RESOURCE CENTER

Wat is het NIST Cybersecurity Framework? De ultieme gids

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

bitwarden

Geschiedenis van NIST

Het National Institute of Standards and Technology (NIST) biedt richtlijnen en best practices voor organisaties om bedrijven, non-profits en andere particuliere instellingen te helpen het risicobeheer voor cyberbeveiliging te verbeteren. NIST maakt deel uit van het Amerikaanse Ministerie van Handel en is een van de oudste (natuurkundige) wetenschapslaboratoria van het land.

In 2013 vaardigde de president Uitvoeringsbevel 13636 uit waarin stond:

> **"Het is het beleid van de Verenigde Staten om de veiligheid en veerkracht van de kritieke infrastructuur van de natie te verbeteren en een cyberomgeving te handhaven die efficiëntie, innovatie en economische welvaart aanmoedigt en tegelijkertijd de veiligheid, beveiliging, vertrouwelijkheid van zakelijke gegevens, privacy en burgerlijke vrijheden bevordert."**

Deze Executive Order stelde bepaalde vereisten vast die NIST toepaste op hun cyberbeveiligingsraamwerk, waaronder:

- Beveiligingsnormen en -richtlijnen identificeren die van toepassing zijn op alle sectoren van kritieke infrastructuur.
- Een geprioriteerde, flexibele, herhaalbare, prestatiegerichte en kosteneffectieve aanpak bieden.
- Eigenaren en beheerders van kritieke infrastructuur helpen bij het identificeren, beoordelen en beheren van cyberrisico's.
- Technische innovatie mogelijk maken en rekening houden met organisatorische verschillen.
- Bieden van begeleiding die technologieneutraal is en kritieke infrastructuursectoren in staat stelt te profiteren van een concurrerende markt voor producten en diensten.
- Richtlijnen opnemen voor het meten van de prestaties van de implementatie van het Cybersecurity Framework.
- Identificeer gebieden voor verbetering die moeten worden aangepakt door toekomstige samenwerking met bepaalde sectoren en organisaties die normen ontwikkelen.

Waarom is dit zo belangrijk geworden?

Simpel gezegd hebben bedrijven en andere organisaties dagelijks te maken met toenemende cyberbeveiligingsbedreigingen. Zonder één enkele bron van waarheid zou het voor bedrijven bijna onmogelijk zijn om een grondig, effectief raamwerk te ontwikkelen waarmee ze effectieve maatregelen kunnen implementeren om beveiligingsrisico's te beperken. Daarom is het NIST Cybersecurity Framework zo cruciaal geworden voor bedrijven; het moedigt efficiënte, innovatieve en veerkrachtige oplossingen aan om de beveiliging te handhaven.

Inhoudsopgave

Wat is het NIST Cybersecurity Framework?

Het NIST Cybersecurity Framework helpt organisaties van alle soorten om de risico's van cyberbeveiliging beter te begrijpen, te beheren en te verminderen. Het eindresultaat van het volgen van deze richtlijnen is een betere bescherming van netwerken en gegevens. Het NIST Cybersecurity Framework is zo opgesplitst dat elk bedrijf of organisatie het kan implementeren om beter te begrijpen waar tijd en middelen naartoe moeten voor een betere bescherming van de cyberbeveiliging. Het gaat erom bedrijven in staat te stellen hun gegevens, de gegevens van hun klanten, hun netwerken en hun werknemers effectiever te beschermen.

Hoewel het NIST Cybersecurity Framework is ontwikkeld door een organisatie in de Verenigde Staten, is het opgesteld met het idee van wereldwijde adoptie. Daarom is het in vele talen vertaald en overgenomen door overheden, bedrijven en organisaties over de hele wereld.

Sinds NIST Cybersecurity Framework 1.1 hebben veel organisaties en overheden het framework met succes overgenomen, waaronder:

- Saoedische Aramco
- Overheid van Bermuda
- Israëlisch Nationaal Cyberdirectoraat
- Cimpress-FAIR
- Multi-State - Centrum voor informatie-uitwisseling en analyse
- Universiteit van Kansas
- Universiteit van Pittsburgh
- ISACA
- Japans sectoroverschrijdend forum
- Universiteit van Chicago
- Autoriteit voor de rivier de Lower Colorado
- Optische Cyberoplossingen

De nieuwste versie van het NIST Cybersecurity Framework (CSF) is gericht op doelgroepen, industriesectoren en organisaties van alle soorten en maten; van kleine scholen en non-profitorganisaties tot grote ondernemingen. Het raamwerk is zo ontworpen dat elke

organisatie, ongeacht de mate van geavanceerdheid op het gebied van cyberbeveiliging, kan profiteren van de informatie die het biedt.

