AUTHENTICATIE

IN DE BEDRIJFSOMGEVING

KOMPAS

WEGWIJS IN CYBERSECURITY

INHOUDSTAFEL

Een goede authenticatie-oplossing vormt de belangrijkste component binnen een robuuste beveiligingsinfrastructuur in een bedrijfsomgeving. Zonder sterke en goed geïmplementeerde gebruikersauthenticatie blijft de volledige IT-infrastructuur kwetsbaar voor allerlei aanvallen. Daarom moeten bedrijven grondig nadenken over hun authenticatiebeleid en de risico's die gepaard gaan met een verouderde of ontoereikende aanpak.

Dit kompas biedt een inzicht in de rol van authenticatie binnen de bedrijfscontext en belicht de tekortkomingen van traditionele authenticatiemethoden. Daarnaast worden moderne strategieën besproken die een verhoogde graad van beveiliging en gebruiksvriendelijkheid bieden. Door de evolutie van dreigingen en best practices in kaart te brengen, ondersteunt dit kompas bedrijven bij het maken van doordachte keuzes om hun authenticatieprocessen te versterken en hun IT-infrastructuur beter te beschermen tegen misbruik.

AUTEURS: Pieter Philippaerts, Wouter Joosen, DistriNet, KU Leuven

Publicatiedatum: 14.02.2025

1 HET BELANG VAN AUTHENTICATIE

Authenticatie is een fundamentele beveiligingspijler binnen de IT-omgeving van elk bedrijf. Het garandeert dat enkel geautoriseerde gebruikers toegang krijgen tot systemen en gegevens, waardoor het een essentiële verdediging is bij het beveiligen van bedrijfsinformatie. Naast het beschermen tegen ongeoorloofde toegang—wat uiteraard essentieel is—wordt authenticatie steeds belangrijker in het licht van nieuwe Europese wetgeving. Nieuwe regelgevingen leggen strengere eisen op aan toegangsbeheer en verplichten bedrijven te investeren in robuuste authenticatiemechanismen.

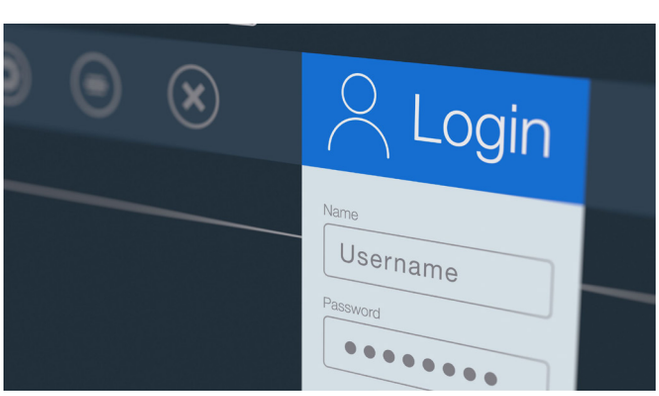
EEN STUKJE GESCHIEDENIS

Wachtwoorden vormen de basis van klassieke authenticatiemethodes, en hun oorsprong gaat terug tot ver voor het digitale tijdperk. In militaire en sociale contexten werden wachtwoorden, herkenningscodes en geheime zinnen gebruikt om toegang te verlenen of identiteiten te verifiëren. De oude Romeinen hanteerden dergelijke woorden bijvoorbeeld om tijdens nachtelijke patrouilles bondgenoten van vijanden te onderscheiden.

De introductie van wachtwoorden in een digitale context vond plaats begin jaren ‘60 aan het Massachusetts Institute of Technology. Daar ontwikkelde Fernando Corbató het *Compatible Time-Sharing System*, een van de eerste systemen die meerdere gebruikers simultaan liet werken op een gedeelde computer. Om de privacy van gebruikers te garanderen, werd een wachtwoordsysteem ingevoerd. Elke gebruiker kreeg een individueel wachtwoord om toegang te krijgen tot hun persoonlijke bestanden en werkruimte. Dit concept vormde de uiteindelijke basis voor vele verdere ontwikkelingen in digitale authenticatie.

