1.1 - Inleiding

Digitale beveiliging is een overkoepelende term voor alle manieren waarop je eigen digitale identiteit beschermd kan worden. Het beveiligen van digitale gegevens gaat voornamelijk over drie aspecten:

- Vertrouwelijkheid: de afscherming van gegevens tegen ongeoorloofde inzage.
- Integriteit: bescherming van gegevens tegen verlies of (on)bedoelde wijzigingen.
- Beschikbaarheid: de mate van storingsvrije toegang tot de gegevens.

1.2 - Vertrouwelijkheid

Voordat er toegang is tot persoonlijke gegevens, is er een controle nodig om te kijken of de gebruiker wel toegang mag hebben. Dit proces wordt authenticatie genoemd. Er zijn verschillende vormen van authenticatie:

- Iets dat je weet: een pincode.
- Iets dat je hebt: een sleutel.
- Iets dat je bent: een vingerafdruk.

Behalve authenticatie worden ook de termen identificatie en verificatie gebruikt. Bij identificatie wordt er aan je gevraagd: ‘Wie ben je?’. Vervolgens vind er een verificatie plaats. Daarbij gaat het om: ‘Ben jij wie je zegt dat je bent?’. Verificatie kan alleen plaatsvinden als er gegevens van jou bekend zijn.

Voor meer veiligheid kunnen meerdere vormen van authenticatie samen gebruikt worden. Bijvoorbeeld met een pinpas. Je hebt iets nodig dat je hebt: een pinpas, en je hebt iets nodig dat je weet: een pincode. Deze combinatie heet two factor authentication.

Een techniek die verwant is aan authenticatie, identificatie en verificatie is screening. Bij screening worden personen of voertuigen geïdentificeerd. Bijvoorbeeld met camera’s.

1.3 - Integriteit

De rechten die een gebruiker heeft op bijvoorbeeld magister zijn verbonden aan diens rol. De gebruiker met de rol ‘docent’ heeft dus meer rechten dan de gebruiker met de rol ‘leerling’.

De controle welke rechten een vertrouwde gebruiker allemaal heeft, heet autorisatie. Dit heet ook de controle van de integriteit

Dit zijn de eisen die aan informatie gesteld worden:

Eis	**Controlevraag**

Volledigheid	Ontbreekt er iets?
Relevantie	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)?

Met de integriteit van gegevens en informatie bedoelen we dat de gegevens aan al deze eisen voldoen.

Integriteit betekent ook dat bepaalde (netwerk)schijven en mappen alleen beschikbaar zijn voor gebruikers met een specifieke rol. Om toegang te krijgen tot deze bestanden, hoeft er niet apart ingelogd te worden. Maar er moet wel autorisatie plaatsvinden: de controle of je toegang hebt. Die autorisatie kan door de systeembeheerder worden ingesteld via file permissions.

Als je installatiebestanden van programma's downloadt via het internet, zie je er soms een checksum bij staan. Deze checksum kun je zien als een vingerafdruk van het bestand. Daarmee kun je controleren of je exact, tot in de laatste bit, hetzelfde bestand hebt als het origineel.

Een andere manier om de integriteit van je data te garanderen, is het maken van back-ups. Mocht er door een onvoorziene oorzaak iets gebeuren met je data, dan is het altijd mogelijk om terug te gaan naar een situatie waarbij de data wel integer was.

Er zit een mechanisme in IBAN's dat typfouten kan voorkomen. Dat systeem heet het controlegetal, en 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.

1.3 - Beschikbaarheid

Data moet altijd beschikbaar zijn. Dit gaat niet vanzelf. Je zult hiervoor waarschijnlijk af en toe beveiligingsupdates moeten installeren. Of, indien nodig, defecte hardware-onderdelen vervangen. Er moet ook een back-up zijn. Dit kan bijvoorbeeld via een clouddienst, een USB-stick of een externe harde schijf.

Beveiligingsexperts raden aan om gebruik te maken van het 3-2-1-systeem voor back-ups. 3 kopieën van gegevens, op 2 verschillende manieren opgeslagen en waarvan 1 kopie op een andere locatie wordt bewaard.

