Samenvatting security (E2)

Over Security

Als je op het internet gaat, wordt er heel veel persoonlijke informatie vastgelegd. (WAT VOOR INFO). Om te voorkomen dat dit op de verkeerde manier wordt gebruikt, doordat hackers bijvoorbeeld aan deze informatie komen, bestaat er security. Hackers zijn mensen die een computersysteem binnendringen, maar ze hoeven niet per se slechte bedoelingen te hebben. Hackers kunnen ook helpen de verdediging, van bijvoorbeeld een website, te verbeteren. Hacker is dus een meer algemene term, maar zelfs internetcriminelen hoeven niet per se hackers te zijn.

Digitale veiligheid

Zoals eerder gezegd, worden veel (persoonlijke) gegevens opgeslagen, bijvoorbeeld de video's die je plaatst op Tiktok, of op Magister. Door digitale veiligheid is het moeilijker om aan deze gegevens te komen. Digitale veiligheid of digital security is de naam voor alle manieren waarop je eigen digitale footprint beschermd kan worden. Iedereen die betrokken is bij het verwerken van jouw digitale gegevens heeft verantwoordelijkheid, de ontwikkelaars die zorgen voor een veilig systeem, of jij die (hopelijk) een sterk wachtwoord heeft bedacht. Bij digitale veiligheid wordt er vooral gekeken naar de volgende punten:

1. Vertrouwelijkheid
   De afscherming van jouw gegevens voor onbevoegde personen
2. Integriteit
   De bescherming tegen verlies of wijzigingen
3. Beschikbaarheid
   Hoeveelheid storingsvrije toegang tot gegevens

Vertrouwelijkheid

Om ervoor te zorgen dat alleen bevoegde mensen toegang krijgen tot persoonlijke informatie wordt er een proces toegepast genaamd authenticatie. Er zijn drie verschillende soorten bij dit proces, bijvoorbeeld doordat je iets weet (zoals een bepaald wachtwoord dat je weet), iets hebt (bijvoorbeeld dat je een bankpas hebt) of iets bent (jij bent de vingerafdruk)

Naast **authenticatie** zijn er ook de begrippen **identificatie** en **verificatie**. Met identificatie bedoelen we: Wie ben je? Dit doe je door middel van gezichtsidentificatie of een wachtwoord. Bij verificatie wordt er gezocht naar het antwoord op de vraag: Ben jij wie je zegt dat je bent? Dit kan alleen gedaan worden als er al gegevens van jou bekend zijn in bijvoorbeeld een database.

Hoe meer vormen je van authenticatie combineert, hoe veiliger jouw gegevens zijn. Als dit met 2 vormen doet, heet dat two factor authentication. Bijvoorbeeld: Als je inlogt op een website, moet je vaak nog je inlog bevestigen met een code die je via mail of sms krijgt.

Een techniek die gelinkt is aan de begrippen (dikgedrukt) heet **screening**. Veel mensen of voertuigen worden hierbij geïdentificeerd en als een van deze op een blacklist staat, wordt hier een melding van gemaakt, wanneer je hier niet op staat, gebeurt er niks.

Integriteit

Met een bepaalde rol, kan je verschillende gegevens zien of veranderen. Als leerling mag je alleen de cijfers zien, maar als docent kun je deze ook veranderen. Als een controle gaat over welke rechten een vertrouwelijke gebruiker heeft, heet dit autorisatie of de controle van de integriteit.

Hieronder verschillende eisen met controlevragen.

Eis	Controlevraag
Volledigheid	Ontbreekt er iets?
Relevante	Is de informatie afgestemd op het te bereiken doel?
Betrouwbaarheid	Is de informatie correct en afkomstig van een goede bron?
Overzichtelijkheid	Is de informatie goed gestructureerd?
Beschikbaarheid	Is de informatie op het juiste moment beschikbaar?
Doelgerichtheid	Is de informatie gericht op de gebruiker (de doelgroep)?

De integriteit van gegevens: kwaliteit van gegevens voldoet aan deze eisen
Als je toegang wilt hebben tot gegevens, met een bepaalde rol, vindt er autorisatie plaats. De controle of jij toegang hebt, dit kan werkelijkheid worden met *file permissions*. Om ervoor te zorgen dat iedereen toegang krijgt tot hetzelfde bestand en er onderweg niet dingen zijn aangepast, maken we gebruik van een checksum. Om op een andere manier te zorgen voor het krijgen van dezelfde data, kan je gebruik maken van backups. Als je een backup maakt en er per ongeluk toch iets verandert, kan je altijd weer de eerdere versie op de backup terugkrijgen.

