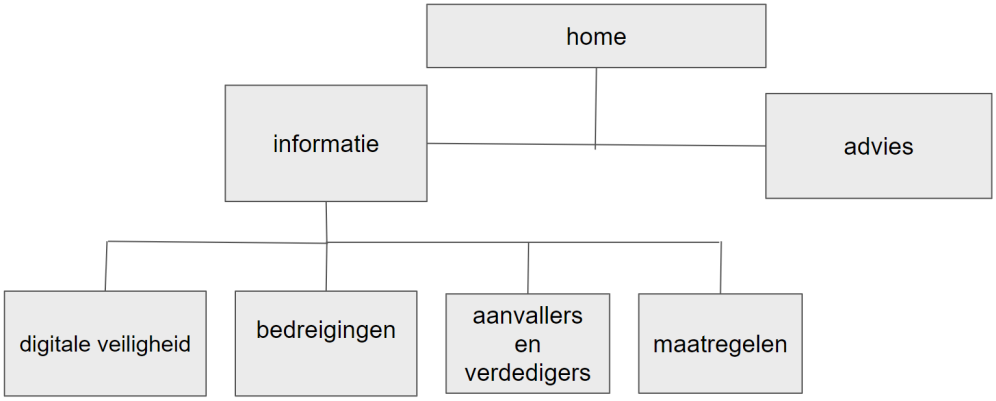
checklist:

- [x] ~~STAP 1: HET ONDERWERP UITDIEPEN~~
- [x] ~~STAP 2: DE SITEMAP~~
- [x] ~~STAP 3: DE KLEURENSTAAL~~
- [x] ~~STAP 4: HET PAGINAONTWERP~~
- [x] ~~STAP 5: EVALUEREN~~
- [ ] STAP 6: SCHEMATISCHE TEKENING

stap 2:



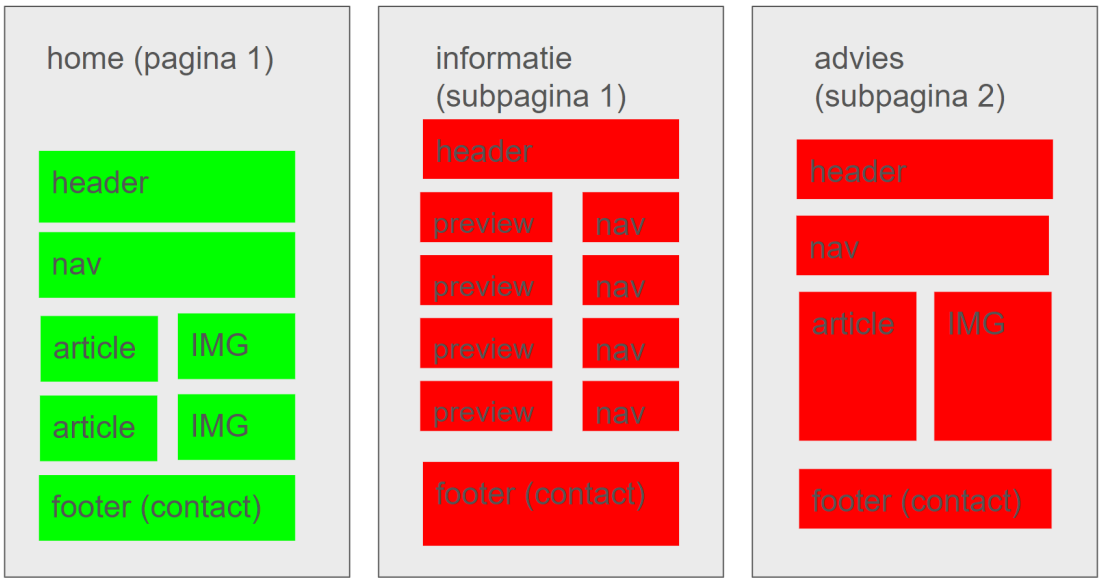
stap 3:

#0050E6

#00E1E6

#00AC62

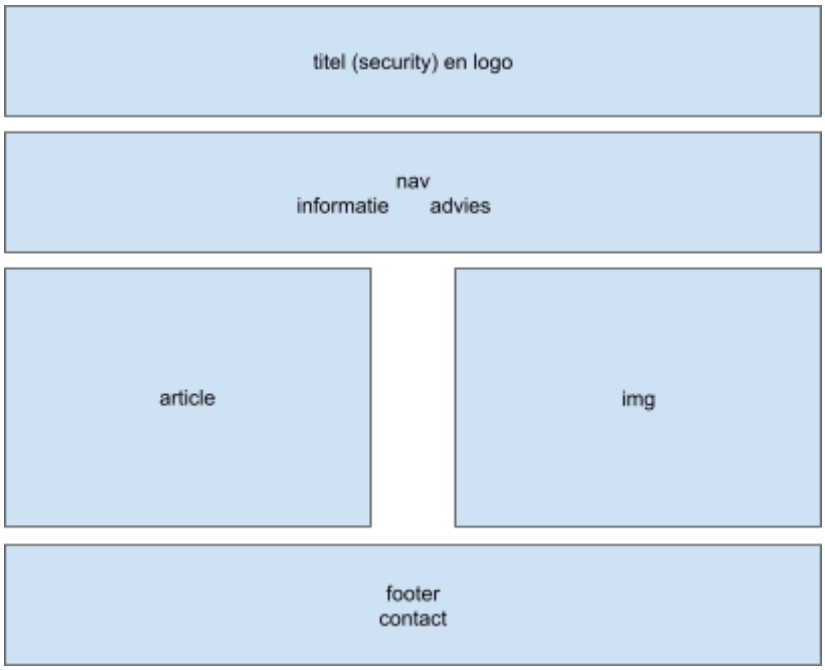
stap 4:



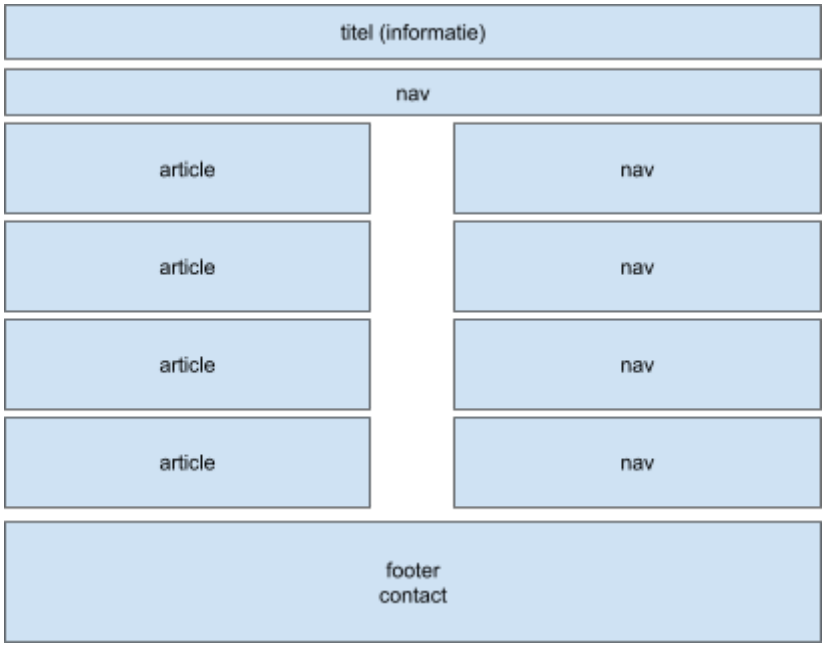
Stap 5:
RICHTLIJNEN

- ☑ ~~Alles richten op één doel.~~
- ☑ ~~Informatie in het middelpunt.~~
- ☑ ~~Plaatjes zijn beter dan woorden.~~
- ☑ ~~Maak belangrijke dingen duidelijker.~~
- ☑ ~~Zorg voor orde en rust.~~
- ☑ ~~Wijk niet af van dingen die overal hetzelfde zijn.~~

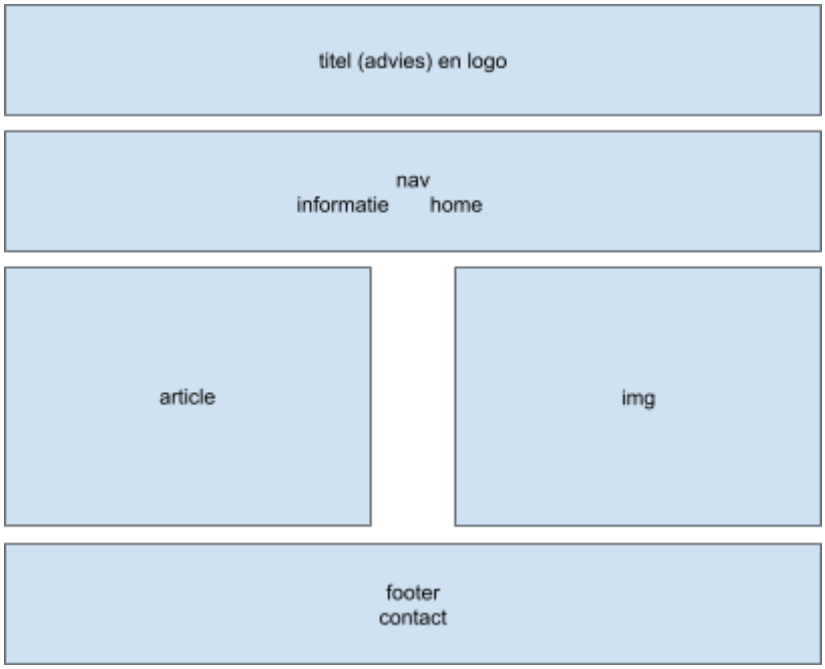
stap 6:
schematische tekeningen
home:



informatie



advies



stap 1:

