MFA: nodig, maar niet zaligmakend

In deze richtlijn legt de VTC in een eerste deel uit wat MFA en MFA-omzeiling inhouden. Daarna geeft ze in deel II een overzicht van mogelijke extra beveiligingsmaatregelen bovenop MFA. In de delen III en IV stelt ze maatregelen voor die respectievelijk de systeembeheerder en de gebruiker kunnen nemen.

DEEL I: MFA en MFA-omzeiling in het kort

Wat is MFA weer?

Als je een online account beveiligt met (enkel) een gebruikersnaam en een wachtwoord (of PIN), heeft een hacker er genoeg aan om je wachtwoord (of PIN) te raden als het eenvoudig is, te berekenen als het kort is, zelf te stelen of je wachtwoord op te zoeken in gestolen wachtwoordenlijsten.

Daarom werd er tweetrapsverificatie (2FA) of meerfactorauthenticatie (MFA) ingevoerd. Daarbij is bv. je wachtwoord factor 1 en neem je er een (2FA) of meer (MFA) extra factoren bij. Die extra factoren zijn dan bij voorkeur telkens een factor uit een andere van de volgende categorieën:

- iets wat je als enige **weet**: bv. wachtwoord, pincode, antwoord op beveiligingsvragen;
- iets wat je als enige **hebt**: bv. je bankkaart, je identiteitskaart, een fysieke beveiligingssleutel (speciale (usb-)stick), je GSM waarop je een tijdelijke code ontvangt;
- iets wat je uniek **bent**: bv. vingerafdruk, irisscan, gezicht;

Het is dan heel moeilijk voor een hacker om over de combinatie van deze factoren te beschikken. Maar, …

Veiligheid van de tweede factor

Niet elke toegevoegde factor is even veilig. Hierna bespreken we er enkele:

- wat je **weet:**
  - er zijn stemmen die verdedigen dat paswoorden volledig achterhaald zijn om de vermelde redenen, maar er zijn ook experten die zeggen dat een (lang[1]) paswoord het enige is wat niet na te maken is;
- wat je **hebt:**
  - SMS/telefoon: hoewel gemakkelijk te gebruiken, zijn SMS-codes gevoelig voor sim-swapping en phishing-aanvallen (zie verder);

[1] Door de mogelijkheid van quantumcomputing zal het nog wat langer moeten zijn.

    - Authenticator Apps, zoals Google Authenticator, Microsoft Authenticator of Authy: deze zijn veiliger dan SMS, omdat ze werken op basis van tijdsgebonden codes (TOTP) en niet afhankelijk zijn van de telecommunicatie-infrastructuur;
    - Hardware Tokens, bijvoorbeeld YubiKeys of RSA SecurID: deze bieden een zeer hoge mate van veiligheid, omdat ze beveiligde fysieke apparaten zijn die moeilijk te kopiëren zijn.
- wat je **bent**:
    - Biometrische Methoden: Zoals vingerafdruk- of gezichtsherkenning. Deze zijn moeilijk (niet onmogelijk) te vervalsen, maar kunnen kwetsbaar zijn voor spoofing en vereisen nauwkeurige implementatie om effectief te zijn.

De verwerkingsverantwoordelijken moeten dus nadenken over de toegestane methodes om een 2de of volgende factor te gebruiken. Afhankelijk van wat kan en mag, zal men al dan niet kwetsbaar zijn voor een bepaalde techniek.

Technieken om MFA te omzeilen

Bij enkele recente datalekken die bij de VTC gemeld werden, werd vastgesteld dat er wel degelijk MFA was geïmplementeerd, maar dat die toch omzeild kon worden. Dat geldt (voorlopig?) voor de MFA-beschermingen van zowel Google als Microsoft 365.

De technieken die hiervoor gebruikt werden, bestonden al, maar nu MFA algemener wordt, worden ze ook meer gebruikt door hackers.

