Samen aanjagen van vernieuwing

Handreiking Gelekte inloggegevens

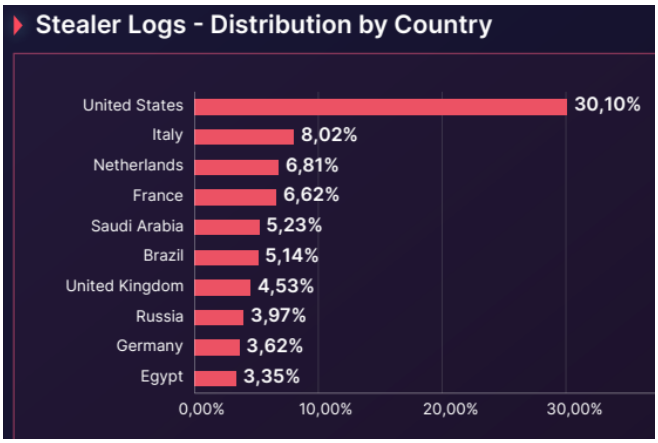
Voorkomen, detecteren en handelen door IT-teams

Auteur(s): Ry Boxem, Mick Deben, Joost Gadellaa, Arne Visscher
Versie: 1.0
Datum: 25 februari 2026
Kenmerk: Handreiking Gelekte inloggegevens

Inhoudsopgave

1 Inleiding

Door de toenemende digitalisering en het tijd- en plaats onafhankelijk werken is de beveiliging van digitale identiteiten (accounts) belangrijker dan ooit. Uitgelekte inloggegevens en gestolen sessiecookies zijn een groot probleem, omdat ze vaak resulteren in ongeautoriseerde toegang tot netwerken en systemen. Gestolen inloggegevens worden op grote schaal verhandeld door Initial Access Brokers (IAB)[1] op het darkweb of gratis beschikbaar gesteld op platformen zoals Telegram of Pastebin. De opkomst van infostealers, die deze gegevens verzamelen, heeft deze handel sterk doen toenemen. Een infostealer is een vorm van malware op je apparaat, die je persoonlijke gegevens verzamelt voor criminele doeleinden. Nederlanders lijken door de zeer laagdrempelige toegang tot het internet bovengemiddeld vatbaar voor infostealers.



Inloggegevens zijn waardevol voor aanvallers en vormen doorgaans op meerdere momenten tijdens een cyberaanval een belangrijke rol.[2] Bijvoorbeeld voor verkenningsactiviteiten, laterale beweging, het verhogen van rechten, data-exfiltratie en het uitvoeren van aanvallen vanuit accounts. Het is daarom van belang om het uitlekken en misbruiken van inloggegevens zo veel mogelijk te voorkomen, maar ook tijdig te detecteren en er adequaat op te reageren. In deze handreiking bieden we daar handelingsperspectief voor. In de handreiking ‘weerstand bieden tegen man-in-the-middle aanvallen’[3] hebben we handelingsperspectief geboden voor gestolen sessiecookies.

Het gaat hierbij specifiek niet alleen om het uitlekken van de inloggegevens die een medewerker of student van de instelling heeft gekregen, maar juist ook om privé-accounts, of andere accounts voor werktoepassingen met dezelfde gebruikersnaam. Juist die vormen een risico: medewerkers gebruiken soms hetzelfde wachtwoord voor hun werk-account als voor andere werk-gerelateerde accounts. Als er daar eentje buiten de controle van de instelling uitlekt, kan dat een bedreiging voor het hoofdaccount vormen bij hergebruikte wachtwoorden.

[1] Partij die illegaal toegang tot netwerken verkrijgt en deze toegang aan anderen verkoopt. Deze anderen gebruiken de gekochte toegang bijvoorbeeld voor de uitvoering van ransomware-aanvallen.

[2] zie bijvoorbeeld Credential Access (TA0006) van Mitre ATT&CK

[3] https://sec.surf.nl/weerstand-bieden-tegen-mitm-aanvallen

2 Preventie

Op door de instelling beheerde apparaten en werkplekken is meer grip en controle op veiligheid vergeleken met privé apparatuur van studenten en medewerkers. Zo kun je op beheerde apparaten en werkplekken bepalen welke rechten de gebruiker heeft, welke software geïnstalleerd en gebruikt mag worden, hoe er gemonitord wordt en kun je een wachtwoordbeleid afdwingen.

