RESOURCE CENTER

Was ist das NIST Cybersecurity Framework? Der ultimative Leitfaden

Get the full interactive view at
https://bitwarden.com/de-de/resources/nist-cybersecurity-framework/

bitwarden

Geschichte von NIST

Das National Institute of Standards and Technology (NIST) bietet Unternehmen Leitlinien und bewährte Verfahren, um Unternehmen, gemeinnützige Organisationen und andere private Institutionen bei der Verbesserung des Risikomanagements für Cybersicherheit zu unterstützen. NIST ist Teil des US-Handelsministeriums und eines der ältesten (physikalischen) Wissenschaftslabors des Landes.

Im Jahr 2013 erließ der Präsident die Executive Order 13636, in der es heißt:

> **"Es ist die Politik der Vereinigten Staaten, die Sicherheit und Widerstandsfähigkeit der kritischen Infrastruktur der Nation zu verbessern und eine Cyber-Umgebung aufrechtzuerhalten, die Effizienz, Innovation und wirtschaftlichen Wohlstand fördert und gleichzeitig Sicherheit, Sicherheit, Geschäftsgeheimnis, Privatsphäre und bürgerliche Freiheiten fördert."**

Diese Executive Order legte bestimmte Anforderungen fest, die NIST an ihren Cybersicherheitsrahmen anwandte, darunter:

- Identifizieren Sie Sicherheitsstandards und -richtlinien, die für alle Bereiche der kritischen Infrastruktur gelten.
- Bieten Sie einen priorisierten, flexiblen, wiederholbaren, leistungsbasierten und kosteneffektiven Ansatz.
- Unterstützung von Eigentümern und Betreibern kritischer Infrastrukturen bei der Identifizierung, Bewertung und Verwaltung von Cyberrisiken.
- Ermöglichen Sie technische Innovationen und berücksichtigen Sie organisatorische Unterschiede.
- Bereitstellung von Leitlinien, die technologieneutral sind und es Sektoren kritischer Infrastrukturen ermöglichen, von einem wettbewerbsintensiven Markt für Produkte und Dienstleistungen zu profitieren.
- Fügen Sie eine Anleitung zur Messung der Leistung der Implementierung des Cybersicherheits-Frameworks hinzu.
- Identifizieren Sie Bereiche für Verbesserungen, die durch zukünftige Zusammenarbeit mit bestimmten Sektoren und Organisationen, die Standards entwickeln, angegangen werden sollten.

Warum ist das so wichtig geworden?

Einfach ausgedrückt, betreffen zunehmende Cybersicherheitsbedrohungen Unternehmen und andere Organisationen täglich. Ohne eine einzige Quelle der Wahrheit wäre es für Unternehmen fast unmöglich, einen gründlichen, effektiven Rahmen zu entwickeln, der ihnen hilft, wirksame Maßnahmen zur Minderung von Sicherheitsrisiken umzusetzen. Aus diesem Grund ist das NIST Cybersecurity Framework für Unternehmen so wichtig geworden; es fördert effiziente, innovative und belastbare Lösungen zur Aufrechterhaltung der Sicherheit.

Inhaltsverzeichnis

Was ist das NIST Cybersecurity Framework?

Im Wesentlichen hilft das NIST Cybersecurity Framework Organisationen aller Art, Cybersicherheitsrisiken besser zu verstehen, zu verwalten und zu reduzieren. Das Endergebnis der Befolgung dieser Anleitung ist ein besserer Schutz von Netzwerken und Daten. Das NIST Cybersecurity Framework ist so unterteilt, dass jedes Unternehmen oder jede Organisation es implementieren könnte, um besser zu verstehen, wo Zeit und Ressourcen für einen verbesserten Cybersicherheitsschutz konzentriert werden müssen. Es geht darum, Unternehmen zu befähigen, ihre Daten, die Daten ihrer Kunden, ihre Netzwerke und ihre Mitarbeiter effektiver zu schützen.

