Vorfall berücksichtigt.
- **RC.RP-05:** Die Integrität der wiederhergestellten Anlagen wird überprüft, Systeme und Dienste werden wiederhergestellt und der normale Betriebszustand wird bestätigt.
- **RC.RP-06:** Das Ende der Wiederherstellung des Vorfalls wird auf der Grundlage von Kriterien erklärt, und die Dokumentation des Vorfalls wird abgeschlossen.

- **Kommunikation zur Vorfall-Wiederherstellung (RC.CO):** Die Wiederherstellungsaktivitäten werden mit internen und externen Parteien koordiniert.
  - **RC.CO-03:** Die Wiederherstellungsmaßnahmen und die Fortschritte bei der Wiederherstellung der Betriebsfähigkeit werden den benannten internen und externen Stakeholdern mitgeteilt.
  - **RC.CO-04:** Die Öffentlichkeit wird über die Wiederherstellung von Vorfällen mit Hilfe genehmigter Methoden und Nachrichten informiert.

Anhang B. CSF-Ebenen

Tabelle 2 enthält eine fiktive Illustration der in Abschnitt 3 erörterten CSF-Ebenen. Die Ebenen charakterisieren die Strenge der Verfahren einer Organisation zur Steuerung von Cybersicherheitsrisiken (GOVERNANCE) und zum Management von Cybersicherheitsrisiken (IDENTIFIZIEREN, SCHÜTZEN, ERKENNEN, REAGIEREN und WIEDERHERSTELLEN).

Tabelle 2. Fiktive Illustration der CSF-Ebenen

Ebene	Governance des Cybersicherheitsrisikomanagements	Cybersicherheitsrisikomanagement
Ebene 1: teilweise	Die Anwendung der organisatorischen Strategie für Cybersicherheitsrisiken wird ad hoc verwaltet. Die Prioritätensetzung erfolgt ad hoc und basiert nicht formell auf den Zielen oder der Bedrohungslage.	Das Bewusstsein für Cybersicherheitsrisiken ist auf organisatorischer Ebene nur begrenzt vorhanden. Die Organisation setzt das Cybersicherheitsrisikomanagement in unregelmäßigen Abständen und von Fall zu Fall um. Die Organisation verfügt möglicherweise nicht über Prozesse, die den Austausch von Cybersicherheitsinformationen innerhalb der Organisation ermöglichen. Die Organisation ist sich im Allgemeinen nicht der Cybersicherheitsrisiken bewusst, die mit ihren Lieferanten und den von ihr erworbenen und genutzten Produkten und Dienstleistungen verbunden sind.
Ebene 2: risikoinformiert	Risikomanagementpraktiken werden von der Geschäftsleitung genehmigt, werdenaber möglicherweise nicht als organisationsweite Richtlinie festgelegt. Die Priorisierung der Cybersicherheitsaktivitäten und des Schutzbedarfs richtet sich direkt nach den Risikozielen des Unternehmens, dem Bedrohungsumfeld oder den Anforderungen des Unternehmens bzw. dem Unternehmenszweck.	Das Bewusstsein für Cybersicherheitsrisiken ist auf organisatorischer Ebene vorhanden, aber ein unternehmensweiter Ansatz für das Management von Cybersicherheitsrisiken wurde nicht eingeführt. Die Berücksichtigung der Cybersicherheit bei organisatorischen Zielen und Programmen erfolgt möglicherweise auf einigen, aber nicht auf allen Ebenen der Organisation. Cyber-Risikobewertungen von organisatorischen und externen Vermögenswerten finden statt, sind aber in der Regel nicht wiederholbar oder nicht wiederkehrend. Informationen zur Cybersicherheit werden innerhalb der Organisation auf informeller Basis ausgetauscht. Die Organisation ist sich der Cybersicherheitsrisiken bewusst, die mit ihren Zulieferern und den Produkten und Dienstleistungen, die sie erwirbt und nutzt, verbunden sind, aber sie reagiert nicht konsequent oder formell auf diese Risiken.