Het opslaan van gegevens voor toegangscontrole brengt uitdagingen met zich mee. Stel je voor dat het hackers lukt om een database met wachtwoorden in te zien. niet alleen wachtwoorden en vingerafdrukken moeten zorgvuldig worden opgeslagen. Gevoelige bestanden kunnen versleuteld worden opgeslagen. Hiervoor wordt gebruikgemaakt van encryptie. Door middel van een sleutel, kan de inhoud van een bestand wiskundig worden ‘gehusseld’. Je hebt dus de sleutel nodig om het bestand normaal te kunnen zien. Encryptie kan ook gebruikt worden om communicatie geheim te houden.

Voor het opslaan van wachtwoorden, vingerafdrukken en dergelijke wordt gebruikgemaakt van hashing. Het wachtwoord wordt dan gehusseld. Alleen kan je bij hashing niet terug naar het origineel. Hoe weet een website dan dat je het juiste wachtwoord invoert wanneer je probeert in te loggen? Dat gebeurt door je wachtwoord nogmaals te hashen. Wanneer je inlogt, wordt er van het wachtwoord dat je opgeeft een hash gemaakt. Die hash wordt vergeleken met de hash in de database. Zijn de hashes gelijk aan elkaar, dan waren de wachtwoorden ook gelijk aan elkaar en mag je verder. Na het hashen wordt er dus niets met het oorspronkelijke wachtwoord gedaan.

Vingerafdrukken worden op smartphones in een apart deel van de hardware opgeslagen, waartoe andere processen geen toegang hebben. Leg je je vinger op de scanner, dan wordt aan dat aparte deel gevraagd of het een bekende vinger is. De apps krijgen je vingerafdruk nooit te zien.

Een DDoS-aanval is een gecontroleerde aanval om een service (tijdelijk) uit te schakelen. Bij zo’n aanval worden er vele duizenden aanvragen per seconde gedaan. Een website kan dit niet allemaal verwerken en zal crashen. DDoS-aanvallen kun je aanvragen tegen een betaling, maar het is heel strafbaar. Dit is omdat het vaak grote gevolgen heeft. Een aanval kan tegengegaan worden door het verkeer richting een website te filteren. Als er veel ongewenst verkeer is, kan er worden gekozen om het internetverkeer om te leiden naar een gespecialiseerde anti-DDoS-dienst.

2.1 - Inleiding

Aanvallers maken gebruik van verschillende zwakheden om toegang te krijgen tot digitale gegevens. In dit hoofdstuk gaat het over de volgende zwakheden:

- Zwakheden in architectuur.
- Zwakheden in communicatie.
- Zwakheden bij gebruikers.

2.2 - Zwakheden in architectuur

Een zwakheid in architectuur maakt gebruik van een tekortkoming in een van de drie lagen van het drielagenmodel. Een voorbeeld is de camera op je telefoon. Wanneer een app gebruik wil maken van je camera, verschijnt er eerst een pop-up waarin je toestemming moet geven. Het kan gebeuren dat er een manier wordt gevonden om de camera te

gebruiken zonder dat de pop-up verschijnt. Een aanvaller kan dan meekijken met je camera zonder dat je dat doorhebt.

Bij een lek in een website of app, heeft een kwaadwillende partij een zwakheid in de architectuur gevonden. Je kunt alle zwakheden verhelpen door de architectuur te testen. Je gaat dan zelf proberen de architectuur aan te vallen.

2.3 - Zwakheden in communicatie

Man-in-the-Middle aanval: De verbinding tussen twee apparaten kan worden afgeluisterd. Bijvoorbeeld als je een wachtwoord invult op een website, worden deze gegevens verzonden naar de website. Maar als er iemand tussen die verbinding zit, kan hij de gegevens ‘afluisteren’.

Met HTTPS wordt de verbinding beveiligd door middel van encryptie. Om dit mogelijk te maken, moet de beheerder van de website een SSL-certificaat installeren. Dat certificaat bevat gegevens over degene van wie de website is. Het certificaat moet door de beheerder van de website worden aangevraagd bij een centrale organisatie. Die organisatie geeft alleen certificaten uit aan mensen, instanties of bedrijven die bewezen hebben dat de website ook echt van hen is, bijvoorbeeld door ze een stukje code op de website te laten publiceren. Een webbrowser vertrouwt alleen certificaten die door zulke organisaties zijn uitgegeven. Dat laat hij zien met een hangslotje in de adresbalk.