Omdat instellingen een beperkte invloedsfeer hebben op gebruikers en de privé gebruikte apparaten (of Bring Your Own Device) kun je nooit 100% voorkomen dat inloggegevens uitlekken. Je kunt wel proberen de kans daarop te verkleinen en jezelf zo goed mogelijk voorbereiden voor wanneer dat wel het geval is. Er is onderscheid gemaakt tussen preventie van het lekken van inloggegevens en preventie voor het misbruik door inloggegevens lekken.

2.1 Preventie van lekken

2.1.1 Bewustwording

Wijs studenten, docenten en (tijdelijke) medewerkers regelmatig op zorgvuldig en veilig omgaan met inloggegevens, bijvoorbeeld met behulp van Cybersafe Yourself.[4] De kracht van boodschap zit hem in de herhaling daarvan.

2.1.2 Wachtwoordbeleid

Dwing het gebruik van sterke Inloggegevens af, zodat het gebruik van makkelijk te raden en te kraken Inloggegevens niet is toegestaan. Controleer daarnaast of ingevoerde Inloggegevens eerder zijn uitgelekt en weiger die, bijvoorbeeld met behulp van wachtwoordlijsten.[5] Het vaak laten wijzigen van wachtwoorden wordt hierbij expliciet afgeraden omdat dit ervoor zorgt dat gebruikers makkelijkere wachtwoorden gaan kiezen.
Het aansturen op wachtwoordzinnen of passkeys is gebruiksvriendelijker én veiliger.

2.1.3 Wachtwoordmanagers

Stimuleer het gebruik van unieke en sterke inloggegevens door *alle* studenten en medewerkers een wachtwoordmanager te faciliteren, zie bijvoorbeeld de handreiking wachtwoordkluis.[6] Idealiter heeft de wachtwoordmanager ook een detectiefunctionaliteit voor bekende gelekte wachtwoorden. Door het gebruik van een wachtwoordmanager hoeven wachtwoorden niet op post-its of andere notities opgeschreven te worden en is het eenvoudiger om unieke, sterke wachtwoorden en - zinnen te genereren, zonder die te hoeven onthouden. Voorwaarde is wel dat het hoofdwachtwoord sterk en uniek is, bij voorkeur gecombineerd met multi-factor authenticatie (MFA), om het risico van ongeautoriseerde toegang te beperken.

Merk hierbij op dat het zinnig kan zijn een oplossing te bieden die studenten en medewerkers ook privé mogen gebruiken. Gelekte privé-inloggegevens zijn ook een risico voor de instelling, en de meeste gebruikers zullen liever geen twee wachtwoordmanagers naast elkaar gebruiken.

[4] https://cybersaveyourself.nl/

[5] https://github.com/danielmiessler/SecLists

[6] https://sec.surf.nl/asset/handreiking-wachtwoordkluis/

2.1.4 Single Sign On

Single-Sign-On (SSO)[7] zorgt ervoor dat eindgebruikers niet voor iedere dienst apart moeten inloggen, maar dit doen met hun identiteit van de centrale *identity provider*. Hierdoor hoeven zij niet meerdere wachtwoorden of -zinnen te onthouden. Dit geeft studenten en medewerkers de gelegenheid om op een gebruiksvriendelijke manier gebruik te maken van een sterke identiteit. Hoe meer diensten je aan deze identiteit kan koppelen, hoe sterker het effect. Daarbij is het van belang om passende beveiligingsmaatregelen toe te passen, zoals herauthenticatie op relevante momenten, het verplicht stellen van een tweede factor (bij toegang tot kritieke systemen) en het hanteren van beperkte geldigheidsduren van sessies.