2FA kan omzeild worden op de volgende manieren:

- **accountovername**: bij overname van een e-mailaccount kan de hacker ook aan paswoorden/codes die soms (als extra beveiliging) naar je e-mailaccount worden gestuurd;

- **malware**: hackers installeren software om je toestel te infecteren De malware kan op verschillende manieren worden geïnstalleerd. Daarmee kunnen ze de controle van het toestel (PC, GSM, …) overnemen en de codes die daarop staan achterhalen;

- **social engineering:** de hacker stuurt misleidende berichten naar de gebruiker om die te overtuigen diens 2FA-code door te geven. De hacker probeert zich meestal voor te doen als een bekende persoon of organisatie. Zie hierna over **phishing.**

- **MFA-moeheid** (*push bombing):* vorm van social engineering: herhaaldelijk autorisatieverzoeken versturen tot de gebruiker in een vlaag van vermoeidheid of onoplettendheid zijn identiteit bevestigt;

- **sim-swapping**: de hacker doet alsof hij jou is en overtuigt uw mobile provider om een nieuwe simkaart te activeren, namelijk die van de hacker. De hacker heeft dan toegang tot al uw gegevens op de GSM inclusief de codes die naar uw nummer worden gestuurd.

MFA omzeilen bij phishing

Via phishingtechnieken hengelt de hacker naar je codes. De hacker probeert je te misleiden door op je in te praten (of schermen te tonen) en zich voor te doen als een betrouwbare partij, bijvoorbeeld een bank of een ander lokaal bestuur. Bij MFA-omzeiling laat hij je eerst je MFA-factoren gebruiken en neemt het dan of eigenlijk tegelijk over.

Om zich als een betrouwbare partij/website/inlogscherm voor te doen, bestaan er verschillende technieken. Deze zijn makkelijk te verkrijgen, relatief gebruiksvriendelijk en als ze gecombineerd worden ook moeilijk te detecteren. Het helpt als je weet hoe het werkt.

Voor het phishen gebruikt de hacker een **phishingtool**. Daarmee worden de mails of smssen verstuurd en de reactie van de ontvangers gemonitord.

Met een reverse proxy tool voert de hacker een zogenaamde **Man-in-the-Middle** (MITM) attack uit. Hij presenteert de gebruiker een kopie van een legitieme website en zet zich zo tussen de gebruiker en die website. Hij kan daardoor zowel de inloggegevens die de gebruiker invoert als de sessiecookies die de legitieme website teruggeeft gebruiken. Een oplettende[2] gebruiker zou nog kunnen opmerken dat de URL niet die van de legitieme website is.

Door de **sessiecookies** die de legitieme authenticatortool aan de gebruiker geeft te kopiëren kan de hacker zich met de gekopieerde sessiecookie aanmelden op de bestaande sessie van het slachtoffer zonder opnieuw te moeten aanmelden. Hij zou dit anders niet kunnen omdat hij niet over alle factoren beschikt (factoren “hebben” en “zijn”). De hacker krijgt zo toegang tot de account van het slachtoffer en alles waarmee deze daarmee toegang heeft en het slachtoffer merkt in eerste instantie niets.

Om het slachtoffer nog beter te misleiden, kan de hacker nog een andere aanvullende techniek gebruiken, **Browser-in-the-Browser**, waarvoor ook tools bestaan. Daarmee wordt op een valse landingspagina[3] een perfect nagemaakte valse inlogpagina[4] met een URL die op de oorspronkelijke lijkt (en zelfs het geruststellende ssl-slotje) boven de legitieme geplaatst.

In de bijlage wordt deze aanval via vergelijkingen verder uitgelegd.

MFA combineren met andere maatregelen

MFA blijft belangrijk, en is in de praktijk een effectief middel om de meeste aanvallen af te weren; maar MFA toepassen zal dus niet steeds voldoende zijn. Je moet bijkomend andere beveiliging inbouwen. Zie verder in de volgende delen.

[2] In gevallen van en op een specifieke persoon of functie gerichte phishing (spearphishing), kan de gebruiker afgeleid worden en onder druk gezet worden door deze tegelijk ook op te bellen.
[3] De pagina waar je denkt terecht te zullen komen als je op de link klikt, zodat je niet verontrust bent.
[4] Een inlogpagina die vertrouwd overkomt.