Waar een HTTPS-verbinding alleen zorgt voor de beveiliging tussen de client en een server, gaat end-to-end encryption nog een stap verder.Bij een HTTPS-verbinding worden de gegevens versleuteld verstuurd tussen de client en de server. De server kan dus de oorspronkelijke, onversleutelde gegevens inzien en opslaan. Aanvallers maken maar hiervan al te graag gebruik door bijvoorbeeld op servers in te breken en de onversleutelde gegevens te stelen.End-to-end encryption versleutelt de gegevens nog voordat ze het internet op gaan, en ontsleutelt ze pas wanneer ze het internet verlaten. Alleen jij en de ontvanger kunnen ze ontsleutelen. Krijgt een hacker toegang tot de server, dan zal hij nooit de onversleutelde gegevens in kunnen zien. End-to-end encryption lost dus problemen als gevolg van zwakheden in de communicatie én zwakheden in de architectuur op!

2.4 - Zwakheden bij gebruikers

Een van de bekendste voorbeelden van zwakheden bij gebruikers is de manier waarop wij met wachtwoorden omgaan. Vaak worden er simpele wachtwoorden gekozen, die makkelijk gekraakt kunnen worden. Dit betekent dat een aanvaller elk mogelijk wachtwoord probeert om in te loggen op je account. Speciale programma’s zijn in staat om duizenden wachtwoorden per seconde te proberen. Dit heet brute force. Om te voorkomen dat je wachtwoord gekraakt kan worden, is het belangrijk om je wachtwoord zo ingewikkeld mogelijk te maken.

- Hoe meer tekens, hoe veiliger. Bij een lang wachtwoord is het al snel niet meer de moeite waard om er een brute force aanval op los te laten.

- Hoe meer soorten tekens, hoe veiliger. Hoe complexer het wachtwoord, hoe meer mogelijkheden een hacker moet inzetten om het ingewikkelde wachtwoord te vinden.
- Gebruik geen voor de hand liggende woorden, zoals woorden in een woordenboek, de naam van de website of je eigen naam of geboortedatum.
- Gebruik voor iedere website of dienst een ander wachtwoord.
- Pas je wachtwoorden minimaal één keer per jaar aan.

Je kunt een passwordmanager gebruiken om je wachtwoorden op te slaan.

2.5 - Technieken

Criminelen gebruiken verschillende technieken om achter persoonlijke gegevens te komen. Dit zijn drie veelgebruikte:

- Social engineering.
- Phishing.
- Malware.

Social engineering maakt gebruik van psychologische trucjes om mensen iets te laten doen wat ze eigenlijk niet willen doen, zoals het vrijgeven van gegevens of wachtwoorden. Aanvallers doen zich dan vaak voor als iemand anders. Slachtoffers kunnen bijvoorbeeld via een e-mail benaderd worden.

Phishing is een techniek die door criminelen gebruikt wordt in combinatie met social engineering. Met phishing worden slachtoffers, veelal via een e-mail, naar een valse website gelokt. Die e-mail en website zijn vaak nauwkeurig nagemaakt. Veelal gaat het om e-mails van banken, waarin staat dat er iets mis is met je rekening. Om het op te lossen moet je dan inloggen en iets herstellen. Maar in plaats van dat je bij je bank inlogt, log je in op een goed nagemaakte kopie, waar je verder niets kunt. Maar hierdoor hebben de aanvallers wel je inloggegevens!

2.6 - Malware

Malware is een samenvoeging van de woorden ‘malicious’ en ‘software’. Dit betekent ‘kwaadaardige software’. Het omvat alle programma’s die ontwikkeld zijn met kwaadwillende bedoelingen. Malware is er in verschillende vormen en soorten. De meest voorkomende zijn:

- Trojan horse
- Virus
- Worm
- Spyware
- Adware
- Ransomware

Vaak wordt malware gebruikt voor aanvallen via een zero day kwetsbaarheid. Dit zijn kwetsbaarheden in software die nog niet bekend zijn bij de ontwikkelaar.