Obwohl das NIST Cybersecurity Framework von einer Organisation in den Vereinigten Staaten entwickelt wurde, wurde es mit der Idee der globalen Einführung geschaffen. Zu diesem Zweck wurde es in viele Sprachen übersetzt und von Regierungen, Unternehmen und Organisationen auf der ganzen Welt übernommen.

Seit NIST Cybersecurity Framework 1.1 haben viele Organisationen und Regierungen das Framework erfolgreich übernommen, darunter:

- Saudi Aramco
- Regierung von Bermuda
- Israelische Nationale Cyber-Direktion
- Cimpress-FAIR
- Multi-State - Informationsaustausch- und Analysezentrum
- University of Kansas Medical Center
- University of Pittsburgh
- ISACA
- Japanisches branchenübergreifendes Forum
- University of Chicago
- Lower Colorado River Authority
- Optische Cyber-Lösungen

Die neueste Version des NIST Cybersecurity Framework (CSF) richtet sich an Zielgruppen, Branchen und Organisationen aller Art und Größe; von kleinen Schulen und gemeinnützigen Organisationen bis hin zu Unternehmen. Das Framework wurde so konzipiert, dass jedes Unternehmen, unabhängig von der Komplexität der Cybersicherheit, von den von ihm bereitgestellten Informationen profitieren kann.

Laut Laurie E. Locascio, NIST-Direktorin und Staatssekretärin im Handelsministerium für Standards und Technologie:

> „Das CSF war für viele Unternehmen ein wichtiges Instrument, um Bedrohungen der Cybersicherheit zu antizipieren und damit umzugehen... Bei CSF 2.0, das auf früheren Versionen aufbaut, geht es nicht nur um ein Dokument. Es geht um eine Reihe von Ressourcen, die individuell angepasst und im Laufe der Zeit oder in Kombination verwendet werden können, wenn sich die Cybersicherheitsanforderungen eines Unternehmens ändern und sich seine Fähigkeiten weiterentwickeln."

Erkundung der Geschichte des NIST Cybersecurity Frameworks

Die neueste Entwicklung des NIST Cybersecurity Framework geht auch über die Konzentration auf kritische Infrastrukturen hinaus und umfasst alle Organisationen (aller Größen) in jedem Sektor.

Als das NIST Cybersecurity Framework erstellt wurde, ging es darum, kontinuierlich mit Stakeholdern aus Regierung, Industrie und Wissenschaft zusammenzuarbeiten. Um diesen Rahmen zu schaffen, nutzte NIST landesweit Outreach und Workshops sowie ein Request For Information (RFI) und ein Request For Comment (RFC). Ihr ursprüngliches Ziel war dreifach:

- Identifizieren Sie bestehende Cybersicherheitsstandards, Richtlinien, Frameworks und Best Practices.
- Geben Sie Lücken mit hoher Priorität an.
- Entwickeln Sie Aktionspläne, um diese Lücken zu schließen.

Die Kommentierungsfrist für die Informationsbeschaffung endete am 8. April 2013, und NIST erhielt über 270 Antworten auf die Informationsanfrage. Aus diesen Antworten entwickelte NIST die Agenda für ihren ersten Cybersecurity Framework-Workshop, der in Washington DC stattfand, mit dem Ziel, Interesse zu wecken, das Bewusstsein zu schärfen und Einblicke in den kollaborativen Entwicklungsprozess zu geben. Zu den Themen des Workshops gehörten die Executive Order, die Ziele für die Entwicklung und die Bekräftigung des Prozesses, der zur Entwicklung des Rahmens verwendet werden würde.

Der zweite Workshop fand vom 29. bis 31. Mai 2013 an der Carnegie Mellon University mit einer Agenda statt, die auf der Analyse der ersten RFI basierte. Ziel war es, die erhaltenen Informationen weiter zu definieren und zu klären und die Debatte über mehrere sicherheitsbezogene Themen anzuregen. Nach Abschluss dieses Workshops analysierte NIST die gesammelten Informationen und erstellte Zusammenfassungen, die mit den Branchen geteilt und zur Erstellung des ersten Entwurfs des Cybersecurity-Frameworks verwendet wurden.