Volgens NIST-directeur en Under Secretary of Commerce for Standards and Technology, Laurie E. Locascio:

> "Het CSF is voor veel organisaties een essentieel hulpmiddel geweest om te anticiperen op en om te gaan met cyberbeveiligingsbedreigingen... CSF 2.0, dat voortbouwt op eerdere versies, gaat niet alleen over één document. Het gaat om een pakket hulpmiddelen dat kan worden aangepast en individueel of in combinatie kan worden gebruikt naarmate de behoeften van een organisatie op het gebied van cyberbeveiliging veranderen en de mogelijkheden van de organisatie zich ontwikkelen."

De geschiedenis van het NIST Cybersecurity Framework verkennen

De nieuwste evolutie van het NIST Cybersecurity Framework richt zich niet alleen op kritieke infrastructuur, maar op alle organisaties (van elke omvang) binnen elke sector.

Toen het NIST Cybersecurity Framework werd gemaakt, ging het om een voortdurende betrokkenheid bij belanghebbenden in de overheid, het bedrijfsleven en de academische wereld. Om dit raamwerk te creëren heeft NIST gebruik gemaakt van outreach en workshops in het hele land, evenals een Request For Information (RFI) en een Request For Comment (RFC). Hun oorspronkelijke doel was drieledig:

- Bestaande cyberbeveiligingsstandaarden, richtlijnen, raamwerken en best practices identificeren.
- Geef hiaten met hoge prioriteit op.
- Actieplannen ontwikkelen om deze lacunes aan te pakken.

De commentaarperiode voor het verzamelen van informatie eindigde op 8 april 2013 en NIST ontving meer dan 270 reacties op het verzoek om informatie. Op basis van deze reacties ontwikkelde NIST de agenda voor de eerste workshop over het Cybersecurity Framework, die plaatsvond in Washington DC met als doel belangstelling te wekken, het bewustzijn te vergroten en inzicht te verschaffen in het gezamenlijke ontwikkelingsproces. De onderwerpen van de workshop waren onder andere het Executive Order, de doelen voor de ontwikkeling en het herbevestigen van het proces dat gebruikt zou worden om het raamwerk te ontwikkelen.

De tweede workshop vond plaats tussen 29 en 31 mei 2013 en werd gehouden aan de Carnegie Mellon University met een agenda die gebaseerd was op de analyse van de eerste RFI. Het doel was om de informatie die ze hadden ontvangen verder te definiëren en te verduidelijken en om het debat over verschillende veiligheidsonderwerpen aan te moedigen. Na afloop van deze workshop analyseerde NIST de verzamelde informatie en maakte samenvattingen die werden gedeeld met de industrieën en werden gebruikt om het eerste concept van het Cybersecurity Framework op te stellen.

Het eerste ontwerp van het NIST Cybersecurity Framework werd uitgebracht op 2 juli 2013.

NIST heeft na de publicatie verschillende workshops gehouden om de oorspronkelijke publicatie te bespreken en te verfijnen. Op 12 februari 2014 werd versie 1.0 van het NIST Cybersecurity Framework uitgebracht.

De kernfuncties van het NIST Cybersecurity Framework

Het NIST Cybersecurity Framework bestaat uit verschillende kernfuncties, die een algemeen overzicht geven van de best practices. Deze functies zijn niet bedoeld als procedurele stappen, maar worden gebruikt om de dynamische aard van cyberbeveiligingsrisico's aan te pakken.

Regeren

Deze functie levert resultaten op die helpen informeren over wat een organisatie kan doen om de overige functies prioriteit te geven in de context van haar missie en de verwachtingen van belanghebbenden.

Identificeer

De identificatiefunctie doet een beroep op de noodzaak om een organisatorisch inzicht te ontwikkelen in de risico's van cyberbeveiliging voor systemen, bedrijfsmiddelen, gegevens en capaciteiten. Dit element richt zich op het bedrijf, zodat het zijn inspanningen kan prioriteren op een manier die consistent is met zijn risicomanagementstrategie.