DEEL II: Extra beveiligingsmaatregelen bij MFA

MFA-methoden die gebruik maken van extra stappen, zoals het presenteren van een extra nummer of symbool dat de gebruiker moet aanduiden, voegen een extra laag beveiliging toe. Deze extra stappen zijn ontworpen om de authenticatie veiliger te maken door een element van interactie of extra verificatie toe te voegen dat moeilijker te omzeilen is voor aanvallers. Hieronder beschrijf ik enkele van deze methoden en hun werking:

Nummerverificatie (Number Matching):

- **Beschrijving:** bij nummerverificatie wordt een nummer (meestal een 2- of 3-cijferig getal) weergegeven op het scherm van de gebruiker tijdens het inlogproces. De gebruiker moet dit nummer invoeren of selecteren op een tweede apparaat (zoals een mobiele telefoon met een authenticator-app) om de authenticatie te voltooien.
- **Werking:** wanneer de gebruiker probeert in te loggen, ziet hij een nummer op het scherm. De gebruiker opent de authenticator-app, waar hij het overeenkomstige nummer moet invoeren of bevestigen.
- **Voordelen:** deze methode zorgt ervoor dat een aanvaller niet alleen toegang moet hebben tot de inloggegevens, maar ook fysieke toegang tot het tweede apparaat van de gebruiker.
- **Voorbeeld:** Microsoft Authenticator app gebruikt nummerverificatie bij het inloggen.

Symboolverificatie (Symbol Matching):

- **Beschrijving:** bij symboolverificatie wordt een symbool of een reeks symbolen weergegeven op het scherm van de gebruiker. De gebruiker moet hetzelfde symbool of dezelfde symbolen selecteren of invoeren op een tweede apparaat.
- **Werking:** tijdens het inlogproces ziet de gebruiker een symbool (bijvoorbeeld een pictogram of een kleurcode) op het scherm. De gebruiker moet dit symbool op zijn authenticator-app selecteren of bevestigen.
- **Voordelen:** het gebruik van symbolen maakt het moeilijker voor aanvallers om de juiste informatie te raden of te verkrijgen, vooral bij social engineering aanvallen.
- **Voorbeeld:** Authenticator-apps zoals Duo kunnen symboolverificatie gebruiken.

Push-Notificaties met Extra Informatie:

- **Beschrijving:** bij deze methode ontvangt de gebruiker een push-notificatie op een mobiel apparaat met extra informatie zoals het IP-adres, locatie of apparaatdetails van de inlogpoging. De gebruiker moet deze informatie controleren en de inlogpoging goedkeuren of afwijzen.
- **Werking:** wanneer een inlogpoging wordt gedaan, ontvangt de gebruiker een push-notificatie met details van de inlogpoging. De gebruiker controleert deze details en keurt de poging goed of af.
- **Voordelen:** dit maakt het voor aanvallers moeilijker om in te loggen zonder dat de gebruiker het opmerkt, omdat de gebruiker details over de inlogpoging moet bevestigen.
- **Voorbeeld:** Duo Security en Okta bieden deze functie aan.

Biometrische Verificatie:

- **Beschrijving:** deze methode gebruikt biometrische gegevens zoals vingerafdrukken, gezichtsherkenning of irisscans als extra verificatiestap.
- **Werking:** na het invoeren van de inloggegevens moet de gebruiker zijn biometrische gegevens verstrekken om de authenticatie te voltooien.
- **Voordelen:** biometrische gegevens zijn uniek voor elke gebruiker en moeilijk te vervalsen, wat een zeer hoge mate van beveiliging biedt.
- **Voorbeeld:** Apple's Face ID en Touch ID, en Windows Hello.

Tijdsgebaseerde Eenmalige Wachtwoorden (TOTP) met Extra Stap:

- **Beschrijving:** naast de standaard TOTP-methode kunnen extra stappen worden toegevoegd, zoals het invoeren van een PIN-code of het bevestigen van een visuele cue (zoals een afbeelding).
- **Werking:** de gebruiker genereert een eenmalige wachtwoordcode met een authenticator-app en moet daarnaast een extra PIN-code invoeren of een afbeelding bevestigen.
- **Voordelen:** de extra stap verhoogt de beveiliging door een extra laag verificatie toe te voegen.
- **Voorbeeld:** Google Authenticator kan worden gecombineerd met extra beveiligingsvragen of PIN-codes.