Trojan horse, is een malware-soort die vernoemd is naar het paard van Troje. Bij deze soort malware hebben gebruikers niet door dat ze malware binnenhalen. Een trojan horse zal schade aanbrengen aan je systemen of het openzetten voor hackers.

Een Worm verspreid zich automatisch. Hij ‘wurmt’ zich door computernetwerken en het internet, en daardoor verspreidt hij zich. Sommige wormen zijn niet gemaakt om schade aan te richten. Het is toch een vorm van malware omdat het zonder toestemming van de gebruiker gebeurt.

Een virus is geen zelfstandig programma, zoals een worm. Het virus besmet bestaande software. Hij nestelt zich in uitvoerbare bestanden. Dat zijn de bestanden waarmee je software opstart. De besmette software richt vervolgens schade aan en verspreidt zichzelf naar andere computers.

Spyware is een type malware dat informatie over het computergebruik probeert te achterhalen. Spyware kan op zoek zijn naar bijvoorbeeld bezochte websites. Spyware zorgt ervoor dat het iedere keer wordt opgestart als een computer opnieuw wordt aangezet.

Adware is het weergeven van advertenties op je computer. Het wordt vaak gebruikt om ongewenste reclames te geven.

Ransomware is een speciaal soort malware, die vaak een systeem binnendringt zoals een trojan horse of een worm. Ransomware versleutelt bestanden, die daardoor niet meer te gebruiken zijn. Het slachtoffer krijgt dan een melding dat hij een geldbedrag moet betalen om toegang te krijgen tot de bestanden.Er wordt over het algemeen aangeraden om geen geld over te maken. Ten eerste omdat het helemaal niet zeker is dat je inderdaad de toegang tot je bestanden terugkrijgt. Ten tweede omdat ransomware hierdoor een lucratieve methode is voor (internet)criminelen om aan geld te komen.

3.1 - Inleiding

In de digitale wereld zijn er veel soorten aanvallers en verdedigers. Die spelen een kat- en muisspel: de verdedigers ontwikkelen steeds betere manieren van beveiliging, aanvallers verzinnen steeds nieuwe manieren om die te doorbreken.In dit hoofdstuk kijken we naar wat computercriminaliteit precies is. Daarna kijken we wat voor soorten aanvallers en verdedigers er zijn.

3.2 - Computercriminaliteit

De belangrijkste vormen van computercriminaliteit of cybercrime zijn diefstal, fraude, afpersing en inbraak (hacken).

Diefstal van data kan op veel manieren gebeuren. Als er diefstal is gepleegd, kan het gebeuren dat je daar helemaal niets van merkt. De gestolen data is vaak geld waard en kan worden doorverkocht. Ook kan er identiteitsfraude worden gepleegd. Afpersing is ook

mogelijk, dat is dat de crimineel dreigt om de persoonlijke gegevens openbaar te maken, tenzij je betaald.

Fraude is een vorm van oplichting. Er wordt bedrog gepleegd, meestal met het doel om mensen geld afhandig te maken. Een voorbeeld is Phishing.

Malware kan worden gebruikt voor afpersing, ransomware bijvoorbeeld. Ook kan de crimineel zelf het slachtoffer afpersen. Afpersen is dat de crimineel dreigt om de persoonlijke gegevens openbaar te maken, tenzij je betaald. Soms dreigt de crimineel, terwijl hij de data helemaal niet heeft.

3.3 - Computervredebreuk

De wet noemt hacken computervredebreuk. Er zijn aparte wetsartikelen voor computervredebreuk, die speciaal zijn gemaakt om allerlei vormen van criminaliteit te kunnen bestraffen. Maar wat is computervredebreuk precies? Het is het ongeoorloofd binnendringen in een computersysteem of een netwerk.

Niet alleen het binnendringen is strafbaar, maar ook een poging wagen tot het binnendringen is strafbaar.

Ook het bezitten van hulpmiddelen met het doel om te hacken is strafbaar. Als je alleen hacksoftware hebt, is dat dus al strafbaar.