Ebene	Governance des Cybersicherheitsrisikomanagements	Cybersicherheitsrisikomanagement
Ebene 3: wiederholbar	Die Risikomanagement-Praktiken der Organisation werden formell genehmigt und als Richtlinie festgelegt. Risikobasierte Richtlinien, Prozesse und Verfahren werden definiert, wie vorgesehen umgesetzt und überprüft. Organisationsweite Cybersicherheitspraktiken werden regelmäßig auf der Grundlage der Anwendung von Risikomanagementprozessen auf Änderungen der Geschäfts-/Auftragsanforderungen, Bedrohungen und der technologischen Landschaft aktualisiert.	Es gibt einen organisationsweiten Ansatz für das Management von Cybersicherheitsrisiken. Informationen zur Cybersicherheit werden routinemäßig in der gesamten Organisation ausgetauscht. Es gibt einheitliche Methoden, um wirksam auf Veränderungen der Risiken zu reagieren. Die Mitarbeiter verfügen über das Wissen und die Fähigkeiten, um die ihnen übertragenen Aufgaben und Verantwortlichkeiten zu erfüllen. Die Organisation überwacht konsequent und genau die Cybersicherheitsrisiken von Anlagen. Leitende Angestellte im Bereich Cybersicherheit und andere Führungskräfte kommunizieren regelmäßig über Cybersicherheitsrisiken. Die Führungskräfte stellen sicher, dass die Cybersicherheit in allen Geschäftsbereichen des Unternehmens berücksichtigt wird. Die Risikostrategie des Unternehmens basiert auf den Cybersicherheitsrisiken, die mit den Zulieferern und den Produkten und Dienstleistungen, die es erwirbt und nutzt, verbunden sind. Die Mitarbeiter gehen formell auf diese Risiken ein, indem sie Mechanismen wie schriftliche Vereinbarungen zur Kommunikation der grundlegenden Anforderungen, Governance-Strukturen (z. B. Risikoräte) sowie die Umsetzung und Überwachung von Richtlinien nutzen. Diese Maßnahmen werden konsequent und wie vorgesehen umgesetzt und kontinuierlich überwacht und überprüft.

Ebene	Governance des Cybersicherheitsrisikomanagements	Cybersicherheitsrisikomanagement
Ebene 4: anpassungsfähig	Es gibt einen organisationsweiten Ansatz für das Management von Cybersicherheitsrisiken, der risikobasierte Richtlinien, Prozesse und Verfahren verwendet, um potenzielle Cybersicherheitsereignisse anzugehen. Die Beziehung zwischen Cybersicherheitsrisiken und Unternehmenszielen wird klar verstanden und bei der Entscheidungsfindung berücksichtigt. Führungskräfte überwachen Cybersicherheitsrisiken im gleichen Kontext wie finanzielle und andere organisatorische Risiken. Das Organisationsbudget basiert auf einem Verständnis des aktuellen und prognostizierten Risikoumfelds und der Risikotoleranz. Die Geschäftseinheiten setzen die Vision der Geschäftsleitung um und analysieren die Risiken auf Systemebene im Rahmen der Risikotoleranz der Organisation. Das Cybersicherheitsrisikomanagement ist Teil der Organisationskultur. Es entwickelt sich aus dem Bewusstsein früherer Aktivitäten und dem kontinuierlichen Bewusstsein für die Aktivitäten in den Systemen und Netzwerken der Organisation. Die Organisation kann Änderungen der Geschäfts-/Missionsziele schnell und effizient berücksichtigen, wenn es darum geht, wie Risiken angegangen und kommuniziert werden.	Die Organisation passt ihre Cybersicherheitspraktiken auf der Grundlage früherer und aktueller Cybersicherheitsaktivitäten an, einschließlich der gewonnenen Erkenntnisse und prädiktiver Indikatoren. Durch einen kontinuierlichen Verbesserungsprozess, der fortschrittliche Cybersicherheitstechnologien und -praktiken einbezieht, passt sich die Organisation aktiv an eine sich verändernde technologische Landschaft an und reagiert rechtzeitig und effektiv auf sich entwickelnde, hochentwickelte Bedrohungen. Die Organisation nutzt Echtzeit- oder echtzeitnahe Informationen, um die mit ihren Lieferanten und den von ihr erworbenen und genutzten Produkten und Dienstleistungen verbundenen Cybersicherheitsrisiken zu verstehen und konsequent darauf zu reagieren. Cybersicherheitsinformationen werden ständig innerhalb des Unternehmens und mit autorisierten Dritten ausgetauscht.

