doel van onze website: informatie cybersecurity
domein e2 fundament

Samenvatting van het onderwerp Security

1. Basisprincipes van Security

- **Confidentiality (Vertrouwelijkheid):** Alleen bevoegde personen hebben toegang tot gevoelige informatie.
- **Integrity (Integriteit):** Gegevens mogen niet onbedoeld of ongeoorloofd worden gewijzigd.
- **Availability (Beschikbaarheid):** Systemen en gegevens moeten toegankelijk zijn wanneer nodig.

2. Soorten bedreigingen

- **Malware:** Schadelijke software zoals virussen, wormen, trojans en ransomware.
- **Phishing:** Pogingen om gevoelige informatie zoals wachtwoorden te verkrijgen via misleidende e-mails of websites.
- **Hacking:** Ongeoorloofde toegang tot systemen.
- **Social engineering:** Manipulatie van mensen om toegang te krijgen tot gevoelige informatie.
- **Denial of Service (DoS) attacks:** Overbelasting van systemen, waardoor deze niet beschikbaar zijn.

3. Beveiligingsmaatregelen

- **Authenticatie:** Verifiëren van de identiteit van een gebruiker, vaak met wachtwoorden, biometrie of tweefactorauthenticatie.
- **Encryptie:** Coderen van gegevens om ze onleesbaar te maken voor onbevoegden.
- **Firewalls:** Barrières die ongewenst netwerkverkeer blokkeren.
- **Antivirussoftware:** Bescherming tegen schadelijke software.
- **Backups:** Kopieën van gegevens om verlies te voorkomen.

4. Netwerkbeveiliging

- **Segregatie:** Netwerken opsplitsen in segmenten om de impact van een aanval te minimaliseren.
- **VPN's:** Virtuele privénetwerken voor veilige communicatie over het internet.
- **Intrusion Detection Systems (IDS):** Systemen die verdachte activiteiten op een netwerk detecteren.

5. Menselijke factor

- **Bewustwording:** Training en educatie om medewerkers bewust te maken van dreigingen.

- **Securitybeleid:** Duidelijke regels en richtlijnen over hoe om te gaan met IT-veiligheid.

6. Relevante wetgeving en normen

- **AVG (GDPR):** Europese privacywetgeving die de verwerking van persoonlijke gegevens reguleert.
- **ISO 27001:** Internationale standaard voor informatiebeveiligingsbeheer.
- **NIS-richtlijn:** Europese richtlijn voor netwerk- en informatiebeveiliging.

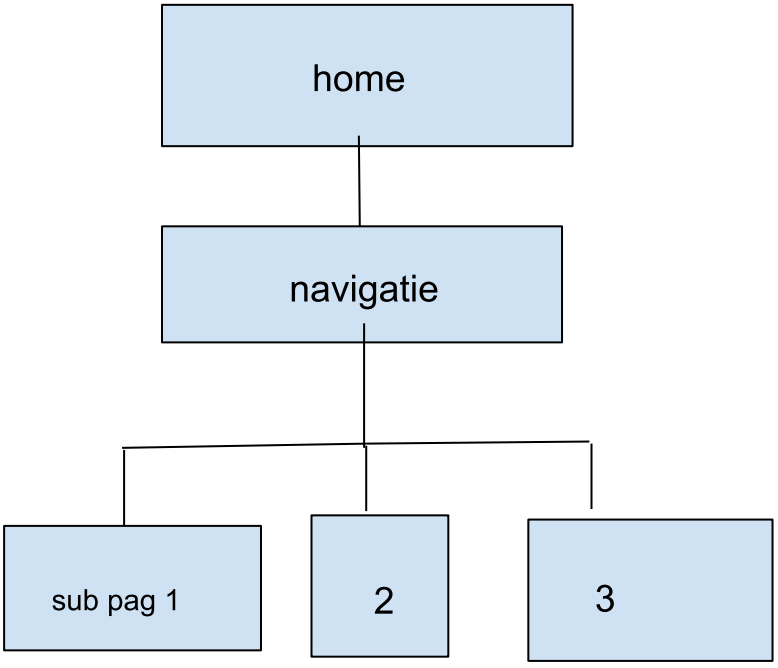
7. Incidentmanagement

- **Detectie:** Het snel identificeren van beveiligingsincidenten.
- **Respons:** Het effectief reageren om schade te minimaliseren.
- **Herstel:** Systemen herstellen en leren van incidenten om herhaling te voorkomen.

