Digitale veiligheid

Alle manieren waarop je eigen digitale identiteit beschermd kan worden, noem je **digitale veiligheid. Vertrouwelijkheid**, **integriteit** en **beschikbaarheid** spelen hierbij de belangrijkste rol.

Bij het toegang geven tot persoonlijke gegevens, wordt er gebruikgemaakt van **authenticatie**, **identificatie** en **verificatie.** Bij authenticatie wordt er gekeken of de persoon recht heeft op de toegang door middel van iets dat je weet of hebt. Vaak wordt dit gecombineerd en dit noem je **two factor authentication.**

Autorisatie (controle van integriteit) is de controle op welke rechten een vertrouwde gebruiker heeft. Deze rechten zijn verbonden aan de **rol** die de persoon heeft. Met de integriteit van gegevens en informatie wordt bedoeld dat de kwaliteit van de gegevens zo is, dat er aan de eisen wordt voldaan (Volledigheid, relevantie, betrouwbaarheid, overzichtelijkheid, beschikbaarheid en doelgerichtheid). De gegevens mogen alleen verwerkt worden door de gebruikers die hier de juiste rechten voor hebben. Om toegang te krijgen tot bestanden die alleen beschikbaar zijn voor gebruikers met een specifieke rol, moet er autorisatie plaatsvinden. Dat kan door de systeembeheerder worden ingesteld via file permissions.

Als je een bestand vestuurt en er onderweg iets mee is gebeurd, waardoor de inhoud is aangepast, is de integriteit van het bestand aangetast. Als je installatiebestanden van programma's downloadt via het internet, zie je er soms een **checksum** bij staan. Deze is gegenereerd toen de makers de bestanden online zetten. Als jij het bestand downloadt en ook een checksum genereert, kun je controleren of je exact hetzelfde bestand hebt. Ook door het maken van back-ups kan je de integriteit van je data gegaranderen. Het controlegetal is een systeem dat typfouten in een IBAN (rekeningnummer) kan voorkomen. Het heeft wat weg van een checksum.

Het systeem werkt als volgt:

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

Als je een getal in het IBAN aanpast, wordt het direct ongeldig. Zo worden typfouten voorkomen en weet je zeker dat je een IBAN goed hebt overgenomen

Voor een toegangscontrole moeten er gegevens worden opgeslagen. Omdat dit veel risico met zich meeneemt, wordt er bij deze bestanden met gegevens gebruikgemaakt van **encryptie.** Het bestand wordt gehusseld en alleen met de 'sleutel' (het wachtwoord) kun je het origineel terugkrijgen. Bij **hashing** wordt bijvoorbeeld het wachtwoord ook gehusseld, waardoor je niet meer terug kan naar het origineel. Een **DDoS-aanval** is een gecontroleerde aanval om een service uit te schakelen. Deze aanval komt omdat er te veel aanvragen worden gedaan en de website crasht. Een DDoS-aanval is strafbaar en kan worden tegengegaan door het filteren van

het verkeer naar de website of door het omleiden van het internetverkeer naar een gespecialiseerde anti-DDoS-dienst.

Bedreigingen

Aanvallers maken gebruik van zwakheden in de architectuur en communicatie van de website en zwakheden bij de gebruikers.

Bij een **lek** heeft de aanvaller een fout gevonden in de architectuur, bijvoorbeeld bij het drielagenmodel. Bij **SQL-injectie** worden er gegevens in een slecht beveiligde databaseverbinding aangepast.Door de architectuur te testen kan je zelf de fouten opsporen en verhelpen.

Met een **man-in-the-middel aanval** kan het internetverkeer tussen twee apparaten afgeluisterd worden. Zonder dat je het doorhebt komt er iemand tussen de verbinding van de twee apparaten, die het internetverkeer afluistert. Als je gebruikmaakt van een protocol HTTPS verbinding, zijn je verstuurde gegevens versleuteld. Bijna alle apps en website maken hiervan gebruik. Beheerders van een website die HTTPS gebruikt, moet een **SSL-certificaat** installeren. Dit certificaat bevat gegevens over de eigenaar van de website en moet worden aangevraagd bij een centrale organisatie.**End-to-end encryptie** versleutelt berichten voordat ze het internet op gaan en ontsleutelt ze pas wanneer ze het internet verlaten. Alleen de verzender en ontvanger kunnen ze versleutelen. Dit lost dus de gevolgen van de zwakheden in zowel de architectuur als de communicatie van de website op.

Bij **brute force** probeert een speciaal programma duizenden wachtwoorden per seconde, met de bedoeling om jouw wachtwoorden te kraken. Websites proberen dit te voorkomen door een maximaal aantal pogingen in te voeren om je wachtwoord in te voeren. Helaas vinden de krakers soms een zwakheid in de architectuur waardoor ze veel meer wachtwoorden kunnen invoeren. Om te voorkomen dat jouw wachtwoord door een brute force aanval wordt gekraakt, moet je het zo ingewikkeld mogelijk maken. Ook moet je nooit hetzelfde wachtwoord gebruiken. Een password manager kan hierbij helpen.