Vertrouwelijkheid

Authenticatie is een controle om te kijken of een gebruiker wel toegang heeft. Er zijn verschillende soorten authenticatie, onder anderen iets wat je weet (wachtwoord, pincode), dingen die je hebt (Sleutel of pas) en wat je bent (vingerafdruk, face ID).

Bij identificatie wordt er gevraagd wie je bent, dit kan je bijvoorbeeld aantonen door een gebruikersnaam en wachtwoord in te voeren.

Daarna vindt er een verificatie plaats, er wordt gekeken of je dat ook echt bent. Het systeem controleert dan of je wachtwoord en gebruikersnaam correct zijn. Er kan alleen verificatie plaatsvinden als gegevens van jou bekend zijn.

Een veiligere toegangscontrole is 2 vormen van authenticatie combineren, 2 step verificatie. Als je gebruikersnaam en wachtwoord dus kloppen, kan je bijvoorbeeld ook nog een code ontvangen om dubbel te verifiëren dat jij het bent. Bij betalingen met bankpas wordt dit al jaren gedaan, je hebt niet alleen je pinpas nodig, maar ook de pincode ervan. Met alleen een pinpas kan je niets, met alleen een pincode ook niet, je hebt ze allebei nodig.

Integriteit

Autorisatie is de controle hoeveel rechten jij hebt. Zo heeft een beheerder van een website meer rechten dan jij als gebruiker. Zo kan jouw docent (beheerder) in magister cijfers invoeren voor jou, terwijl jij als leerling (gebruiker) ze alleen maar kan bekijken. Autorisatie wordt ook wel de controle van de integriteit genoemd.

De volgende dingen worden gecontroleerd:

Volledigheid
Ontbreekt er iets?

Relevantie
Is de informatie afgestemd op het te bereiken doel?

Betrouwbaarheid
Klopt de informatie en komt het van een betrouwbare bron?

Overzichtelijkheid
Is de informatie goed gestructureerd?

Beschikbaarheid
Is de informatie op het juiste moment beschikbaar?

Doelgerichtheid
Is de informatie gericht op de gebruiker?

Met integriteit kan je sommige schijven of mappen alleen beschikbaar maken voor gebruikers met een specifieke rol. Voor toegang tot deze bestanden hoeft niet apart ingelogd te worden, er wordt alleen gecontroleerd of je toegang hebt. Dit kan ingesteld worden via ‘file permissions’.

Checksums:

Als jij online een bestand met iemand wil delen, kan het dat het onderweg aangepast wordt. Als jij iets op het internet download, staat er vaak een checksum bij. Je kan dit dan vergelijken met het checksum van jouw gedownloade bestand, om te checken of het nog hetzelfde is.

IBAN:

Als jij geld naar iemand over wilt maken, wil je zeker weten dat het de juiste persoon is, en dat je het naar de juiste IBAN overmaakt. Er zit een mechanisme in IBAN's dat typefouten kan voorkomen, dat systeem het een controlegetal, en lijkt op een checksum.

Het werkt als volgt:

Verplaats de eerste vier karakters naar het einde van het IBAN.
Vervang elke letter door twee cijfers, volgens het systeem A = 10, B = 11, enz.
Bereken het getal modulo 97. Dit houdt in dat je het getal deelt door 97, en de restwaarde onthoudt.
Als de restwaarde 1 is, dan gaat het om een valide IBAN.

3. aanvallers en verdedigers

Er zijn veel vormen van cybercrime. Daaronder vallen meerdere dingen zoals: diefstal, fraude en afpersing. Hiervan heb ik nu wat voorbeelden:

- iemands identiteit kan gestolen worden. Dit is een veel voorkomende manier van online diefstal waarbij iemand dus bijvoorbeeld de inloggegevens van iemands Instagram account hackt en dan alles daarmee kan doen.
- Fraude is ook een vorm van oplichting: er wordt bedrog gepleegd, meestal met het doel om mensen geld afhandig te maken, een bekend voorbeeld daarvan is phishing.
- Je kan ook afgeperst worden, hier wordt vaak met informatie die jij niet op het internet wilt hebben staan gedreigd. Dingen waar vaak mee gedreigd wordt is inloggegevens of naaktfotos

Online inbreken (hacken) is een van de grootste bedreigingen van cybersecurity. In de wet staat het beschreven als computervredebreuk. Wat is allemaal strafbaar als het gaat om hacken?