Tijdens de opkomst van persoonlijke computers in de jaren ‘80 en de vroege dagen van het internet in de jaren ‘90 groeide het belang van wachtwoorden sterk. Toegang tot bedrijfsnetwerken, softwaretoepassingen en later websites en online diensten vereiste een vorm van authenticatie. Dit leidde tot een breed maatschappelijk gebruik van wachtwoorden om digitale identiteiten te beschermen. In de loop der jaren werd de rol van wachtwoorden verder versterkt door de standaardisering en regulering van IT-beveiliging. In 2003 ontwikkelde het Amerikaanse National Institute of Standards and Technology (NIST) richtlijnen om wachtwoorden complexer en veiliger te maken, wat de basis legde voor hedendaagse wachtwoordbeleidstrategieën.

Ondanks hun beperkingen zijn wachtwoorden nog steeds een essentieel onderdeel van de IT-infrastructuur. Ze zijn diep verweven in zowel persoonlijke als professionele omgevingen en blijven een fundamentele bouwsteen van hedendaagse beveiligingssystemen.



HET BELANG VAN STERKE AUTHENTICATIE

Klassieke authenticatie kent een aantal inherente zwakheden waar aanvallers misbruik van maken. Zo worden gestolen inloggegevens vaak gebruikt om aanvallen zoals ransomware op te zetten.

Ransomware is het meest-voorkomende type cyberaanval waar ook Belgische bedrijven mee te maken hebben. Hoewel er verschillende beveiligingsmaatregelen mogelijk zijn, is een van de meest fundamentele en effectieve stappen het implementeren van een robuust authenticatiemechanisme.

In veel gevallen begint een ransomware-aanval met gestolen inloggegevens van een gebruiker. Met deze gegevens kunnen aanvallers niet alleen toegang verkrijgen tot afgeschermde systemen, maar ook vrij bewegen binnen het bedrijfsnetwerk. Dit fenomeen, bekend als laterale beweging, stelt hen in staat om kwetsbare systemen te identificeren en het bedrijf verder te compromitteren. Het gebruik van sterke authenticatiemethoden kan de impact van deze dreiging sterk verminderen.

Bijvoorbeeld, het Cybersecurity Centre Belgium schat dat tot 80% van de cyberaanvallen voorkomen kan worden door de implementatie van multifactorauthenticatie. Microsoft gaat nog een stap verder en claimt in hun onderzoek dat multifactorauthenticatie het risico van compromittering vermindert met 99.22%.

WANNEER AUTHENTICATIE MISLOOPT

Ondanks het feit dat iedereen het belang van sterke authenticatie inziet, loopt het in de praktijk toch nog vaak mis. De eerste grote hack van dit jaar trof Telefonica, een van de grootste telecommunicatie-bedrijven in Europa, waarbij hackers ongeveer 2,3GB aan gevoelige data exfiltreerden. De aanval begon met *infostealer-malware* waarmee de inloggegevens van minstens vijftien medewerkers werden buitgemaakt. Vervolgens gebruikten de aanvallers *social engineering* om hun toegang verder uit te breiden, specifiek gericht op twee werknemers met

administratieve rechten. Via deze accounts konden ze *brute-force-aanvallen* uitvoeren op de SSH-authenticatie van kritieke servers.

De impact kan ook verder reiken dan alleen datadiefstal en kan ook gevolgen hebben in de fysieke wereld. Dit werd duidelijk bij de Colonial Pipeline-aanval in 2021, een van de meest ingrijpende cyberaanvallen op de Amerikaanse energie-infrastructuur. Hackers wisten toegang te krijgen tot het netwerk van Colonial Pipeline via een verouderd VPN-account zonder multifactorauthenticatie, wat hen de mogelijkheid gaf om ransomware te installeren die de oliepijpleiding lamlegde. Als gevolg hiervan werd de brandstoftoevoer in grote delen van de Verenigde Staten ernstig verstoord, wat leidde tot brandstoftekorten en prijsstijgingen.