Er zijn drie technieken om achter persoonlijke gegevens te komen:

1. **Social engineering:** een niet-digitale techniek die gebruikmaakt van psychologische trucjes die mensen iets laten doen wat ze eigenlijk niet willen, zoals het vrijgeven van wachtwoorden. Ze doen zich vaak voor als iemand anders.
2. **Phishing:** een techniek die in combinatie met social engineering gebruikt kan worden. Slachtoffers worden hierbij bijvoorbeeld door middel van een mail naar een valse website gelokt waarbij ze hun wachtwoord moeten invullen.
3. **Malware:** alle programma's die ontwikkeld zijn met kwaadwillende bedoelingen. Vaak wordt malware gebruikt via aanvallen via een **zero day kwetsbaarheid.** Deze kwetsbaarheden zijn nog niet bekend bij de ontwikkelaar en daarom niet snel op te lossen.

De meest voorkomende soorten malware zijn:

- **Trojan horse:** vernoemd naar het paard van Troje. Gebruikers hebben namelijk niet door dat ze malware binnen halen via bijvoorbeeld een e-mail of chat bijlage of bij een download via een website. Het programma verspreidt zich niet. Het zal schade aanbrengen aan je systeem en het openzetten voor hackers.
- **Worm:** een worm verspreidt zichzelf automatisch door tussen alle computernetwerken en het internet door te 'wurmen'. Sommige wormen zijn niet gemaakt om schade aan te richten, toch zijn ze malware omdat ze geen toestemming hebben van de gebruiker. Een bekende worm uit het verleden is de 'ILOVEYOU' worm. Deze worm veranderde bestanden op het systeem en verspreidde zichzelf per e-mail. Hiervoor gebruikte de worm het adresboek van het mailprogramma Outlook. Automatisch verzond de worm een e- mail naar alle e-mailadressen in het adresboek, met zichzelf als bijlage.
- Sommige wormen hebben geen kwade bedoelingen, maar vragen wel altijd netwerkcapaciteit om zichzelf te verspreiden. Een worm heeft dus altijd een negatieve invloed op een computernetwerk.
- **Virus:** een virus is geen zelfstandig programma, maar het besmet een bestaande software. Het nestelt zich meestal in uitvoerbare bestanden of executables (bestanden waarmee je software opstart). De besmette software richt vervolgens schade aan en verspreidt zichzelf naar andere computers.
- Ook een worm nestelt zich meestal in een bestand. Het verschil met een virus is dat een worm zelf een compleet computerprogramma is.
- **Spyware:** probeert informatie over het computergebruik te achterhalen. Dit wordt vervolgens doorgegeven aan de maker van spyware. Ze kunnen bijvoorbeeld op zoek zijn naar geïnstalleerde programma's, bezochte websites, verstuurde e-mails of toetsenbordaanslagen. Spyware wordt iedere keer opgestart als een computer opnieuw wordt aangezet.
- **Adware:** het doel van adware is het weergeven van advertenties (ad staat voor advertentie). Het kan ook legaal zijn, bijvoorbeeld bij de installatie van shareware waarbij regelmatig een advertentie kan komen die aanspoort om de volledige versie van het programma aan te schaffen.
- Vaak wordt adware gebruikt om ongewenste reclames weer te geven. Vaak bevat adware ook technieken die in spyware zitten. Zo kan adware gerichte reclames aan de gebruiker voorschotelen.
- Spyware en adware worden vaak gezien als hetzelfde soort malware, maar ze hebben een andere functie, die in praktijk wel vaak gecombineerd wordt.
- **Ransomware:** een speciaal soort malware die een systeem binnendringt als Trojan horse/door middel van een worm. Als het eenmaal op een systeem staat, versleutelt het bestanden die hierdoor niet meer te gebruiken zijn. De gebruiker moet vervolgens geld betalen om weer toegang te krijgen tot het bestand. Er wordt over het algemeen aangeraden om niet te betalen omdat het niet zeker is dat je je toegang terugkrijgt en (internet)criminelen hierdoor aan geld komen. Ransomware is een van de nieuwste soorten malware.Bij ransomware-aanvallen wordt vaak gebruikgemaakt van tijdsdruk. Het slachtoffer moet snel betalen, anders vernietigen de aanvallers de data definitief of dreigen ze op een andere manier nog meer schade aan te richten. Daarom zijn slachtoffers vaak geneigd om te betalen zodat meer schade voorkomen kan worden. Criminelen komen daardoor eerder hun beloftes na en zo zorgen ze ervoor dat betalen de moeite waard is. Gelukkig vinden onderzoekers steeds vaker foutjes in de

ransomware, waardoor slachtoffers ook zonder betaling hun bestanden terug kunnen krijgen.