- binnendringen, dit is heel logisch want dat is een letterlijke inbreuk alleen dan online, maar ook al proberen binnendringen is al strafbaar.
- Het bezitten van hulpmiddelen met het doel om te hacken is ook strafbaar. Dus alleen al hack software op je computer hebben staan is strafbaar.

Als een slecht beveiligde website gehackt wordt en jouw gegevens staan daarop dan is de eigenaar van de website strafbaar. Je mag ook geen openstaande achterdeur gebruiken om binnen te dringen, maar die mag je wel melden.

Als je hebt ingebroken in een computer, ben je dus schuldig aan computervredebreuk. Dat is al zo, als je na de inbraak verder niets hebt gedaan. Als je daarna ook nog gegevens kopieert, verwijdert of wijzigt of op een andere manier schade aanbrengt, dan telt het als extra strafbaar.

Ethisch hacken

Dit is een vorm van hacken die juist voor goed bedoeld is. Bij ethisch hacken ben je nog steeds wel aan het inbreken maar nadat je ingebroken hebt informeer je bedrijven hoe het veiliger kan zijn. Dit is dan niet strafbaar omdat je een publiek belang dient, dat betekent dat je iets doet voor de overheid of de mensheid wat goed is. Er gelden natuurlijk wel regels. Je mag alleen hacken als dat de enige manier is om een misstand aan te tonen. Die misstand moet ook ernstig genoeg zijn. En je moet het daarbij laten. Als je vervolgens ook nog onnodige gegevens steelt of onnodig veel computers hebt gehackt, word je daar wel voor vervolgd.

Spionage en oorlogsvoering

Een zero day is een nog niet ontdekte kwetsbaarheid. Zero days zijn belangrijke middelen die kunnen worden gebruikt om te hacken. Daarom zijn ze geld waard. Er bestaat veel handel in. Belangrijke zero days worden verkocht voor enkele tienduizenden tot wel honderdduizenden euro’s. Deze Zero days worden gebruikt op meerdere manieren maar de meest onveilige manieren zijn spionage en oorlogsvoering. Bij spionage worden deze middelen gebruikt om belangrijke data te halen uit wat de eigenaar denkt veilige programma's. Het meest spectaculaire voorbeeld van het gebruik van zero days in oorlog, is de inzet van Stuxnet, malware die door de Amerikaanse en Israëlische inlichtingendiensten is ontwikkeld om het Iraanse kernprogramma te saboteren. Stuxnet bevatte verscheidene zero days, waardoor het mogelijk was om de software ongemerkt te installeren bij de Iraanse centrale bij Natanz. Daar zorgde de software er vervolgens voor dat de centrifuges, die werden gebruikt om uranium te verrijken, veel sneller of veel trager gingen draaien. Zo konden Amerika en Israël het Iraanse programma om kernwapens te ontwikkelen vertragen.

4. maatregelen

Preventie:

preventieve beveiligingsmaatregelen zijn de maatregelen die worden genomen om problemen te voorkomen. Dat begint bij hard- en software. Die moet veilig worden gemaakt en de software moet up-to-date blijven. Dat betekent bijvoorbeeld dat een softwareontwikkelaar op de hoogte moet zijn van manieren waarop je goed beveiligde software maakt. Een voorbeeld van een software security maatregel is sandboxing, hierbij geef je een app niet toegang tot alles op je computer maar alleen wat het nodig heeft om te functioneren. Dit zie je bijvoorbeeld terug als je telefoon bij het openen van een app vraagt om toegang tot je camera.

Detectie

Software is nooit perfect en dat is waarom je systemen nodig hebt om de imperfecties te detecteren, een controle op misbruik. Een voorbeeld hiervan is een detectiesysteem die detecteert hoeveel mislukte inlogpogingen er zijn gedaan met dezelfde gebruikersnaam. Om detectie mogelijk te maken, worden allerlei gegevens over het

gebruik van het systeem gelogd.

Een belangrijk hulpmiddel is de firewall. Die scant al het binnenkomende netwerkverkeer. Alle datapakketten worden gecontroleerd op kwaadaardige gegevens. Ook kan een firewall controleren of het verkeer afkomstig is van een vertrouwde bron. Firewalls beschermen tegen hackers, malware en spam. Er zijn firewalls voor computers en voor netwerken. Je hebt ook IDS, dat staat voor: Intrusion Detection System. Dit systeem checkt alles wat in het netwerk zit, dus als er iets niet normaal verloopt dan kan hij dat detecteren met statistieken.

Het tweede belangrijke hulpmiddel is anti-malware software. De naam zegt het al maar alle malware die die software tegenkomt wordt verwijderd. Bijvoorbeeld de appstore van Apple gebruikt deze techniek om malware in apps te voorkomen.

SecureVibe