Der erste Entwurf des NIST Cybersecurity Framework wurde am 2. Juli 2013 veröffentlicht.

NIST hielt nach der Veröffentlichung mehrere Workshops ab, die darauf abzielten, die erste Veröffentlichung zu diskutieren und zu verfeinern. Am 12. Februar 2014 wurde die Version 1.0 des NIST Cybersecurity Framework veröffentlicht.

Die Kernfunktionen des NIST Cybersecurity Frameworks

Das NIST Cybersecurity Framework besteht aus mehreren Kernfunktionen, die einen allgemeinen Überblick über die Best Practices geben. Diese Funktionen sollen nicht als Verfahrensschritte betrachtet werden, sondern vielmehr dazu dienen, die Dynamik von

Cybersicherheitsrisiken anzugehen.

Regieren

Diese Funktion liefert Ergebnisse, die darüber informieren, was eine Organisation tun kann, um die verbleibenden Funktionen im Kontext ihrer Mission und der Erwartungen der Stakeholder zu priorisieren.

Identifizieren

Die Identifizierungsfunktion fordert die Notwendigkeit, ein organisatorisches Verständnis der Cybersicherheitsrisiken für Systeme, Assets, Daten und Fähigkeiten zu entwickeln. Dieses Element konzentriert sich auf das Geschäft, so dass es seine Bemühungen in einer Weise priorisieren kann, die mit seiner Risikomanagementstrategie übereinstimmt.

Schützen

Diese Funktion unterstützt die Fähigkeit eines Unternehmens, Vermögenswerte zu sichern und die Wahrscheinlichkeit und die Auswirkungen eines Cybersicherheitsereignisses zu verhindern oder zu verringern.

Erkennen

Diese Funktion ermöglicht die rechtzeitige Erkennung und Analyse von Anomalien, Indikatoren für Kompromittierungen und anderen unerwünschten Ereignissen, die darauf hinweisen, dass ein Cybersicherheitsereignis eingetreten ist oder eintreten wird.

Antworten

Diese Funktion trägt dazu bei, alle Auswirkungen eines Cybersicherheitsvorfalls einzudämmen, einschließlich Vorfallsmanagement, Analyse, Schadensbegrenzung, Berichterstattung und Kommunikation.

Wiederherstellen

Diese Funktion konzentriert sich auf die rechtzeitige Wiederherstellung des normalen Geschäftsbetriebs, um die Auswirkungen eines Cybersicherheitsvorfalls zu reduzieren und die notwendige (und angemessene) Kommunikation während der Wiederherstellung zu ermöglichen.

Das ultimative Ziel dieser Funktionen ist es, einen strategischen Überblick darüber zu geben, wie sich ein Unternehmen auf Cybersicherheitsereignisse vorbereitet, darauf reagiert und sich davon erholt.

Implementierung des NIST Cybersecurity Frameworks

Mit einem soliden Verständnis dessen, was das NIST Cybersecurity Framework tut und wie es sich entwickelt hat, fragen Sie sich wahrscheinlich, wie Sie es am besten implementieren können.

NIST empfiehlt einen 7-stufigen Ansatz für die Implementierung, der wie folgt aussieht:

1. **Priorisierung und Umfang** – Priorisierung der Ziele und Ressourcen Ihres Unternehmens, die geschützt werden müssen.
2. **Orientieren** – Machen Sie sich und Ihr Team mit den Prozessen, Systemen und Komponenten im Geltungsbereich sowie den wichtigsten Compliance-Vorschriften vertraut, die sie einhalten müssen.
3. **Erstellen Sie ein aktuelles Profil** – Geben Sie an, welche Kontrollergebnisse des Frameworks bereits in Ihrer Organisation erreicht werden, und erstellen Sie dann eine Liste der noch zu integrierenden Elemente.
4. **Führen Sie eine Risikobewertung** durch – Analysieren Sie Ihre Betriebsumgebung, um die Wahrscheinlichkeit von Cybersicherheitsereignissen sowie deren Auswirkungen zu ermitteln.
5. **Erstellen Sie ein Zielprofil** – Konzentrieren Sie sich auf die Bewertung der Cybersicherheits-Framework-Kategorien und Unterkategorien, um Ihre gewünschten Cybersicherheitsergebnisse zu beschreiben.

6. **Lücken ermitteln, analysieren und priorisieren** - Bestimmen Sie alle Cybersicherheitslücken, die in Ihrem Unternehmen bestehen. Aus dieser Analyse können Sie dann einen priorisierten Plan erstellen, um diese Bedürfnisse zu erfüllen.

7. **Implementieren Sie Ihren Aktionsplan** - Ergreifen Sie Maßnahmen und implementieren Sie den von Ihnen erstellten Plan, um alle in den vorherigen Schritten festgestellten Probleme zu beheben.

Eine Sache, die man beachten sollte, ist, dass der Rahmen nicht unflexibel ist. Tatsächlich bietet das Framework genügend Flexibilität, um sich in Ihre bestehenden Sicherheitsprozesse zu integrieren. Sie sollten sehen, wie das innerhalb der oben aufgeführten sieben Schritte funktioniert.

Vorteile der Einführung des NIST Cybersecurity Frameworks

Aufgrund der Art und Weise, wie NIST die sieben Schritte zur Implementierung des Frameworks darlegt, erhalten Unternehmen einen umfassenden Überblick darüber, für welche Risiken sie anfällig sind, wie sie entsprechend diesen Risiken planen, wie sie die unternehmensweite Kommunikation verbessern und die Compliance stärken können. Die Aufklärung über die Schwächen einer Organisation und wie sie gemildert werden können, ist einer der entscheidenden Vorteile des NIST-Frameworks.

> Laut der Federal Trade Commission hilft das NIST-Framework "Unternehmen jeder Größe, ihr Cybersicherheitsrisiko besser zu verstehen, zu verwalten und zu reduzieren und ihre Netzwerke und Daten zu schützen."

NIST versteht, dass jede Organisation anders ist, und bietet sogar 3 Tipps, um Ihre Passwörter sicher zu halten (was als universell angesehen werden sollte).

Herausforderungen und Überlegungen bei der Rahmenübernahme

Das NIST Cybersecurity Framework kann komplex sein. Es ist wichtig, die Kernfunktionen vollständig zu verstehen, bevor Sie mit den oben aufgeführten sieben Schritten fortfahren können. Um einen dauerhaften Erfolg zu gewährleisten, ist es wichtig, eine Cybersicherheitskultur in Ihrem Unternehmen zu fördern. Andernfalls stoßen Sie auf Widerstand gegen eine möglicherweise dramatische Veränderung von Prozessen und Systemen.

Weitere Herausforderungen sind:

- Ressourcenbeschränkungen - Sie verfügen derzeit möglicherweise nicht über die Mitarbeiter, die in der Lage sind, diese Änderungen umzusetzen.
- Sie werden höchstwahrscheinlich Zeit damit verbringen müssen, das Cybersicherheits-Framework anzupassen, um es besser an Ihr Unternehmen anzupassen.
- Bedrohungen entwickeln sich ständig weiter, was bedeutet, dass Ihre Sicherheitspraktiken Schritt halten müssen.
- Sie sollten das Cybersecurity-Framework in alle vorhandenen Prozesse integrieren, die Sie eingerichtet haben.
- Es kann schwierig sein, die Einbindung von Stakeholdern zu fördern, was sich direkt auf die Förderung einer Cybersicherheitskultur bezieht, die in der Lage ist, diese Anforderungen zu erfüllen.