Een bepaalde versie van checksums heet IBAN, dit wordt gebruikt bij het overmaken van (grote) bedragen door middel van rekeningnummers. Voor het gebruiken van dit systeem zijn er 4 stappen:

1. De eerste 4 karakters (van het rekeningnummer) naar het einde.
2. Elke letter krijgt twee cijfers, waarbij A=10, B=11, etc.
3. Je deelt het gehele getal door 97 en onthoudt de rest.
4. Als restwaarde=1, dan is de IBAN valide.

Beschikbaarheid
Je wilt natuurlijk niet dat je opeens niet meer bij je gegevens kan. De data moet altijd beschikbaar zijn, dit doe je bijvoorbeeld door beveiligingsupdates te installeren of eventueel kapotte hardware-onderdelen te vervangen. Zoals al eerder gezegd kan je ook hier gebruik maken van back-ups. Het beste kan je een fysieke back-up, zoals een USB, op een andere plek bewaren, om te voorkomen dat als bijvoorbeeld je computer kapot gaat, je op een andere plek nog wel de data hebt bewaard.
Beveiligingsexperts raden je daarom vaak aan om het 3-2-1-systeem voor back-ups te gebruiken: Het hebben van minimaal 3 kopieën, minimaal op 2 verschillende plekken opgeslagen en één kopie op een andere plek.

Encryptie

Als je een toegangscontrole uitvoert, wil je het liefste niet dat hackers opeens bij de database met al jouw inlogcodes kunnen. Deze belangrijke of gevoelige bestanden kan je versleutelen door middel van encryptie. Het werkt op de volgende manier: Met een sleutel (bijvoorbeeld een wachtwoord) wordt het bestand gehusseld en zonder dat je de sleutel hebt, zal je niks van het nieuwe bestand begrijpen, maar dan moet je die sleutel wel achter slot en grendel bewaren!

Gelukkig zijn je wachtwoorden toch wel wat beter beveiligd dan je zou denken. Er bestaat namelijk hashing. Hashing heeft hetzelfde principe als encryptie, alleen kan je hierbij het origineel niet terughalen. Het wachtwoord dat je invoert als je probeert in te loggen, wordt ook gehasht en dit wordt vergeleken met het eerste gehashte wachtwoord, als dit overeenkomt, dat is het het goede wachtwoord!

DDoS-aanval
Een DDoS-aanval is een manier waardoor je (voor geld) een server of website (tijdelijk) kunt laten crashen. Dit gebeurt als je veel meer aanvragen stuurt dan deze server of website aankan. De DDoS-aanval is voltooid wanneer gewone gebruikers niet meer bij de server of website kunnen. DDoS staat voor: Distributed Denial Of Service.
Om dit te voorkomen kan je het verkeer naar een website of server filteren. Als dit niet helpt, bestaan er anti-DDoS-diensten met geavanceerde methodes om de DDoS-aanval tegen te gaan.

Bedreigingen

Zwakheden bij…

de architectuur: Bij een lek is er een probleem door een tekortkoming in een van de 3 lagen (toepassingslaag, logische laag, fysieke laag) of de communicatie tussen die lagen, waardoor een onbevoegd persoon bijvoorbeeld bij jouw camera of microfoon kan. Iets anders wat fout kan gaan heet SQL. Hierbij wordt de vraag aan de website of app veranderd, om andere informatie te krijgen (, te verwijderen of aan te passen), dit heet een SQL-injectie. Om dit te voorkomen kan je de architectuur 'testen', dit is het proces waarbij ethische hackers de apparatuur proberen aan te vallen en hierbij te testen of dit mogelijk is of niet.

de communicatie: Je wilt natuurlijk dat de communicatie die er mogelijk is tussen verschillende apparaten veilig gebeurt. Wanneer dit niet het geval is, kan er sprake zijn van een 'man-in-the-middel' aanval. Hierbij is de verbinding tussen twee apparaten niet veilig en kunnen er dingen afgeluisterd worden. Dit kan makkelijk gedaan worden als een hacker zelf een openbaar wifi-netwerk opzet.

