Les 1. Security

V1.0

ROC Horizon College

HORIZONCOLLEGE.NL ALKMAAR | HEERHUGOWAARD | HOORN | PURMEREND

HORIZON COLLEGE

Samen werk maken van je opleiding

Wat is de bedoeling?

1. Wat is security?
2. Het School examen?
3. Certificering?
4. Nist Framework?
5. Volgende les?

Wat is of betekent security volgens jullie?

Wat is of wat betekent security?

Het begint al bij de Engelse vertaling; Safety staat voor veiligheid en Security staat voor beveiliging. Waar safety zich richt op niet-moedwillig handelen zoals een bedrijfsongeval, richt security zich op moedwillig handelen; bijvoorbeeld iemand die probeert in te breken.

Bij security gaat het over gevaren die wel met opzet worden nagestreefd, Physiek, of online en deze of elke manier te voorkomen en of op te lossen.

Het Schoolexamen?

Kandidatenset uitleg over de leerdoelen!!

Certificering?

Network security certificaat behalen aan het eind van de eerste periode!!! 6 weken

Certificaat 700 punten

Behalen van voldoende 550 punten

HET NIST CYBERSECURITY FRAMEWORK

Security is een cruciaal element van de Cloud en Fundaments wil maximale veiligheid hiervan kunnen bieden. Deze maximale veiligheid is dan ook niet te bieden met slechts één security-maatregel, maar door middel van een set van maatregelen.

Deze set van maatregelen is ingericht op basis van het NIST Cybersecurity Framework.

NIST Framework zijn vijf functies te onderscheiden, namelijk:

identify, protect, detect, respond en recover.

NIST Framework zijn vijf functies te onderscheiden, namelijk:

identify, protect, detect, respond en recover.

IDENTIFY - IDENTIFICEREN VAN CYBERSECURITY RISICO'S

Veel organisaties weten niet hoe ze ervoor staan als het gaat om (cyber-) beveiliging. Toch is dit vrij essentieel, want om een omgeving en daarmee een organisatie goed te beveiligen, is het belangrijk om exact te weten wat de huidige status is van het beveiligingsniveau. Hoe ziet bv. uw Cloud-omgeving eruit? Welk deel hiervan is kritisch voor de bedrijfsprocessen? Waar zitten eventuele zwakke plekken? Inzicht hierin verkrijgen is dus van groot belang om een effectief NIST framework op te stellen. Ofwel, identificeren wat er is, wat er beschermd moet worden en waar de mogelijke risico's liggen. Binnen het NIST Cybersecurity Framework wordt dit ***identify*** genoemd. Voor het identificeren van cybersecurity risico's biedt Fundaments de dienst Vulnerability Management.

PROTECT - BESCHERMEN VAN DATA

Het daadwerkelijk beschermen en dus het nemen van maatregelen voor de juiste beveiliging, is het onderdeel *protect*.

Deze hebben te maken met technische access-control: het implementeren van BV. firewalls. Daarnaast is er op techniek een maatregel beschikbaar voor het filteren van aanvalsverkeer: bv. Tegen DDoS-aanvallen. Deze maakt het mogelijk om aanvalsverkeer en legitiem verkeer door te zetten. Ook de mogelijkheid van bakups is niet onbelangrijk

DETECT - SIGNALEREN VAN BEVEILIGINGSINCIDENTEN

Wat moet er verder nog gebeuren voor optimale bescherming van uw Cloud-omgeving? Simpel: de beveiligingsmaatregelen in de gaten houden en cybersecurity incidenten tijdig signaleren, ofwel het onderdeel: *detect*.

Jaarlijks worden vele organisaties gehackt of krijgen ze te maken met een datalek. Gemiddeld genomen hebben hackers maanden vrij spel tot deze hacks en datalekken worden ontdekt, áls ze al worden ontdekt. Zelfs bedrijven die duizenden euro's uitgeven aan digitale veiligheid, hebben geen idee of er momenteel een hacker aanwezig is op hun netwerk. Bij *detect* draait alles om het implementeren en ontwikkelen van maatregelen om een cybersecurity-incident (en dus hackers) tijdig te signaleren.

RESPOND - REAGEREN OP BEVEILIGINGSINCIDENTEN

Nu komen we op het punt dat er actie ondernomen moet worden. In het NIST Cybersecurity Framework heet deze functie: *respond*. Als er een alarm afgaat, is het belangrijk dat er allerlei processen en procedures zijn ingericht om hier snel op te reageren. Hoe ziet het incident managementproces eruit? Is support voorbereid op alle telefoontjes en belletjes? Zijn de juiste mensen op de juiste plekken aan het werk om hiermee om te gaan? Op al dit soort vragen moet een antwoord zijn. Daarnaast is forensisch onderzoek en het zoeken naar de juiste inzichten om het incident op te lossen cruciaal.

Om een adequaat *respond*-draaiboek te faciliteren en opvolging te kunnen geven aan een melding moet er goed gekeken worden naar het bedrijf en wie waar verantwoordelijk voor is ook rekening houden met de AVG wet is hierin heel belangrijk.

RECOVER - TERUGKEREN NAAR DE SITUATIE VAN VÓÓR HET BEVEILIGINGSINCIDENT

Nadat er een beveiligingsincident is geweest, deze is geïdentificeerd en er actie is ondernomen, is het mogelijk dat uw Cloud-omgeving is beschadigd of gecompromitteerd. Om dan terug te keren naar een werkende situatie, is het belangrijk om hierop voorbereid te zijn. Dit heet *recover*. Het is hierbij cruciaal dat de data uit de Cloud-omgeving is veiliggesteld en u voorbereid bent om terug te keren naar een situatie voordat het beveiligingsincident plaatsvond.

Wat zou volgens jullie een oplossing kunnen bieden?

Alles op een rij:

- **IDENTIFY**

Identificeren van cybersecurity risico's.

- **PROTECT**

Beschermen van data.

- **DETECT**

Signaleren van beveiligingsincidenten.

- **RESPOND**

Reageren op beveiligingsincidenten.

- R**ECOVER**

Terugkeren naar de situatie van vóór het beveiligingsincident.

C:\Users\LANGP000\OneDrive - ROC Horizon College\Documenten\Security lessen\cybersecurity-health-check-schema (1).pdf

Volgende les?

1.Ethiek?

2.Labomgeving maken:

Belangrijke links:

Portal.azure.com

Downloaden van Microsoft ISO bestanden

Kali.org

Downloaden van Linux image