Conclusie van dit deel

Het gebruik van extra stappen in MFA-methoden, zoals nummerverificatie, symboolverificatie, push-notificaties met extra informatie, biometrische verificatie, en TOTP met extra stappen, **verhoogt de algehele beveiliging door aanvallers te dwingen meerdere vormen van verificatie te omzeilen**. Deze methoden zijn effectief omdat ze een aanvullende controle toevoegen die moeilijk te repliceren is zonder toegang tot meerdere vertrouwelijke gegevens van de gebruiker.

DEEL III: Voor de systeembeheerder

Als systeembeheerder zijn er verschillende adviezen die je kunt volgen om je te beschermen tegen aanvallen op Multi Factor Authenticatie (MFA). Hier zijn enkele belangrijke maatregelen en adviezen:

Opsomming maatregelen

Gebruik Robuuste MFA-methoden:

- **Authenticator Apps:** Gebruik apps zoals Google Authenticator, Authy, of Microsoft Authenticator die tijdgebaseerde eenmalige wachtwoorden (TOTP) genereren.
- **Hardware Tokens:** Overweeg fysieke beveiligingssleutels zoals YubiKeys die FIDO2 of U2F ondersteunen.
- **Biometrische Verificatie:** Integreer biometrische methoden (vingerafdruk, gezichtsherkenning) waar proportioneel.

Bewustwording en Training:

- **Regelmatige Training:** Zorg ervoor dat alle gebruikers bewust zijn van de risico's van phishing en social engineering, en hoe ze verdachte activiteiten kunnen herkennen.
- **Simulaties:** Voer regelmatig phishing-simulaties uit om gebruikers alert te houden.

Veiligheidsbeleid en Procedures:

- **Sterke Wachtwoordbeleid:** Dwing het gebruik van sterke, unieke wachtwoorden af en gebruik wachtwoordmanagers.
- **Wachtwoordrotatie:** Zorg voor periodieke wachtwoordrotatie en minimaliseer hergebruik van wachtwoorden.
- **Accountvergrendeling:** Implementeer accountvergrendeling na een aantal mislukte inlogpogingen.
- **Credential Leak Monitoring:** Het monitoren van credential leaks helpt bij het snel reageren op datalekken en gestolen inloggegevens.

Technische Maatregelen:

- **HTTPS en HSTS:** Gebruik HTTPS voor alle communicatie en implementeer HTTP Strict Transport Security (HSTS) om alleen HTTPS-verbindingen toe te staan.
- **Zero Trust Architectuur:** Adopteer een Zero Trust-beveiligingsmodel waarbij geen enkele entiteit wordt vertrouwd zonder verificatie.
- **Contextuele en Adaptieve MFA:** Gebruik contextuele gegevens (zoals locatie, tijdstip, apparaat) om adaptieve MFA te implementeren die alleen MFA vereist wanneer het risico verhoogd is.

Netwerkbeveiliging:

- **Netwerksegmentatie:** Segmenteer je netwerk om laterale bewegingen van aanvallers te beperken.

- **Intrusion Detection and Prevention Systems (IDPS):** Gebruik IDPS om verdachte activiteiten te detecteren en te blokkeren.

Monitoring en Incident Response:

- **Security Information and Event Management (SIEM):** Implementeer een SIEM-systeem om real-time analyses van beveiligingswaarschuwingen te bieden en proactief te reageren op bedreigingen.
- **Credential Leak Monitoring:** Monitor het internet en dark web voor gelekte inloggegevens van je organisatie.
- **Incident Response Plan:** Zorg voor een gedetailleerd incident response plan voor het geval van een beveiligingsincident.

Software- en Systeembeheer:

- **Regelmatige Updates:** Houd alle software en systemen up-to-date met de laatste beveiligingspatches.
- **Verwijder Ongebruikte Accounts:** Verwijder of deactiveer accounts die niet meer in gebruik zijn om het aanvalsoppervlak te verkleinen.