2.1.5 Credential discovery

Naast hacks bij derde partijen kunnen wachtwoorden ook intern 'lekken', bijvoorbeeld als lijstjes met wachtwoorden die ergens worden opgeslagen of gedeeld via een fileshare of een chat. Instellingen kunnen pro-actief scannen naar verkeerd beveiligde shares en of daar credenitals op staan en op basis daarvan corrigerende acties ondernemen, met als doel voorkomen dat ze in verkeerde handen vallen. Dit kan bijvoorbeeld met behulp van tools zoals Trufflehog.[8]

2.2 Preventie van misbruik

2.2.1 Multi Factor Authenticatie

Multi-Factor Authenticatie (MFA)[9] zorgt ervoor dat meerdere factoren nodig zijn om toegang te verkrijgen en is **de belangrijkste maatregel** om incidenten naar aanleiding van gelekte wachtwoorden te voorkomen. Zoals we in de handreiking 'Weerstand bieden tegen man-in-the-middle aanvallen'[10] hebben beschreven is MFA geen wondermiddel, maar het maakt het wel lastiger voor aanvallers om ongeautoriseerd toegang te verkrijgen. Een gelekt wachtwoord is dan, in ieder geval voor de belangrijkste systemen of toegang van buitenaf, niet genoeg om binnen te komen. Bij veel van de recente incidenten in de sector was de combinatie van gelekte toegangsgegevens en de afwezigheid van MFA aan te wijzen als belangrijke oorzaak.

[7] https://www.surf.nl/diensten/identiteits-en-toegangsbeheer/surfconext

[8] https://github.com/trufflesecurity/trufflehog

[9] https://www.surf.nl/diensten/identiteits-en-toegangsbeheer/surfsecureid

[10] https://sec.surf.nl/asset/handreiking-weerstand-bieden-tegen-mitm-aanvallen

3 Detectie

Er zijn meerdere mogelijkheden waarop detectie van gelekte Inloggegevens plaats kan vinden en we hebben de voornaamste mogelijkheden op een rijtje gezet.

3.1 SURFcert

Alle bij SURF aangesloten instellingen ontvangen meldingen van SURFcert[11] zodra zij op de hoogte zijn gebracht van gelekte inloggegevens, bijvoorbeeld door de politie of het Nationaal Cyber Security Centrum (NCSC) nadat criminele IT-infrastructuur geconfisqueerd is. Uiteraard kan dit ook op basis van eigen onderzoek het geval zijn of door leden van de SURF community.

3.2 Studenten en medewerkers

Studenten en medewerkers kunnen stuiten op kwetsbaarheden of misconfiguraties waardoor zij bijvoorbeeld onbedoeld toegang krijgen tot Inloggegevens. Ook kunnen ze hun inloggegevens per ongeluk ergens invullen of delen. Het is daarom belangrijk om een duidelijke en laagdrempelige meldprocedure te hebben, deze regelmatig communiceren en het maken van meldingen te stimuleren, hetzij via de servicedesk of de security incidentprocedure (‘no-blame’ cultuur).

3.3 Darkweb monitoring

Gestolen of gekraakte Inloggegevens worden vaak verhandeld op het darkweb in cybercrime fora, maar ook gedeeld op platformen zoals Pastebin of Telegram. Het monitoren van dergelijke bronnen stelt instellingen in staat om uitgelekte Inloggegevens te detecteren. Desondanks adviseren wij om dit niet zelfstandig te doen en over te laten aan SURFcert of gebruik te maken van tooling.

Instellingen kunnen ook andere oplossingen zoals Have I Been Pwned gebruiken om notificaties te ontvangen zodra er nieuwe Inloggegevens op zijn gedoken in datalekken en dumps.[12] Hierdoor kan de instelling snel acteren en voorkomen dat de gelekte Inloggegevens bruikbaar zijn.

3.4 Coordinated Vulnerability Disclosure

Instellingen met een Coordinated Vulnerability Disclosure (CVD) beleid kunnen meldingen via dit proces ontvangen over geïdentificeerde kwetsbaarheden en misconfiguraties. Er zijn voorbeelden bekend waarbij bijvoorbeeld Inloggegevens tijdelijk toegankelijk waren voor derden. Wij raden alle instellingen daarom aan om een CVD-beleid op te stellen en RFC 9116 (security.txt) te implementeren, zie ook de berichtgeving van SURF hierover.[13]

3.5 Honey tokens

Honey tokens zijn lokmiddelen die bestaan om misbruik te detecteren. Honeytokens zouden in dit geval inloggegevens zijn van accounts die er interessant uitzien, maar geen daadwerkelijke toegang heeft. Zodra een aanvaller een honeytoken gebruikt, krijgt de instelling een melding en kan een onderzoek naar de potentiële aanval direct gestart worden.