3.4 - Ethisch hacken

En zijn allerlei hackers actief die helpen om het internet veilig te maken. Dit zijn Ethische hackers. Zij melden een beveiligingslek aan het betrokken bedrijf, zodat zij het kunnen oplossen. Vaak maakt het bedrijf het niet openbaar, zodat hackers niet op de hoogte worden gesteld van het lek.

Er zijn ook bedrijven die een beveiligingsprobleem niet of niet snel genoeg oplossen als het is gemeld. Ook dat is gevaarlijk, want gebruikers kunnen slachtoffer worden van het lek. Daarom is het soms verstandig om een lek wel openbaar te maken: de gebruikers worden zo gewaarschuwd.

De meeste hackers kiezen voor een tussenvorm: responsible disclosure. Eerst wordt het beveiligingslek gemeld bij degene die ervoor verantwoordelijk is. Na een bepaalde periode maakt de hacker het lek openbaar. Zo slaat de hacker twee vliegen in één klap. De verantwoordelijke wordt gedwongen het probleem snel op te lossen en de hacker krijgt alle eer voor het vinden van het lek.

Ook ethische hackers overtreden de wet door te hacken. Toch zullen ze niet worden vervolgd. Dat komt omdat ze een publiek belang dienen: het internet wordt er veiliger van. Maar dat is niet de enige reden waarom ze niet vervolgd worden. Het publiceren van informatie over gevaarlijke beveiligingsproblemen valt onder de persvrijheid. Het maakt

daarbij niet uit of je journalist bent of niet. 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 onnodig gegevens steelt of onnodig veel computers hackt, word je daar wel voor vervolgd.

3.5 - Spionage en oorlogsvoering

Een zero day is een nog niet ontdekte kwetsbaarheid, die veel geld waard is. Je kunt zero days beschouwen als de wapens van de digitale oorlogsvoering en de verkoop ervan als een vorm van wapenhandel. Want met zero days kunnen schadelijke aanvallen worden uitgevoerd, gegevens gestolen en systemen worden platgelegd.

Criminelen zijn geïnteresseerd in zero days, maar ook beveiligingsbedrijven kopen ze met het doel om de lekken te dichten. Ook overheden gebruiken ze, om te spioneren.

4.1 - Inleiding

Om veiligheid van ICT-systemen goed te maken en te houden, zijn er veel partijen nodig die zich daarvoor inzetten: cybersecuritybedrijven, de overheid, softwareontwikkelaars en zeker ook de gebruikers. Er zijn vier soorten maatregelen die genomen kunnen worden om veiligheid te vergroten: preventie, detectie, repressie en correctie.

4.2 - Preventie

Preventieve beveiligingsmaatregelen zijn de maatregelen die worden genomen om problemen te voorkomen. Dat begint bij hard- en software.

Ook is encryptie goed om het te voorkomen, als de data in verkeerde handen valt, kan de crimineel er niets mee tenzij hij de sleutel heeft.

Het maken van back-ups is een belangrijke preventieve stap in de bescherming tegen verlies of onbedoelde wijziging van data.

Wanneer een bedrijf persoonsgegevens verwerkt, is het wettelijk verplicht preventieve maatregelen te nemen om de gegevens te beschermen. Dat is vastgelegd in de Europese privacywetgeving. Verder moet het bedrijf uitleggen hoe het de gegevens beschermt.

4.3 - Detectie

Er zullen altijd kwetsbaarheden in zitten die kunnen worden misbruikt. Daarom is detectie nodig: controle op misbruik. Bijvoorbeeld door bij te houden hoe vaak er een inlogpoging wordt gedaan met een bepaalde gebruikersnaam. Als dat te vaak is, kan de gebruiker worden geblokkeerd. Een belangrijk hulpmiddel is de firewall, die scant al het binnenkomende netwerkverkeer. De data wordt dan gecontroleerd op kwaadaardige

gegevens. Ook kan een firewall controleren of het verkeer afkomstig is van een vertrouwde bron.

Ook is anti-malwaresoftware een belangrijk detectiehulpmiddel. Die scant een apparaat op malware en verwijdert die.