NIST Cybersecurity Framework Profile und Tiers

Es gibt vier NIST-Implementierungsebenen, nämlich:

- **Tier 1 Partial** - Unternehmen mit On-Demand- oder Zero-Security-Verfahren.
- **Tier-2-Risikoinformiert** - **Unternehmen**, die sich der Bedrohungen, denen sie ausgesetzt sind, bewusst sind und über einige Richtlinien verfügen, denen jedoch eine koordinierte Strategie fehlt.
- **Stufe 3 Wiederholbar** - Unternehmen mit Best Practices für Risikomanagement und Cybersicherheit, die die Genehmigung der Geschäftsleitung erhalten haben. Diese Unternehmen messen sich oft mit Wettbewerbern und arbeiten sogar mit anderen Organisationen zusammen, um sicherzustellen, dass ihre Praktiken aufeinander abgestimmt sind.
- **Tier 4 Adaptive** - Unternehmen in stark regulierten Branchen (wie Banken und Gesundheitswesen), die routinemäßig zu einem breiten Risikobewusstsein beitragen.

Laut NIST ist das Cybersecurity-Framework-Profil „die Ausrichtung der Funktionen, Kategorien und Unterkategorien an den Geschäftsanforderungen, der Risikotoleranz und den Ressourcen der Organisation“. Diese Profile helfen Unternehmen, eine Roadmap zur Reduzierung von Cybersicherheitsrisiken zu erstellen.

NIST bietet eine anpassbare Vorlage für Organisationsprofile des Cybersecurity-Frameworks sowie eine Liste von Community-Profilen, die verwendet werden können.

Aktualisierung und Weiterentwicklung mit dem NIST-Framework

Denken Sie daran, dass das NIST Cybersecurity Framework als lebendiges Dokument konzipiert ist, das von regelmäßigen Updates abhängt, die die sich ständig verändernde Landschaft der Cybersicherheit und aufkommende Bedrohungen widerspiegeln. Aus diesem Grund ist es wichtig, dass Unternehmen über die neuesten Bedrohungen auf dem Laufenden bleiben, damit sich das Cybersicherheits-Framework weiterentwickeln kann, um den aktuellen Anforderungen gerecht zu werden und sich kontinuierlich zu verbessern.

Um sicherzustellen, dass Ihr Unternehmen in der Lage ist, sich mit dem NIST Cybersecurity Framework weiterzuentwickeln, sollten Sie überlegen, wie Sie den besten Cybersecurity-Tech-Stack für Ihr Unternehmen aufbauen können, um sicherzustellen, dass Sie in der Lage sind, die beste Technologie zu nutzen, die sich mit dem Cybersecurity Framework weiterentwickeln kann.

Nutzung von Bitwarden für eine stärkere Cybersicherheit

Es sollte selbstverständlich sein, dass Sicherheit zu einem der wichtigsten Schwerpunktbereiche für Unternehmen geworden ist. Ohne robuste Cybersicherheitsrisikomanagementpraktiken könnten Unternehmen in freier Wildbahn einer beliebigen Anzahl von Bedrohungen zum Opfer fallen. Mit Hilfe des NIST Cybersecurity Frameworks und sorgfältiger Planung/Kommunikation könnte sich die Sicherheit Ihres Unternehmens erheblich verbessern. Gehen Sie das NIST Cybersecurity Framework gründlich an, befolgen Sie die 7 Schritte und seien Sie immer bereit, es zu aktualisieren und weiterzuentwickeln, damit Ihr Unternehmen besser vor Cybersicherheitsrisiken geschützt ist.

Sind Sie bereit, noch heute loszulegen? Erwägen Sie die Einführung einer Passwortverwaltungslösung, um Ihr Unternehmen auf den richtigen Weg zu bringen. Sehen Sie sich die Bitwarden Business-Tarife an, kontaktieren Sie den Vertrieb und vergleichen Sie die Tarife.