Anhang C. Glossar

CSF-Kategorie
Eine Gruppe von zusammenhängenden Cybersicherheitsergebnissen, die zusammen eine CSF-Funktion bilden.

CSF-Gemeinschaftsprofil
Eine Basis von CSF-Ergebnissen, die erstellt und veröffentlicht wird, um gemeinsame Interessen und Ziele einer Reihe von Organisationen zu berücksichtigen. Ein Gemeinschaftsprofil wird in der Regel für einen bestimmten Sektor, Teilsektor, eine bestimmte Technologie, eine bestimmte Bedrohungsart oder einen anderen Anwendungsfall entwickelt. Eine Organisation kann ein Gemeinschaftsprofil als Grundlage für ihr eigenes Zielprofil verwenden.

CSF-Kern
Eine Taxonomie übergeordneter Ergebnisse der Cybersicherheit, die jeder Organisation bei der Verwaltung ihrer Cybersicherheitsrisiken helfen kann. Ihre Komponenten sind eine Hierarchie von Funktionen, Kategorien und Unterkategorien, die jedes Ergebnis detailliert beschreiben.

aktuelles CSF-Profil
Ein Teil eines Organisationsprofils, der die Hauptergebnisse angibt, die eine Organisation derzeit erreicht (oder zu erreichen versucht), und beschreibt, wie oder in welchem Ausmaß die einzelnen Ergebnisse erreicht werden.

CSF-Funktion
Die höchste Organisationsebene für Cybersicherheitsergebnisse. Es gibt sechs CSF-Funktionen: Governance, Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen.

Beispiel für die CSF-Umsetzung
Eine prägnante, handlungsorientierte, fiktive Illustration eines Weges, der zum Erreichen eines CSF-Kernergebnisses beiträgt.

Informative CSF-Referenz
Eine Zuordnung, die eine Beziehung zwischen einem CSF-Kernergebnis und einer bestehenden Norm, Richtlinie, Vorschrift oder einem anderen Inhalt angibt.

Organisatorisches CSF-Profil
Ein Mechanismus zur Beschreibung der aktuellen und/oder angestrebten Cybersicherheitslage einer Organisation in Bezug auf die Ergebnisse des CSF-Kerns.

CSF-Kurzanleitung
Eine zusätzliche Ressource, die kurze, umsetzbare Anleitungen zu spezifischen CSF-bezogenen Themen enthält.

CSF-Unterkategorie
Eine Gruppe spezifischerer Ergebnisse von technischen und verwaltungstechnischen Cybersicherheitsaktivitäten, die eine CSF-Kategorie bilden.

CSF-Zielprofil
Ein Teil eines Organisationsprofils, der die gewünschten Hauptergebnisse spezifiziert, die eine Organisation ausgewählt und priorisiert hat, um ihre Ziele im Bereich des Cybersicherheitsrisikomanagements zu erreichen.

CSF-Ebene
Eine Charakterisierung der Strenge der Cybersicherheitsrisiko-Governance und -Managementpraktiken einer Organisation. Es gibt vier Ebenen: teilweise (Ebene 1), risikoinformiert (Ebene 2), wiederholbar (Ebene 3) und anpassungsfähig (Ebene 4).

Bestimmte kommerzielle oder nichtkommerzielle Geräte, Instrumente, Software oder Materialien werden in diesem Dokument genannt, um das Versuchsverfahren angemessen zu beschreiben. Eine solche Kennzeichnung bedeutet weder eine Empfehlung oder Befürwortung eines Produkts oder einer Dienstleistung durch das NIST, noch bedeutet sie, dass die genannten Materialien oder Geräte notwendigerweise die besten für den jeweiligen Zweck sind.

NIST-Richtlinien für technische Serien
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Wie man diese Publikation der NIST Technical Series zitiert:
National Institute of Standards and Technology (2024) Das NIST-Cybersicherheits-Framework (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 ger. https://doi.org/10.6028/NIST.CSWP.29.ger

Kontaktinformation
cyberframework@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Alle Kommentare können gemäß dem Freedom of Information Act (FOIA) veröffentlicht werden.