4.4 - Repressie en correctie

Als er sprake is van een aanval of als er malware is aangetroffen, moeten er maatregelen worden genomen (repressie) en moet eventuele schade worden hersteld (correctie).

Als er malware is aangetroffen, kan het voldoende zijn als die verwijderd wordt door anti-malwaresoftware. Een DDoS-aanval die niet sterk genoeg is, kan tijdelijk zorgen voor een iets tragere website. En als een server niet meer beschikbaar is vanwege beschadigde data, een hackpoging of malware, kan er worden overgeschakeld op een back-upsysteem. Het beveiligingslek moet dan wel zo snel mogelijk worden gedicht.

Als de problemen serieuzer zijn, zullen er systemen uitvallen of moeten worden uitgezet. Om bijvoorbeeld te voorkomen dat data in verkeerde handen valt.

4.5 - Symmetrische encryptie

Het versleutelen van gegevens is belangrijk om te voorkomen dat het in verkeerde handen komt. Encryptie is in alle tijden toegepast. Stel dat je elke letter verandert door de letter die drie plaatsen verder in het alfabet staat. Dan wordt elke a een d, elke b een e, enzovoorts. Het woord encryptie wordt dan hqfubswlh. Je kunt er ook voor kiezen om niet drie, maar vijf letters verderop te kiezen: elke a wordt dan een e, b een f, enzovoorts. dit is Caesar-encryptie. Het aantal letters dat je vooruit schuift in het alfabet, is de sleutel.

De aanvaller probeert dankzij de encryptie vaak het originele bericht te vinden. Er zijn een paar oplossingen: De sleutel kan slimmer gekozen worden, waardoor het zo veel tijd kost om de sleutel te vinden dat het de moeite niet waard is. Ook kan het algoritme verbeterd worden, zodat het heel moeilijk wordt om te kraken.

Encryptie die gebruikmaakt van één sleutel, heet symmetrische encryptie. Die sleutel wordt zowel gebruikt voor het versleutelen als het weer ontsleutelen van de data. Een van de bekendste symmetrische encryptie-algoritmen is Advanced Encryption Standard (AES). Dit wordt bijvoorbeeld gebruikt om bestanden op een opslagmedium te versleutelen.

4.6 - Asymmetrische encryptie

Als je versleutelde data verstuurd, heeft de ontvanger de sleutel nodig om het bericht te ontsleutelen. Het transporteren van de sleutel is riskant, want die kan worden onderschept.

Om dit probleem op te lossen, is asymmetrische encryptie bedacht. Dit wordt ook wel public key encryptie genoemd. Bij deze vorm van encryptie zijn er twee sleutels: een publieke

sleutel en een geheime sleutel. Met de publieke sleutel wordt een bericht versleuteld. Met de geheime sleutel kan het versleutelde bericht weer worden ontsleuteld. Iedereen mag de publieke sleutel weten. Dat is geen probleem, want je versleutelt er alleen maar mee. De geheime sleutel wordt nooit verspreid.

4.7 - Wat kun je zelf doen?

Dit zijn absoluut noodzakelijke maatregelen om je veiligheid te verbeteren:

- Installeer updates meteen.
- Zorg voor automatische vergrendeling van je smartphone, tablet en computer.
- Gebruik sterke wachtwoorden en vervang ze minimaal 1x per jaar.
- Zorg voor back-ups.
- Controleer of je een beveiligde verbinding hebt op een website.
- Download apps en andere software alleen vanuit de play store, app store of van de website van een betrouwbare fabrikant.
- Klik niet zomaar op gedeelde linkjes op social media, whatsapp of e-mails.

Deze maatregelen zijn verstandig om te nemen:

- Klik niet meteen op ‘ja’ als een app om toegang vraagt tot bepaalde gegevens op je smartphone.
- Installeer anti-malware- en anti-adwaresoftware op je computer en stel in dat deze je apparaat regelmatig scannen.
- Als je data opslaat op een externe databron, zoals een externe harde schijf of USB-stick, versleutel dan de gegevens.
- Wees heel voorzichtig met het (permanent) aansluiten van zelfgeprogrammeerde apparaten op het internet, zoals een Arduino en Raspberry Pi. Deze apparaten zijn heel kwetsbaar voor automatische hacks.