Aanvallers en verdedigers

Er zijn verschillende vormen van **computercriminaliteit/cybercrime:**

1. **Diefstal:** diefstal van data (bijvoorbeeld persoonlijke gegevens) kan gebeuren doordat een apparaat gehackt wordt of omdat er gegevens worden gestolen vanuit een database. Met deze data kan de dief **identiteitsfraude** plegen. Ook kan de data verkocht worden of kan je er mee afgeperst worden.
2. **Fraude:** een vorm van oplichting. Er wordt bedrog gepleegd, meestal met het doel om mensen geld afhandig te maken.
3. **Afpersing:** malware kan worden gebruikt voor afpersing. Maar ook met gevoelige gegevens (die van gestolen zijn) kan men afgeperst worden.

Computervredebreuk (digitaal inbreken) is een misdrijf. Ook het proberen of inbreken of het in bezit hebben van hulpmiddelen met het doel om te hacken is strafbaar.

Er zijn ook hackers die helpen om het internet veiliger te maken. Dit noem je **ethische hackers.** In plaats van indringen in een website door middel van een beveiligingslek, melden ethische hackers dit lek bij een betrokken bedrijf. Vaak krijgen ze hier een beloning voor.

Een beveiligingslek kan ook gevaarlijk zijn voor de gebruikers van de website; hun gegevens lopen gevaar. Hackers kiezen daarom vaak voor **responsible disclosure:** eerst wordt het lek gemeld bij de verantwoordelijke, daarna wordt het openbaar gemaakt om de gebruikers te waarschuwen. De verantwoordelijke moet hierdoor snel het lek oplossen en de hacker krijgt alle lof voor het vinden van de lek. Ethische hackers worden niet vervolgd omdat ze het internet veiliger maken en omdat het publiceren van informatie over gevaarlijke beveiligingsproblemen valt onder persvrijheid. Er zijn natuurlijk wel limieten in hoeverre hacken legaal is.

Zero day: een nog niet ontdekte kwetsbaarheid; een belangrijk middel om te hacken en daarom veel geld waard. Er wordt in gehandeld door criminelen maar ook door bedrijven. Zo kunnen ze dit lek dichten. Overheden maken gebruik van zero days om te spioneren. Ze kunnen zo vijandige systemen hacken en platleggen. Maar omdat overheden zero days blijven gebruiken, worden de lekken niet opgelost en wordt het internet een stukje onveiliger. Voor de Nederlandse overheid zijn er daarom zeer strikte voorwaarden omtrent het gebruiken van zero days.

Maatregelen

De maatregelen die gebruikers kunnen nemen om de veiligheid van een systeem te vergroten, kun je verdelen in vier soorten:

1. **Preventie:** hierbij worden maatregelen genomen om problemen te voorkomen. Dat begint bij goed ontworpen en onthouden hard-en software; zij hebben zo min mogelijk kwetsbaarheden. Encryptie van gegevens en het maken van back-ups vallen ook onder

preventieve maatregelen. Voor een bedrijf dat persoonsgegevens verwerkt, zijn preventieve maatregelen verplicht om de gegevens te beschermen.

2. **Detectie:** controle op misbruik. Hiervoor worden allerlei gegevens over het gebruik van een systeem gelogd. **Firewall** is een belangrijk hulpmiddel dat al het binnenkomende netverkeer scant op kwaadaardige gegevens en controleert of het verkeer afkomstig is van een vertrouwde bron. Een ander hulpmiddel is een **anti-malware software:** die scant een apparaat op malware en verwijdert die, door middel van databases met kenmerken van malware.
3. **Repressie:** het nemen van maatregelen nadat er een aanval of malware is aangetroffen.
4. **Correctie:** het herstellen van schade van een aanval of malware. Encryptie speelt een centrale rol in de beveiliging van gegevens.

Algoritme: de manier waarop encryptie werkt; elke letter wordt vervangen door een volgende letter uit het alfabet. Het aantal letters dat je vooruitschuift in het alfabet, is de **sleutel.** Door slimmer de sleutel te kiezen en het algoritme te verbeteren kan encryptie veiliger worden.

Symmetrische encryptie: encryptie die gebruikmaakt van één sleutel (zowel voor het versleutelen en ontsleutelen van de data). Omdat er maar één sleutel is, is het riskant om data te delen (en dus ook de sleutel te delen).

Asymmetrische encryptie: er is een **publieke sleutel** (versleuteld bericht) en een **geheime sleutel** (ontsleuteld bericht). Asymmetrische encryptie wordt bij vrijwel alle vormen van beveiligde data-overdracht gebruikt.

De absoluut noodzakelijke dingen die je als gebruiker kunt doen om de veiligheid te vergroten:

- Installeer updates direct
- Zorg voor automatische vergrendeling van je apparaat
- Gebruik sterke wachtwoorden
- Zorg voor back-ups van je apparaat/gegevens
- Controleer de verbinding en URL van een website waar je inlogt
- Download apps en software alleen van de play store, app store of van de website van een vertrouwde fabrikant
- Klik niet zomaar op gedeelde linkjes

Verstandig om te doen:

- Geef een app niet automatisch toegang als het om gegevens vraagt.
- Installeer anti-malware en anti-adware software
- Versleutel de gegevens als je data opslaat op een externe databron
- Wees voorzichtig met het aansluiten van zelf programmeerde apparaten op het internet. Ze zijn namelijk kwetsbaar voor automatische hacks.