Sterke authenticatie is essentieel, maar moet ook correct worden geïmplementeerd. Zo werd Microsoft onlangs opgeschrikt door een kwetsbaarheid in hun multifactorauthenticatie, waardoor brute-force-aanvallen mogelijk waren. Zelfs bedrijven die gespecialiseerd zijn in *identity security* zijn niet immuun voor authenticatiefouten. Dit werd pijnlijk duidelijk bij de Okta-hack in november 2023, waarbij een aanvaller toegang kreeg tot het klantenservicesysteem van het bedrijf. De aanval was mogelijk doordat een Okta-medewerker zich met een bedrijfsapparaat had aangemeld bij een persoonlijk Google-account, waarin vervolgens de inloggegevens van een interne serviceaccount werd opgeslagen. Nadat de persoonlijke Google-account vermoedelijk werd gecompromitteerd, kregen de aanvallers toegang tot gevoelige klantgegevens en konden ze die data misbruiken om bij de systemen van die klanten in te loggen.

AUTHENTICATIE EN AUTORISATIE

Authenticatie en autorisatie worden vaak met elkaar verward, maar ze vervullen verschillende functies binnen een beveiligingsstrategie. Authenticatie is het proces waarbij de identiteit van een gebruiker of systeem wordt geverifieerd. Autorisatie daarentegen bepaalt welke rechten een geauthenticeerde gebruiker krijgt en welke acties hij mag uitvoeren binnen een systeem. Hoewel authenticatie en autorisatie vaak samen worden toegepast, zijn ze afzonderlijke stappen in het toegangsbeheer.

Autorisatie houdt zich bezig met het beheer van rechten en zorgt ervoor dat gebruikers enkel toegang krijgen tot de middelen die nodig zijn voor hun functie. Dit wordt bereikt door gebruik te maken van toegangscontrolemodellen zoals *Role-Based Access Control (RBAC)* en *Attribute-Based Access Control (ABAC)*.

RBAC kent rechten toe op basis van rollen binnen een organisatie. Een medewerker in de boekhouding kan bijvoorbeeld toegang krijgen tot financiële gegevens, terwijl een IT-beheerder administratieve rechten heeft over het netwerk.

ABAC biedt een fijnmazigere controle door toegang te baseren op kenmerken zoals de locatie van de gebruiker, het tijdstip van toegang of de gevoeligheid van de gevraagde gegevens.

Een belangrijk principe binnen autorisatiebeheer is het principe van *least privilege*. Dit houdt in dat gebruikers alleen de minimale rechten krijgen die nodig zijn om hun taken uit te voeren. Op die manier wordt het risico op misbruik of menselijke fouten beperkt. De gebruikersrechten moeten continu geëvalueerd worden, waarbij ongebruikte of overbodige rechten tijdig worden ingetrokken. Dit vermindert niet alleen het risico op ongeautoriseerde toegang, maar draagt ook bij aan een betere naleving van beveiligingsrichtlijnen en eventuele regelgeving.

2 PROBLEMEN MET KLASSIEKE AUTHENTICATIE

Het klassieke gebruik van wachtwoorden leidt tot tal van beveiligingsproblemen. Ondanks pogingen om ze veiliger te maken, blijven wachtwoorden inherent onveilig, vooral omdat gebruikers moeite hebben ze op een veilige manier te beheren. We bespreken enkele van de meest voorkomende problemen, variërend van zwakke wachtwoorden en hergebruik tot implementatieproblemen.