HTTPS

Er zijn bepaalde protocollen over hoe het internetverkeer geregeld is, zoals HTTP en HTTPS. Door deze twee protocollen is het mogelijk een beveiligde verbinding te verkrijgen tussen client en server. Het blijft mogelijk om mee te luisteren, maar niet te zien, door het gebruik van asymmetrische encryptie. Het is al een paar jaar verplicht voor apps om gebruik te maken van HTTP.

Bij HTTPS, moet de beheerder een SSL-certificaat maken, hierin staan gegevens over wie de beheerder van de website. Het gebruik van HTTPS kan je zien op de adresbalk, waar dan een slotje moet staan.

End-to-end encryption

Bij end-to-end encryptie worden alle gegevens versleuteld tot jij het internet weer verlaat, waarbij alleen jij en de ontvanger de officiële gegevens kunnen ontsleutelen, dit voorkomt dat hackers de gegevens kunnen zien, zelfs áls ze toegang krijgen tot de server.

de gebruikers: Wij, als gebruikers, zijn een grote zwakheid, vooral als het gaat om wachtwoorden handhaven. We gebruiken vaak makkelijke, dezelfde wachtwoorden, wat het makkelijk maakt voor hackers om zo snel al onze gegevens te weten te komen. Een manier die hackers hiervoor gebruiken heet brute force: ze gebruiken programma's om duizenden wachtwoorden per seconde te proberen, om zo achter jouw wachtwoord te komen. Hoe moeilijker jouw wachtwoord, hoe langer het duurt om het te kraken dus. Hierdoor verplichten veel websites je een wachtwoord te maken van bijvoorbeeld 8 tekens, minimaal één hoofdletter en speciale tekens.

Om dan toch 10+ wachtwoorden te onthouden is moeilijk, daarom zijn er password managers, maar hier moet je dan een bijna onkraakbaar wachtwoord voor aanmaken! Hackers kunnen, als het ze toch lukt om bij jouw inloggegevens te komen, deze verkopen of nep-mails te sturen. Zo kunnen ze nog meer informatie van jouw verkrijgen! Goede wachtwoorden verzinnen dus.

Technieken voor het hacken van gegevens

1.Social engineering
De mens is een zwakheid, daar maken hackers gebruik van. Zo kunnen hackers psychologische trucjes gebruiken, door te doen alsof ze iemand anders zijn, om jouw gegevens met hen te laten delen. Dit kan d.m.v. een telefoongesprek of een e-mail.

2.Phishing
Deze techniek wordt gebruikt in combinatie met social engineering. Bij deze techniek wordt de gebruiker namelijk via social engineering naar een andere, valse website gelokt. Er wordt bijvoorbeeld gezegd dat er iets mis is en je opnieuw moet inloggen. Deze inloggegevens worden gelijk opgevangen door de hackers en opeens ben je je account kwijt!

3.Malware
We gaan het hebben over de 6 meest voorkomende malware (kwaadaardige software):

1. Trojan Horse
2. Virus
3. Worm
4. Spyware
5. Adware
6. Ransomware

Vaak wordt bij malware gebruikgemaakt van zero day kwetsbaarheid, dit zijn zwakke plekken die nog niet bekend zijn bij de ontwikkelaar.

Trojan Horse
Verwezen naar het paard in de oorlog van Troje, krijgt de gebruiker als het ware ‘een cadeautje’, zoals een e-mail met: U heeft net de Jumbo klant van het jaar prijs gewonnen! Klik op deze link om uw prijs te ontvangen! Veel gebruikers zullen dan misschien toch op die link klikken, onwetend malware geïnstalleerd te krijgen. Dit kan bijvoorbeeld jouw systeem openzetten voor hackers. De Trojan Horse kan zichzelf niet verspreiden.

Worm
De worm kan zichzelf, in tegenstelling tot de Trojan horse, wel zelf vermeerderen. Het baant zich een weg door het internet via een e-mail of bestanden. Niet alle wormen zijn kwaadaardig, maar wel malware, aangezien je er de toestemming van de gebruiker niet voor vraagt.

Virus
Een virus besmet vaak uitvoerbare bestanden of executables (bestanden voor het opstarten van software). Het richt dan schade aan en verspreidt zich naar andere computers. Het enige verschil met een worm is dat een worm op zichzelf al een compleet computerprogramma is en een virus niet.