Bescherm

Deze functie ondersteunt het vermogen van een organisatie om bedrijfsmiddelen te beveiligen en de kans op en de impact van een cyberbeveiligingsgebeurtenis te voorkomen of te verkleinen.

opsporen

Deze functie maakt de tijdige ontdekking en analyse mogelijk van anomalieën, compromisindicatoren en andere ongunstige gebeurtenissen die erop wijzen dat er een cyberbeveiligingsgebeurtenis heeft plaatsgevonden of zal plaatsvinden.

Reageer op

Deze functie helpt de gevolgen van een cyberbeveiligingsincident te beperken en omvat incidentbeheer, analyse, beperking, rapportage en communicatie.

Herstel

Deze functie richt zich op het tijdig herstellen van de normale bedrijfsactiviteiten om de gevolgen van een cyberbeveiligingsincident te beperken en de noodzakelijke (en gepaste) communicatie tijdens het herstel mogelijk te maken.

Het uiteindelijke doel van deze functies is om een strategisch overzicht op hoog niveau te bieden van hoe een organisatie zich voorbereidt op, reageert op en herstelt van cyberbeveiligingsgebeurtenissen.

Het NIST-cyberbeveiligingsraamwerk implementeren

Nu je goed weet wat het NIST Cybersecurity Framework doet en hoe het zich heeft ontwikkeld, vraag je je waarschijnlijk af hoe je het het beste kunt implementeren.

NIST beveelt een 7-stappen aanpak aan voor implementatie, die er als volgt uitziet:

1. **Stel prioriteiten en bereik** - Stel prioriteiten bij de doelstellingen en bedrijfsmiddelen van uw organisatie die moeten worden beschermd.

2. **Oriënteren** - Maak jezelf en je team vertrouwd met de processen, systemen en componenten binnen het toepassingsgebied, evenals met de belangrijkste compliance-regels waaraan ze zich moeten houden.

3. **Maak een huidig profiel** - Geef aan welke controle-uitkomsten van het raamwerk al worden bereikt binnen uw organisatie, en maak vervolgens een lijst van wat nog moet worden geïntegreerd.

4. **Voer een risicobeoordeling uit** - Analyseer uw operationele omgeving om de waarschijnlijkheid van cyberbeveiligingsgebeurtenissen te bepalen, evenals de impact die ze kunnen hebben.

5. **Maak een doelprofiel** - Richt u op de beoordeling van de categorieën en subcategorieën van het Cybersecurity Framework om uw gewenste cyberbeveiligingsresultaten te helpen beschrijven.

6. **Hiaten bepalen, analyseren en prioriteren** - Bepaal de hiaten in uw organisatie op het gebied van cyberbeveiliging. Op basis van deze analyse kun je vervolgens een geprioriteerd plan opstellen om deze behoeften aan te pakken.

7. **Implementeer je actieplan** - Onderneem actie en implementeer het plan dat je hebt gemaakt om alle problemen aan te pakken die in de vorige stappen zijn ontdekt.

Een ding om in gedachten te houden is dat het raamwerk niet inflexibel is. In feite biedt het framework genoeg flexibiliteit om te integreren met je bestaande beveiligingsprocessen. Je zou moeten zien hoe dat werkt binnen de zeven stappen die hierboven zijn opgesomd.

Voordelen van het aannemen van het NIST Cybersecurity Framework

Door de manier waarop NIST de zeven stappen voor het implementeren van het raamwerk uiteenzet, krijgen organisaties een uitgebreid overzicht van de risico's waar ze vatbaar voor zijn, hoe ze moeten plannen op basis van die risico's, hoe ze de communicatie binnen de hele organisatie kunnen verbeteren en de naleving kunnen versterken. De voorlichting over de zwakke punten van een organisatie en hoe deze te beperken, is een van de cruciale voordelen van het NIST Framework.

> Volgens de Federal Trade Commission"helpt het NIST Framework bedrijven van elke omvang om hun risico's op het gebied van cyberbeveiliging beter te begrijpen, te beheren en te beperken en hun netwerken en gegevens te beschermen".

NIST begrijpt dat elke organisatie anders is en geeft zelfs 3 tips om je wachtwoorden veilig te houden (die als universeel beschouwd moeten worden).

Uitdagingen en overwegingen bij de invoering van kaders

Het NIST Cybersecurity Framework kan complex zijn. Het is belangrijk om de kernfuncties volledig te begrijpen voordat je verder kunt gaan met de zeven stappen die hierboven zijn opgesomd. Om blijvend succes te garanderen, is het essentieel om een cyberbeveiligingscultuur binnen uw organisatie te stimuleren, anders zult u op weerstand stuiten tegen wat een drastische verandering in processen en systemen zou kunnen zijn.