BRUTE FORCE AANVALLEN

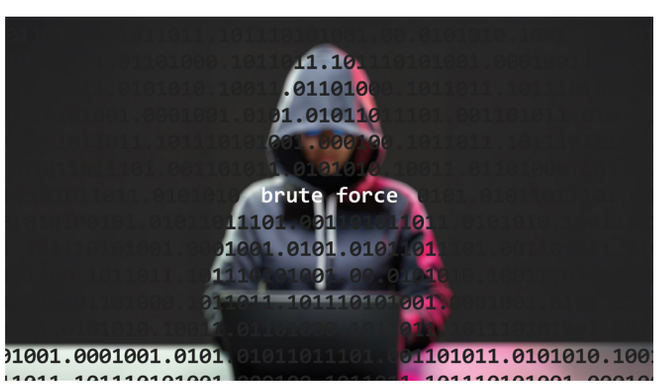
Een *brute force*-aanval bestaat uit het systematisch uitproberen van wachtwoordcombinaties tot de juiste combinatie wordt gevonden. Aanvallen kunnen *online* of *offline* zijn. In een online aanval maakt de aanvaller gebruik van geautomatiseerde scripts om grote aantallen inlogpogingen uit te voeren in korte tijd. In een offline aanval kraakt een aanvaller buitgemaakte wachtwoorden die nog beveiligd zijn met een hash-algoritme. Een hash is een unieke tekenreeks die wordt berekend op basis van het wachtwoord, en waarbij dezelfde invoer altijd dezelfde uitvoer geeft. De aanvaller kan eenvoudigweg hetzelfde hash-algoritme toepassen op gegenereerde wachtwoorden totdat er een overeenkomst gevonden wordt.

Een van de belangrijkste redenen waarom brute force-aanvallen succesvol blijven, is het gebruik van zwakke wachtwoorden. Veel gebruikers hanteren eenvoudig te raden wachtwoorden zoals “123456”, “password” of varianten daarop. Daarnaast worden vaak persoonlijke gegevens, zoals geboortedata of namen van familieleden, gebruikt als wachtwoord, wat een aanvaller al snel kan achterhalen. Wanneer wachtwoorden onvoldoende complex zijn, wordt de benodigde rekenkracht om ze te kraken drastisch verminderd, waardoor het succespercentage van brute force-aanvallen verhoogt.

Een specifieke variant van brute force-aanvallen is de *dictionary attack*. Hierbij maken aanvallers gebruik van woordenlijsten met veelvoorkomende wachtwoorden en wachtwoordpatronen. De aanval verloopt sneller dan een volledige brute force-aanval omdat niet alle mogelijke tekencombinaties worden geprobeerd, maar enkel de meest waarschijnlijke.

Naast traditionele brute force en dictionary attacks bestaan er geavanceerdere technieken zoals het gebruik van *rainbow tables*. Rainbow tables bevatten vooraf berekende hash-waarden van veelvoorkomende wachtwoorden, waardoor een aanvaller zonder langdurige berekeningen een wachtwoord kan achterhalen door simpelweg de hash op te zoeken in de tabel.

Password spraying is een variant van brute force waarbij een aanvaller een beperkt aantal veelgebruikte wachtwoorden test op meerdere accounts. Dit vermijdt dat een specifieke account



vergrendeld wordt, omdat niet herhaaldelijk op één account wordt ingelogd. Door de aanval over meerdere accounts en een langere periode te spreiden, blijft detectie vaak uit.

SOCIAL ENGINEERING EN PHISHING

Social engineering maakt misbruik van het natuurlijke vertrouwen dat mensen hebben in anderen en van hun neiging om autoriteit niet in vraag te stellen. Aanvallers gebruiken manipulatieve technieken om individuen ertoe te brengen vertrouwelijke informatie, zoals wachtwoorden, prijs te geven. Dit gebeurt vaak via telefonische oproepen, e-mails of persoonlijke interacties waarbij de aanvaller zich voordoet als een betrouwbare bron, zoals een collega, een IT-medewerker of een externe dienstverlener. Veel mensen behandelen wachtwoorden niet als strikt vertrouwelijk en geven deze door wanneer hen er expliciet naar wordt gevraagd.

Een aanvaller kan bijvoorbeeld contact opnemen met een medewerker en zich voordoen als een systeembeheerder die een probleem met het account van de medewerker moet oplossen. Door gebruik te maken van overtuigende taal en een gevoel van urgentie te creëren, zoals het dreigen met een onmiddellijke blokkering van het account, kan de aanvaller het slachtoffer ertoe brengen zijn wachtwoord door te geven. Ook via informele gesprekken kunnen aanvallers gevoelige informatie verkrijgen. Een kwaadwillende kan subtiel vragen stellen die helpen om gebruikersgegevens of interne processen bloot te leggen. Dergelijke methoden werken omdat slachtoffers meestal niet beseffen dat ze waardevolle informatie prijsgeven.