Spyware en Adware
Spyware probeert informatie over jouw computergebruik te achterhalen, vaak wordt via het internet de informatie overgebracht aan de maker van de desbetreffende spyware.

Adware is het weergeven van advertenties op je computer, wat nota bene zelfs legaal kan zijn, maar natuurlijk kan adware ook ongewenste advertenties weergeven. Ook kan het gerichte reclame aan jou weergeven.
Adware en spyware hebben overeenkomsten, maar zijn qua functie toch verschillend.

Ransomware
Ransomware is malware die een systeem binnendringt en vervolgens bestanden versleutelt, waardoor jij deze als gebruiker niet meer kunt gebruiken. Er kan daarna een melding verschijnen (soms met tijdsdruk), waarin staat dat jij geld moet betalen om je bestanden weer terug te krijgen. Dit moet je over het algemeen niet doen, omdat teruggave niet zeker is en omdat je niet wilt dat criminelen aan geld komen.

Aanvallers en verdedigers

Computercriminaliteit
Diefstal, fraude, afpersing en inbraak (hacken) zijn voorbeelden van computercriminaliteit (cybercrime). Beveiligingsbedrijven kunnen helpen om cybercrime te bestrijden.

Diefstal
Een computercrimineel kan proberen data te stelen van jouw computer of van een database waarin gegevens van jou staan. De crimineel verkoopt deze gestolen data.

Fraude
Als een computercrimineel onder jouw naam criminele activiteiten uitvoert, heet dat identiteitsfraude. Ook op andere manieren kan er gefraudeerd worden, vaak met als doel om geld van mensen te krijgen. Voorbeelden van deze vorm van oplichting zijn: phishing, spyware of fraude door online shops, sociale media of online dating.

Afpersing
Ransomware of andere malware kan gebruikt worden om mensen of bedrijven af te persen. Ook kan een crimineel gevoelige (gestolen) gegevens of naaktfoto's gebruiken voor afpersing.

Hacken
Een van de grootste bedreigingen van cybersecurity is hacken (computervredebreuk). Voor computervredebreuk kun je in de gevangenis terechtkomen. Computervredebreuk is het ongeoorloofd binnendringen in een computersysteem of een netwerk. Dat is dus digitaal inbreken.
Hacken is ook al strafbaar als je het alleen maar probeert en het niet eens lukt. Ook alleen het hebben van hulpmiddelen, zoals een keylogger of hack software, is al strafbaar. Kopieer, verwijder of wijzig je gegevens na de inbraak? Dit is dan extra strafbaar.

Ethisch hacken
Soms zijn websites of computersystemen niet goed beveiligd. Dit is verwijtbaar. De eigenaar van een slecht beveiligde website waarop persoonsgegevens bewaard worden, is zelfs strafbaar. Toch mag je dan niet inbreken. Je mag zo'n beveiligingslek wel melden. Dat heet ethisch hacken en is juist heel goed. Het internet wordt daar veiliger van.
Als een beveiligingslek openbaar wordt, kunnen criminelen er misbruik van maken. Daarom geven veel bedrijven (ethische) hackers een beloning, als zij een lek melden. De bedrijven kunnen zo op tijd het lek dichten, voordat er grote schade ontstaat.
Sommige ethische hackers maken een lek wel openbaar om de gebruikers te waarschuwen. Vaak kiezen ze voor een tussenvorm: eerst melden ze het lek bij de verantwoordelijke persoon en na een bepaalde periode maken ze het lek openbaar. Dit heet responsible disclosure.

Spionage en oorlogsvoering
Een kwetsbaarheid die nog niet ontdekt is, heet een zero day. Die zijn geld waard, want daarmee kunnen schadelijke aanvallen worden uitgevoerd, gegevens worden gestolen of systemen worden platgelegd. Criminelen, maar ook beveiligingsbedrijven zijn natuurlijk zeer geïnteresseerd in zero days.

Ook overheden gebruiken zero days om bijvoorbeeld te spioneren of vijandelijke systemen plat te leggen. Door zero days te gebruiken en niet te melden, wordt het internet natuurlijk onveiliger. Het gebruik van zero days is daarom omstreden. De Nederlandse overheid mag zero days alleen onder strenge voorwaarden gebruiken.