Geavanceerde Beveiligingstools:

- **Advanced Threat Protection (ATP):** Gebruik ATP-oplossingen om geavanceerde aanvallen te detecteren en te voorkomen.
- **Endpoint Detection and Response (EDR):** Implementeer EDR om bedreigingen op eindpunten te detecteren en te reageren.

Gebruik authenticatorapps die het gebruik van sessiecookies beveiligen

Deviceless MFA (browser token) gebruiken:

Dit token kan verifiëren of de URL legitiem is en een niet legitieme blokkeren;

Wachtwoordloos inloggen mogelijk maken eventueel.

Praktisch

Schema

Hier is een overzicht van aanvullende maatregelen die je kunt nemen, samen met een beoordeling van hun effectiviteit:

Maatregel	Beschrijving	Effectiviteit
Opleggen van Authenticatiemethodes	Dwing af welke MFA-methodes wel en niet mogen worden gebruikt (bijv. geen SMS, alleen authenticator apps of hardware tokens). Sommige leveranciers bieden deze mogelijkheid aan in hun beheerdersconsoles.	**Hoog**: Zorgt voor consistent gebruik van sterke MFA-methoden en voorkomt het gebruik van minder veilige opties.
Tijdsverloop van Her-verificatie	Stel een tijdslimiet in voor hoe vaak gebruikers opnieuw moeten verifiëren tijdens een sessie (bijv. elke 8 uur).	**Hoog**: Vermindert het risico van langdurige sessies die kunnen worden gekaapt. In praktijk duurt het soms heel lang voordat de gebruiker opnieuw moet her-identificeren. Zo blijft de browser dagen/weken en soms maanden aangemeld zonder her-authenticatie. Soms zie je dat men dit instelt per risicoprofiel. Zo moeten gastaccounts sneller opnieuw aanmelden dan andere gebruikers.
Beperken van Mogelijke Tools van Eindgebruikers	Beperk welke browsers en applicaties mogen worden gebruikt voor toegang tot bedrijfssystemen (bijv. alleen goedgekeurde browsers).	**Hoog**: Verkleint het aanvalsoppervlak door ervoor te zorgen dat alleen beveiligde en gecontroleerde software wordt gebruikt. Concreet verplicht je dat de gebruiker enkel via een beperkte set softwareproducten kan aanmelden. Zo kan de gebruiker niet aanmelden met een andere browser dan deze die door de systeembeheerder is weerhouden. Samen met bijvoorbeeld het opleggen van plug-ins kan dit effectief zijn.
Copy/Pasten tussen Bedrijfs- en Privé Applicaties	Leg beperkingen op voor het kopiëren en plakken tussen bedrijfsapplicaties en privé applicaties om gegevensverlies te voorkomen.	**Middelmatig**: Verhoogt de gegevensbeveiliging, maar kan de gebruikerservaring beïnvloeden. Daardoor kunnen sessies niet eenvoudig uit de bedrijfsomgeving worden gekopieerd.

Details en Implementatie

1. Opleggen van Authenticatiemethodes:
    - **Implementatie:** Gebruik een centrale beheerconsole om policies te configureren die specifieke MFA-methoden afdwingen.
    - **Effectiviteit:** Verhoogt de veiligheid aanzienlijk door alleen robuuste authenticatiemethoden toe te staan.
2. Tijdsverloop van Her-verificatie:
    - **Implementatie:** Configureer sessie time-outs en herverificatie-intervallen in de beveiligingsinstellingen van applicaties.
    - **Effectiviteit:** Verhoogt de beveiliging door regelmatig herverificatie te vereisen, wat de kans op sessiekaping vermindert.
3. Beperken van Mogelijke Tools van Eindgebruikers:
    - **Implementatie:** Gebruik beleidsregels en tools voor apparaatbeheer (MDM, Group Policies) om te bepalen welke browsers en tools zijn toegestaan.
    - **Effectiviteit:** Verkleint het aanvalsoppervlak en zorgt ervoor dat alleen veilige, bijgewerkte software wordt gebruikt voor toegang tot bedrijfsbronnen.
4. Copy/Pasten tussen Bedrijfs- en Privé Applicaties:
    - **Implementatie:** Gebruik Data Loss Prevention (DLP) oplossingen om te controleren en beperken wat kan worden gekopieerd of geplakt tussen applicaties.
    - **Effectiviteit:** Vermindert het risico op datalekken, maar kan de productiviteit beïnvloeden als het te streng wordt toegepast.