8. Trends in Security

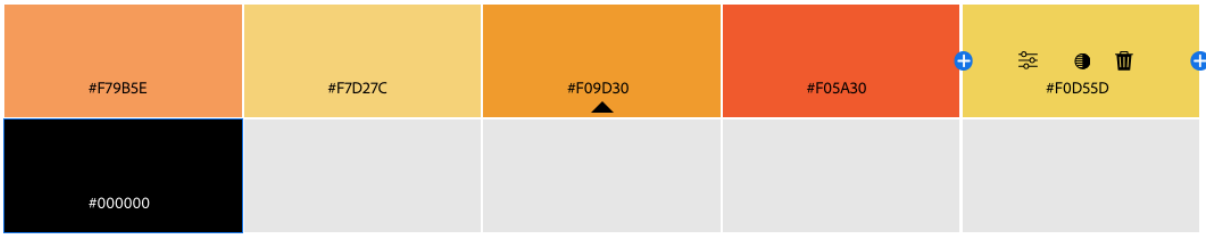
- **Zero Trust:** Een model waarbij niemand automatisch wordt vertrouwd, zelfs binnen het netwerk.
- **AI in Security:** Gebruik van kunstmatige intelligentie om aanvallen sneller te detecteren.
- **IoT-beveiliging:** Beveiligen van verbonden apparaten (Internet of Things).

