Samen aanjagen van vernieuwing

Weerstand bieden tegen Man-in-the-Middle aanvallen

Handreiking

Auteur(s): SURF
Versie: 1.2
Datum: 20 februari 2026
Kenmerk: Weerstand bieden tegen MitM-aanvallen

Inhoudsopgave

1 Inleiding

Een Man-in-the-Middle (MitM) is een aanval waarbij de aanvaller zich tussen twee partijen bevindt. De partijen denken direct met elkaar te communiceren, echter is de aanvaller in staat informatie af te luisteren (vertrouwelijkheid) en/of te wijzigen (integriteit) en hier misbruik van te maken. Het probleem bij dergelijke aanvallen is voornamelijk dat het voor het slachtoffer lastig of zelfs onmogelijk is om de authenticiteit van een netwerkverbinding, website, applicatie, etc. vast te stellen.

In deze handreiking gaan we specifiek in op het weerstand bieden tegen session hijacking.

2 Session hijacking

Het is een positieve ontwikkeling dat men steeds vaker gebruik maakt van Multifactor authenticatie (MFA). Hierdoor is het voor kwaadwillende lastiger om ongeautoriseerd toegang tot accounts te bemachtigen, bijvoorbeeld omdat (zwakke) wachtwoorden worden (her)gebruikt of ze zijn uitgelekt. Ongeacht het aantal factoren dat men toepast om zich te authentiseren is het resultaat altijd hetzelfde, namelijk een sessiecookie of token. Als kwaadwillende die kunnen bemachtigen kunnen zij zogenaamde replay aanvallen (T1557) uitvoeren en de sessie van de gebruiker overnemen. Kwaadwillende zijn dan ook in mindere mate geïnteresseerd in het kraken, raden of bemachtigen van wachtwoorden en focussen zich steeds meer op het kunnen stelen van sessiecookies en tokens. Deze trend is sterk waarneembaar aan de vele varianten infostealers en phishing panels en -kits die zich specialiseren in het verkrijgen van deze gegevens.

2.1 Hoe kun je het voorkomen (prevent)?

- Implementeer Device-bound session credentials (DBSC)[1];
- Download en installeer nooit software uit een onbekende bron (o.a. usenet, torrents, P2P);
- Implementeer IP cookie binding en/of token binding (cryptografisch signen)[2][3];
- Beperk de geldigheidsduur van access tokens en identity tokens;
- Implementeer de http-security headers[4] en controleer dit via https://securityheaders.com;
- Sta niet meer dan één sessie tegelijkertijd toe;
- Configureer browsers om regelmatig persistente cookies te verwijderen;
- Verkort de geldigheidsduur van sessiecookies maar houdt wel rekening met de werkbaarheid voor studenten en medewerkers. Een sessieduur van bijvoorbeeld 8 uur zorgt ervoor dat tokens slechts één werkdag geldig zijn, maar dat men niet meermaals per dag opnieuw hoeft te authentiseren;
- Zorg ervoor dat de Secure cookie vlag ingesteld is voor sessiecookies. Eerder is dit bijvoorbeeld voor de hoofdwebsites van mbo-instellingen onderzocht[5] en kun je zelf ook doen bijvoorbeeld via ‘inspecteren’ in de browser of een proxy (bijvoorbeeld ZAP of Foxyproxy);
- Zorg ervoor dat sessie ID’s opnieuw gegenereerd worden na het inloggen om sessie fixatie te voorkomen[6];
- Overweeg het implementeren van conditionele toegang waarbij succesvol inloggen alleen kan wanneer men voldoet aan bepaalde condities, zoals bijvoorbeeld geografische beperkingen (IP-adressen, ASN, proxy), patchlevels van endpoints of tijdstippen (zoals ’s nachts);
- Implementeer just-in-time toegang en hanteer het least privilege principe voor geprivilegieerde gebruikers[7];

[1] https://w3c.github.io/webappsec-dbsc/

[2] https://learn.microsoft.com/en-us/power-platform/admin/block-cookie-replay-attack

[3] https://datatracker.ietf.org/doc/rfc8473/

[4] https://sec.surf.nl/asset/handreiking-tls

[5] Mick Deben: Privacy & cookies (*alleen toegankelijk voor leden Netwerk IBP)

[6] https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

[7] https://sec.surf.nl/controls/sb-13-003-privileged-access/

- Installeer in alle webbrowsers een malwareblokkerende browser-extensie zoals uBlock Origin[8]. Deze extensie zorgt ervoor dat advertenties en pop-ups geblokkeerd worden. Veel endpoints raken geïnfecteerd via malvertising, waarbij kwaadaardige code in advertenties geïnjecteerd wordt. Alleen door het bezoeken van een pagina kan een endpoint al geïnfecteerd raken. Deze extensie draagt daarom bij aan het beperken van de mogelijkheden daartoe en draagt bij aan het waarborgen van de privacy van medewerkers en studenten;
- Zorg ervoor dat alle endpoints voorzien zijn van een (extended) endpoint detection & response (XDR/EDR) oplossing. EDR's dragen bij aan het detecteren en isoleren/verwijderen van malware, zoals infostealers. Monitor dit actief bijvoorbeeld aan de hand van passief en actief asset discovery;
- Implementeer webfiltering om het bezoeken van bekende schadelijke websites door gebruikers te voorkomen, bijvoorbeeld met behulp van de DNS-firewall van SURF[9]. Let op dat dit alleen effect heeft op gebruikers die verbonden zijn met het netwerk van de instelling.

2.2 Hoe kun je het detecteren (detect)?

- Meldingen van SURFcert, bijvoorbeeld wanneer instellingen opduiken op bekende fora, darkweb, Telegram groepen of ShadowServer meldingen, kunnen een indicatie zijn van infostealer infecties;
- Implementeer detectie (en geautomatiseerde respons) op endpoints om data exfiltratie (TA0010) door infostealers tijdig te detecteren;
- Voer regelmatig analyses uit op logging om afwijkende activiteiten te detecteren, bijvoorbeeld meerdere logins met dezelfde sessie cookies (vanaf verschillende apparaten, locaties, IP-adressen), onverwachte loginpogingen, etc. Monitoring op misbruik van sessie cookies in Microsoft Azure kan bijvoorbeeld via Entra ID Protection en voor webapplicaties via Defender for Cloud Apps (ook SaaS).

2.3 Hoe kun je erop reageren (respond)?

- Beëindig direct alle sessies van gecompromitteerde accounts en reset de credentials;
- Identificeer de bron van de infectie (machine, malware(familie), IP-adres, student, medewerker, etc.) en ondersteun de student of medewerker bij het verhelpen van de infectie;
- Verzamel en deel indicators of compromise (IoC) met SURFcert.

[8] https://ublockorigin.com/
[9] https://www.surf.nl/diensten/surfdomeinen