Aanvullende Maatregelen:

1. Apparaatbeheer en -beperkingen:

    - **Beschrijving:** Dwing af dat alleen goedgekeurde en beheerde apparaten toegang hebben tot bedrijfsgegevens.
    - **Effectiviteit: Hoog**: Zorgt ervoor dat alleen veilige en gecontroleerde apparaten toegang hebben tot bedrijfsbronnen.

2. Contextuele en Adaptieve MFA:

    - **Beschrijving:** Implementeer contextuele verificatie, waarbij gebruikers extra verificatie moeten doorlopen als hun gedrag afwijkt van het normale patroon.
    - **Effectiviteit: Hoog**: Verhoogt de beveiliging door risicovolle aanmeldpogingen te identificeren en extra verificatie te vereisen.

3. Gebruik van Geavanceerde Browserbeveiliging:

    - **Beschrijving:** Gebruik browserextensies of instellingen die verdachte websites en phishing-aanvallen kunnen detecteren en blokkeren.
    - **Effectiviteit: Middelmatig**: Verbetert de beveiliging door gebruikers te beschermen tegen bekende bedreigingen tijdens het browsen.

DEEL V: Tips voor de gebruikers

Volgende tips pas je best gecombineerd toe:

- **lees de uitleg** over MFA-omzeiling in deel I;
- niet zonder meer op toegestuurde links klikken, maar naar originele website gaan (plaats op tijd een **bladwijzer**);
- niet reageren op **onverwachte** berichten;
- vermijd zeker om te reageren op **ongevraagde** berichten die je vragen om 2FA-codes te delen. Je 2FA-codes alleen delen op het moment dat je inlogt op je account;
- blijf de **URL** van de website en het mailadres controleren op anomalieën (bv. dubbele letters), ook als ze op het eerste zicht bekend voorkomen (bv. met “login” beginnen);
- als je twijfelt, **stop** en contacteer dan de mogelijke verzender op een veilige manier (een al van voor het bericht bekend telefoonnummer bv.);
- als je twijfelt, **stop** en haal de IT, de DPO of een collega erbij;
- gebruik een **authenticator app**: dit is niet sluitend, maar beter dan codes laten smssen of via mail laten versturen omdat die app lokaal werkt en zo moeilijker te hacken is.

↑↑↑↑↑

BIJLAGE: MiTM en MiTB anders uitgelegd

Man-in-the-Middle

Stel je voor dat je een brief wilt sturen naar je bank om een belangrijke transactie te regelen. Hier zijn de stappen bij een in de echte wereld vergelijking:

1. **de Gebruiker (jij)** schrijft een brief met vertrouwelijke informatie en steekt deze in een envelop met het adres van de bank erop.
2. **de Hacker** (een postbode die kwaad in de zin heeft) onderschept de brief voordat deze bij de bank aankomt.
3. **de Hacker** opent de envelop, leest de vertrouwelijke informatie en maakt een exacte kopie van de brief (voor het verkrijgen van een zegel van de bank – zie hierna over sessiecookies) .
4. **de Hacker** stuurt een valse brief naar jou terug met de naam en het adres van de bank, maar deze brief wordt door de hacker geschreven en bevat instructies om gevoelige informatie terug te sturen.
5. **de Gebruiker (jij)** ontvangt de valse brief en denkt dat deze echt van de bank komt. Je volgt de instructies en stuurt je vertrouwelijke informatie naar het adres dat in de valse brief staat.
6. **de Hacker** onderschept deze informatie opnieuw en gebruikt deze om toegang te krijgen tot je bankrekening of om transacties uit te voeren.
7. **de Echte Bank** ontvangt nooit de oorspronkelijke brief en is zich niet bewust van de communicatie die jij hebt gehad met de hacker.