Andere uitdagingen zijn onder andere:

- Beperkte middelen - het kan zijn dat je momenteel niet het personeel hebt dat deze veranderingen kan doorvoeren.
- U zult waarschijnlijk tijd moeten besteden aan het aanpassen van het Cybersecurity Framework zodat het beter past bij uw organisatie.
- Bedreigingen veranderen voortdurend, wat betekent dat uw beveiligingspraktijken gelijke tred moeten houden.
- U wilt het Cybersecurity Framework integreren met bestaande processen.
- Het kan een uitdaging zijn om de betrokkenheid van belanghebbenden te stimuleren, wat direct verband houdt met het bevorderen van een cyberbeveiligingscultuur die aan deze eisen kan voldoen.

NIST Cybersecurity Framework profielen en niveaus

Er zijn vier NIST-implementatieniveaus:

- **Tier 1 Gedeeltelijk** - Bedrijven met on-demand of nul beveiligingsprocedures.
- **Tier 2**: **Risico-geïnformeerd** - Bedrijven die zich bewust zijn van de bedreigingen waarmee ze worden geconfronteerd en een aantal beleidsmaatregelen hebben genomen, maar geen gecoördineerde strategie hebben.
- **Herhaalbaar op niveau 3** - Bedrijven met best practices op het gebied van risicobeheer en cyberbeveiliging die de goedkeuring van het management hebben gekregen. Deze bedrijven meten zichzelf vaak met concurrenten en werken zelfs samen met andere organisaties om ervoor te zorgen dat hun werkwijzen op elkaar zijn afgestemd.
- **Tier 4 Adaptief** - Bedrijven in sterk gereguleerde sectoren (zoals het bankwezen en de gezondheidszorg) die routinematig bijdragen aan een breed risicobewustzijn.

Volgens NIST is het Cybersecurity Framework Profile "de afstemming van de functies, categorieën en subcategorieën op de bedrijfsvereisten, risicotolerantie en middelen van de organisatie." Deze profielen helpen organisaties bij het opstellen van een stappenplan om de risico's voor cyberbeveiliging te beperken.

NIST biedt een aanpasbaar Cybersecurity Framework Organizational Profile Template, evenals een lijst met gemeenschapsprofielen die kunnen worden gebruikt.

Bijwerken en evolueren met het NIST Framework

Houd in gedachten dat het NIST Cybersecurity Framework is ontworpen als een levend document dat afhankelijk is van regelmatige updates die het steeds veranderende landschap van cyberbeveiliging en opkomende bedreigingen weerspiegelen. Daarom is het cruciaal dat organisaties op de hoogte blijven van de nieuwste bedreigingen, zodat het Cybersecurity Framework kan worden aangepast aan de huidige behoeften en voortdurend kan worden verbeterd.

Om ervoor te zorgen dat uw organisatie in staat is om mee te evolueren met het NIST Cybersecurity Framework, kunt u overwegen hoe u de beste cyberbeveiligingstechnologie voor uw bedrijf kunt bouwen, als een manier om ervoor te zorgen dat u in staat bent om gebruik te maken van de beste technologie die in staat is om mee te evolueren met het Cybersecurity Framework.

Bitwarden inzetten voor een sterkere cyberbeveiliging

Het spreekt voor zich dat beveiliging een van de belangrijkste aandachtsgebieden voor organisaties is geworden. Zonder robuuste praktijken voor risicobeheer op het gebied van cyberbeveiliging kunnen bedrijven het slachtoffer worden van allerlei bedreigingen in het wild. Met behulp van het NIST Cybersecurity Framework en zorgvuldige planning/communicatie kan de beveiliging van uw organisatie enorm verbeteren. Benader het NIST Cybersecurity Framework grondig, volg de 7 stappen en wees altijd klaar om bij te werken en te evolueren zodat je organisatie beter beschermd is tegen cyberbeveiligingsrisico's.

Klaar om vandaag nog aan de slag te gaan? Overweeg het gebruik van een oplossing voor wachtwoordbeheer om uw organisatie op de juiste manier te starten. Bekijk de plannen van Bitwarden Business, neem contact op met de verkoopafdeling en vergelijk de prijzen van de plannen.