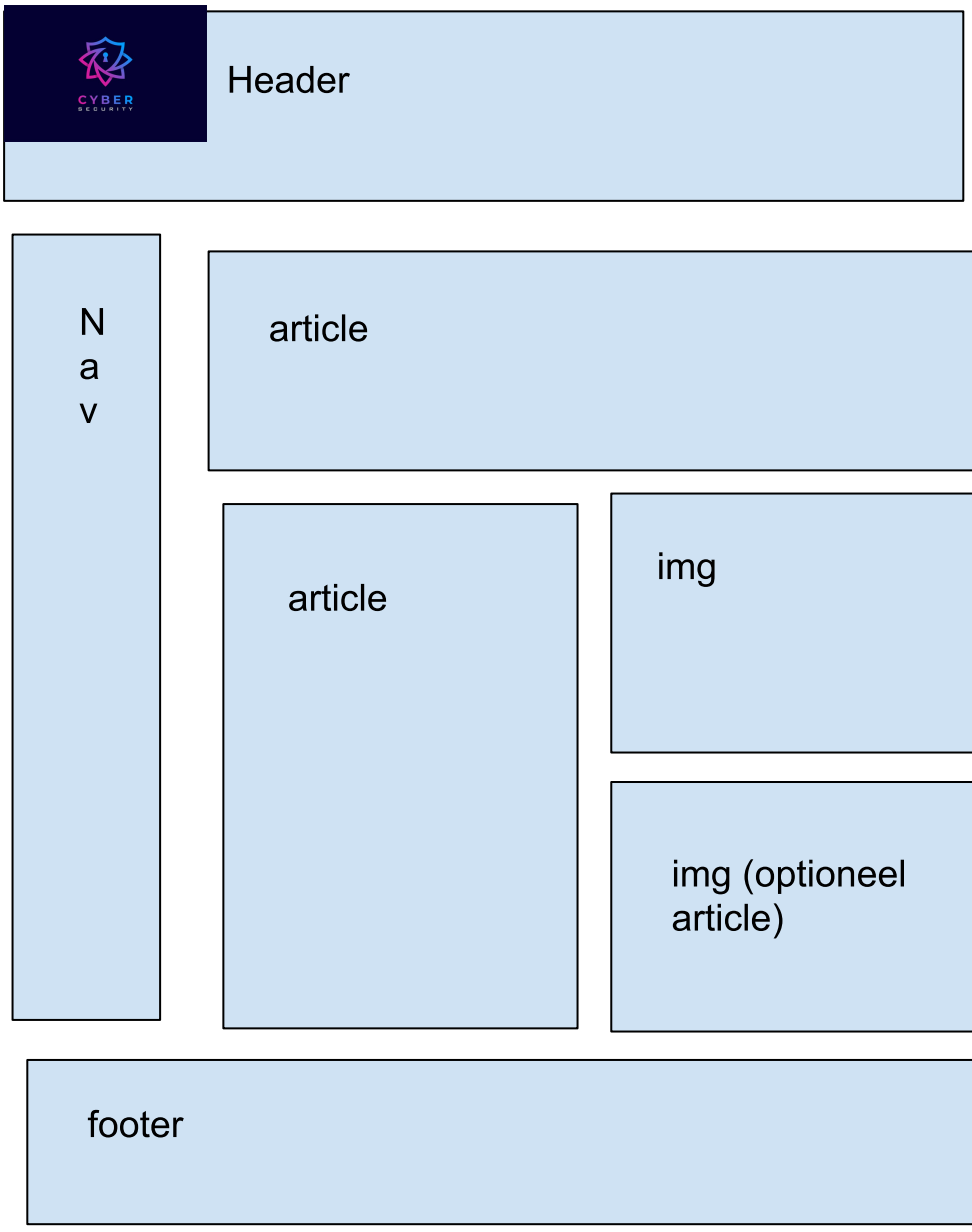
2 kopjes per subpagina



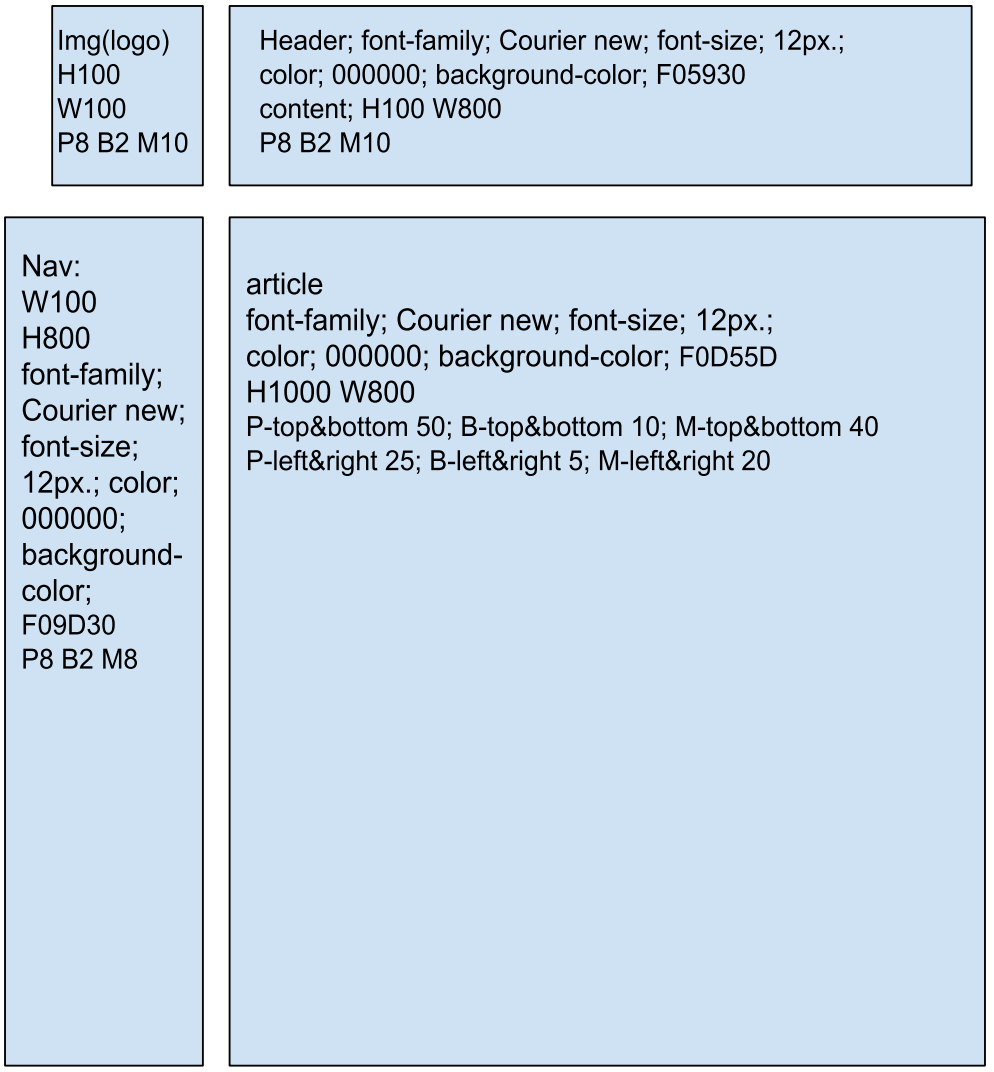
kleuren

1. #F79B5E
2. #F7D27C
3. #F09D30
4. #F05930
5. #F0D55D
6. #000000





logo-adres;
https://www.google.com/url?sa=i&url=https%3A%2F%2Fstock.adobe.com%2Fsearch%3Fk%3Dsecurity%2Blogo&psig=AOvVaw3h6SLjc4U-TYTrfiHO4URE&ust=1734174905016000&source=images&cd=vfe&opi=89978449&ved=0CBQQjRxqFwoTCMCo5fXPpIoDFQAAAAAdAAAAABAJ


Img(logo)
H100
W100
P8 B2 M10
Header; font-family; Courier new; font-size; 12px.;
color; 000000; background-color; F05930
content; H100 W800
P8 B2 M10
Nav:
W100
H800
font-family;
Courier new;
font-size;
12px.; color;
000000;
background-
color;
F09D30
P8 B2 M8
article
font-family; Courier new; font-size; 12px.;
color; 000000; background-color; F0D55D
H1000 W800
P-top&bottom 50; B-top&bottom 10; M-top&bottom 40
P-left&right 25; B-left&right 5; M-left&right 20
footer
font-family; Courier new; font-size; 12px.; color; 000000;
background-color; F7D27C
H100 W100%
P8 B2 M8