In deze vergelijking:

- **de Gebruiker** is de persoon die probeert toegang te krijgen tot de legitieme website.
- **de Brief** vertegenwoordigt de inloggegevens en vertrouwelijke informatie.
- **de Hacker** is de tussenpersoon die de communicatie onderschept en vervalst.
- **de Valse Brief** is de kopie van de legitieme website die de hacker presenteert aan de gebruiker.
- **de Echte Bank** is de legitieme website.

Een oplettende gebruiker zou kunnen opmerken dat de brief er anders uitziet dan de normale correspondentie van de bank, net zoals een oplettende internetgebruiker kan opmerken dat de URL van de valse website niet overeenkomt met de legitieme website.

Stelen van Sessiecookies

Vergelijking met in het echte leven:

1. **de Gebruiker (jij)** stuurt een brief naar de bank met een verzoek voor een belangrijke transactie.

2. de Hacker (een kwaadaardige postbode) onderschept de brief, opent deze en leest de vertrouwelijke informatie.
3. de Hacker maakt een kopie van de brief, plaatst de originele brief terug in de envelop en stuurt deze door naar de bank.
4. de Bank ontvangt de originele brief, verwerkt het verzoek en stuurt een bevestiging terug naar jou met een unieke zegel (sessiecookie) die bewijst dat de transactie is goedgekeurd.
5. de Hacker onderschept de bevestiging van de bank met de unieke zegel en maakt een kopie van deze zegel.
6. de Hacker gebruikt deze zegel om zich voor te doen als jou en voert transacties uit op jouw bankrekening zonder dat jij het merkt.
7. de Gebruiker ontvangt uiteindelijk de originele bevestiging, maar ondertussen heeft de hacker al toegang gekregen tot je bankrekening.

Uitleg:

- de unieke zegel in deze vergelijking vertegenwoordigt de sessiecookie die door de legitieme website wordt verstrekt nadat de gebruiker succesvol is ingelogd.
- de Hacker onderschept deze sessiecookie en gebruikt deze om toegang te krijgen tot de sessie van de gebruiker zonder de wachtwoorden opnieuw in te voeren.

Browser-in-the-Browser Aanval

Vergelijking met in het echte leven:

1. de Gebruiker (jij) gaat naar een openbare plek zoals een winkelcentrum en ziet een informatiebalie met een officiële uitstraling.
2. de Hacker (een oplichter) heeft een vals loket opgezet dat er precies uitziet als de echte informatiebalie van een bekende organisatie, bijvoorbeeld je bank.
3. de Gebruiker nadert het valse loket en ziet alle gebruikelijke logo's en documenten die de echte bank ook zou hebben.
4. de Hacker vraagt om je identiteitsbewijs en andere vertrouwelijke documenten, net zoals de echte informatiebalie zou doen.
5. de Gebruiker geeft de informatie aan de hacker, denkend dat het de echte bank is.
6. de Hacker gebruikt de verstrekte informatie om toegang te krijgen tot je bankrekening of andere diensten.
7. de Gebruiker realiseert zich misschien niet meteen dat hij is bedrogen, omdat de valse informatiebalie zo authentiek leek.

Uitleg:

- de valse informatiebalie vertegenwoordigt de browser-in-the-browser aanval, waarbij de hacker een inlogscherm presenteert dat lijkt op het echte inlogscherm van een website.
- de gebruiker wordt misleid om zijn inloggegevens in te voeren in het valse scherm, denkend dat het echt is.
- de browser-in-the-browser aanval misleidt de gebruiker door een zeer overtuigende kopie van een inlogscherm te presenteren, vaak met de juiste URL en uiterlijk, waardoor het moeilijk te onderscheiden is van de echte website.

Samenvatting

- Stelen van Sessiecookies: De hacker onderschept de sessiecookie na een succesvolle inlog en gebruikt deze om toegang te krijgen tot de gebruiker zijn sessie zonder opnieuw in te loggen.
- Browser-in-the-Browser Aanval: de hacker creëert een zeer overtuigende kopie van het inlogscherm binnen de browser, waardoor de gebruiker zijn inloggegevens invoert in een valse interface.