[11] https://www.surf.nl/diensten/beveiliging/surfcert

[12] https://haveibeenpwned.com

[13] https://sec.surf.nl/handreiking-cvd-en-security-txt

3.6 Security monitoring

De voornaamste bron voor het detecteren van *misbruik* van uitgelekte Inloggegevens is security monitoring, zoals bijvoorbeeld SIEM/SOC oplossingen[14]. Zorg ervoor dat authenticatie logs, met name ook van cloudoplossingen, nauwlettend gemonitord worden om misbruik tijdig te kunnen detecteren. Gelekte wachtwoorden worden vaak breed geprobeerd door middel van password spraying en brute forcing, dit type acties is detecteerbaar.

3.7 Entra ID Protection

Specifiek voor gebruikers van Microsoft Entra ID helpt Protection & Conditionele toegang organisaties bij het detecteren, onderzoeken en verhelpen van identiteitsgerelateerde risico's, waaronder uitgelekte Inloggegevens voor aan de instelling verbonden accounts.[15] Deze risico's kunnen worden ingevoerd in tools zoals Conditional Access om (automatisch) beslissingen over toegang te nemen, of worden verzonden naar een SIEM-tool[16] voor verder onderzoek, correlatie en eventueel geautomatiseerde maatregelen.

[14] https://www.surf.nl/diensten/beveiliging/surfsoc

[15] https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

[16] https://www.surf.nl/diensten/beveiliging/surfsoc

4 Reactie

Zodra wordt vermoed dat inloggegevens van de instelling zijn uitgelekt is het van belang om actie te ondernemen om ongeautoriseerde toegang en gevolgschade te beperken.

4.1 Bepalen relevantie

Een uitdaging met gelekte Inloggegevens is vaststellen of ze relevant zijn. In de praktijk blijkt namelijk dat veel Inloggegevens worden 'geremixt' in gecombineerde lijsten ('combolists') of onder een andere noemer opnieuw worden aangeboden. Het kan daarom zijn dat Inloggegevens worden gemeld van accounts die geruime tijd niet meer bestaan. Het belangrijkste bij de relevantie is of het gaat om een instellingsaccount, of een ander account van de medewerker wat eventueel hergebruikt kan zijn en of het account nog actief is.

4.2 Eerste stappen

Zodra bevestigd is dat de uitgelekte inloggegevens authentiek en nieuw zijn, treedt het incident response plan in werking. De eerste maatregelen zijn gericht op het beperken van verdere schade (containment) en het verkrijgen van inzicht in mogelijke misbruik.

4.2.1 Fase 1 – Directe maatregelen (uitvoerbaar door de instelling)

De onderstaande stappen zijn in deze volgorde opgenomen om eerst de potentiële impact vast te stellen, vervolgens direct verdere schade te beperken en daarna verdiepend onderzoek en communicatie uit te voeren.

Voer in ieder geval de volgende stappen uit:

1. Stel vast of het account actief is en of er aanwijzingen zijn dat de inloggegevens zijn misbruikt.
2. Bepaal het autorisatieniveau van het account (bijvoorbeeld normale gebruiker, beheerder, student) om de potentiële impact in te schatten.
3. Forceer een wachtwoord- en/of MFA-reset en blokkeer of isoleer indien nodig tijdelijk het mogelijk gecompromitteerde apparaat (werkplek, server, etc.).
4. Trek actieve sessies en geldige tokens gericht in indien er een vermoeden bestaat van misbruik (bijvoorbeeld refresh tokens).
5. Scherp indien noodzakelijk tijdelijk de conditionele toegangsregels aan voor het betreffende account.
6. Onderzoek of de betreffende inloggegevens ook bij andere diensten of systemen worden hergebruikt, zodat aanvullende resets of intrekkingen kunnen worden uitgevoerd.
7. Analyseer recente inlogactiviteiten op afwijkingen, zoals ongebruikelijke IP-adressen, locaties of tijdstippen.
8. Informeer de gebruiker van het account over de ondernomen maatregelen en de consequenties daarvan.
9. Registreer het incident conform de geldende incidentprocedure en leg de uitgevoerde handelingen vast.
10. In situaties waarin geen aanwijzingen zijn voor misbruik, kunnen bovenstaande maatregelen in veel gevallen voldoende zijn.

4.2.2 Fase 2 – Nader onderzoek bij (vermoed) misbruik

Indien misbruik is vastgesteld of aannemelijk wordt geacht, is verdiepend onderzoek noodzakelijk. Richt dit onder meer op:

- Pogingen tot laterale beweging binnen de omgeving.
- Escalatie van privileges.
- Het realiseren van persistentie.
- Nieuwe e-mailregels (zoals automatisch doorsturen).
- Verzonden phishingmails naar collega's of externen.
- Ongebruikelijke OAuth- of app-registraties.
- Data-exfiltratie.
- Wijzigingen in MFA-instellingen.
- Analyse of wijziging van relevante logbronnen en/of log instellingen

4.2.3 Kantelpunt: zelf onderzoeken of escaleren

Bij vastgesteld of vermoed misbruik dient de instelling expliciet de afweging te maken of zij:

- Voldoende capaciteit, expertise en tooling heeft om het incident zelfstandig te onderzoeken en af te handelen.
- In staat is om relevante loggegevens en systemen op een forensisch verantwoorde wijze veilig te stellen.

Escalatie naar SURFcert of het inschakelen van een gespecialiseerde DFIR-partij (Digital Forensics & Incident Response) is in het bijzonder aangewezen wanneer:

- Sprake is van compromittering van beheerdersaccounts of kritieke systemen.
- Aanwijzingen bestaan voor datalekken of grootschalige impact.
- Strafbare feiten niet kunnen worden uitgesloten.
- Interne expertise of capaciteit tekortschiet.
- Juridische procedures of aansprakelijkheidskwesties denkbaar zijn.

In dergelijke situaties is het van belang om wijzigingen aan mogelijk bewijsmateriaal te minimaliseren en zorgvuldig vast te leggen welke acties zijn uitgevoerd (chain of custody), zodat bevindingen indien nodig juridisch bruikbaar blijven.

Volg hierin ook de aanwijzingen van bevoegde autoriteiten.

4.3 Templates

Zorg voor communicatietemplates om stakeholders te informeren over uitgelekte inloggegevens, waarbij ook vooraf vastgelegde alternatieve contactmethoden beschikbaar zijn voor situaties waarin e-mail niet toegankelijk is.

Een stap verder is om de reactie op misbruikte Inloggegevens te automatiseren met Security Orchestration, Automation & Response (SOAR). Er zijn allerlei playbooks beschikbaar waar

instellingen gebruik van kunnen maken.[17][18][19] Pas de reactie aan op basis van de gevoeligheid en consequenties voor accounts en gebruikers.

4.4 Kennisdeling

Deel informatie over incidenten en de lessen die geleerd zijn tijdens de opvolging met SURFcert en SCIRT zodat de rest van de sector hiervan kan profiteren. Betrek indien nodig SURFcert bij het afhandelen van incidenten.

[17] https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks

[18] https://github.com/phantomcyber/playbooks

[19] https://github.com/correlatedsecurity/Awesome-SOAR?tab=readme-ov-file#Playbooks-Resources

5 Herstel

Mochten uitgelekte Inloggegevens succesvol zijn misbruikt en daardoor schade zijn ontstaan, dan kan het nodig zijn om herstelwerkzaamheden te verrichten. De benodigde reactie is sterk afhankelijk van het soort incident, is bijvoorbeeld een wachtwoord gestolen of een geldig sessiecookie?

5.1 Herstelplannen

In het algemeen geldt dat herstelplannen onderdeel dienen uit te maken van business continuity en disaster recovery plannen en -procedures.[20]

5.2 Oefenen

De effectiviteit van plannen, rolverdelingen en procedures wordt pas duidelijk zodra je ze gaat oefenen. Zorg er daarom voor dat je dit regelmatig doet zodat je niet voor ongewenste verassingen komt te staan op het moment dat herstellen noodzakelijk is.[21]

5.3 Opschonen

Afhankelijk van de impact van het incident kan het nodig zijn om regels uit mailboxen te verwijderen, malafide mails uit mailboxen te verwijderen, ongewenste apps te verwijderen, geplande taken verwijderen, etc. Zorg er in ieder geval voor dat ieder incident response plan de stappen bevat om te herstellen naar de gewenste situatie, waarbij benodigde queries en scripts vooraf zijn voorbereid en getest, zodat deze direct inzetbaar zijn tijdens een incident.

[20] https://sec.surf.nl/asset/category/bedrijfscontinuiteitsbeheer/

[21] https://sec.surf.nl/crisismanagement/