Phishing is een veelgebruikte techniek binnen social engineering en vormt een nog grotere dreiging omdat de aanval moeilijker te herkennen is. Bij phishing-aanvallen bouwen criminelen overtuigende frauduleuze websites die er identiek uitzien als legitieme inlogpagina's van banken, cloudservices of bedrijfsportalen. Slachtoffers ontvangen doorgaans een e-mail die afkomstig lijkt van een vertrouwde partij, zoals hun werkgever of een bekende dienstverlener, met de vraag om in te loggen. De link in de e-mail leidt echter naar een nagemaakte website waar de inloggegevens worden onderschept door de aanvaller. Dit maakt phishing in essentie een vorm van *man-in-the-middle-aanval*, waarbij de aanvaller zich tussen het slachtoffer en de echte dienst plaatst om gevoelige gegevens te stelen.

Phishing komt in verschillende vormen voor, afhankelijk van het gebruikte communicatiekanaal. Bij *smishing* worden frauduleuze berichten via sms verstuurd, vaak met links naar valse inlogpagina's. *Vishing* maakt gebruik van telefonische oproepen waarbij de aanvaller zich voordoet als een betrouwbare instantie. Daarnaast bestaan er geavanceerdere methoden, zoals *spear phishing*, waarbij aanvallers doelgericht te werk gaan en hun berichten aanpassen op basis van eerder verzamelde informatie over het slachtoffer.

CREDENTIAL STUFFING

Credential stuffing is een aanvalstechniek waarbij aanvallers gebruikmaken van eerder buitgemaakte inloggegevens om toegang te verkrijgen tot andere online accounts. Dit type aanval maakt misbruik van het feit dat veel gebruikers dezelfde combinatie van gebruikersnaam en wachtwoord op meerdere diensten hergebruiken. Wanneer inloggegevens worden gelekt, kunnen deze worden gebruikt om andere accounts van hetzelfde slachtoffer te compromitteren.

De aanval begint met het verzamelen van gestolen inloggegevens, vaak afkomstig uit openbaar gemaakte of op het dark web verhandelde databases. Deze databases bevatten miljoenen tot miljarden combinaties van e-mailadressen, gebruikersnamen en wachtwoorden, vaak in leesbare tekst of in een eenvoudig te ontsleutelen vorm. Aanvallers

gebruiken gespecialiseerde tools om deze gegevens geautomatiseerd in te voeren in de inlogpagina's van diverse websites en applicaties. Deze tools kunnen duizenden tot miljoenen inlogpogingen per dag uitvoeren en zijn ontworpen om detectie te omzeilen door onder andere proxyservers en geavanceerde botnettechnieken te gebruiken.

In tegenstelling tot traditionele brute force-aanvallen, waarbij wachtwoorden willekeurig worden geraden, werkt *credential stuffing* uitsluitend met bestaande, eerder geverifieerde inloggegevens. Hierdoor ligt de succesratio aanzienlijk hoger. Onderzoek suggereert dat tussen 0,1% en 2% van de gestolen credentials succesvol wordt gebruikt om toegang te krijgen tot andere accounts. Dit betekent dat een dataset van één miljoen gestolen inloggegevens al snel tot tienduizenden overgenomen accounts kan leiden.

KEYLOGGING

Door gebruik te maken van *keyloggers* kunnen aanvallers toetsaanslagen registreren en gevoelige informatie zoals wachtwoorden onderscheppen. Software keyloggers, een vorm van spyware, worden op een systeem geïnstalleerd zonder dat de gebruiker dit merkt en sturen de geregistreerde invoer door naar de aanvaller. De aanval begint meestal met een schadelijke e-mailbijlage, een geïnfecteerde softwaredownload of een malafide link die de gebruiker misleidt om de malware te activeren.

Eenmaal actief, registreert een keylogger systematisch alle ingetikte tekst en kan hij zo complete inloggegevens verzamelen. Sommige varianten zijn specifiek geprogrammeerd om gerichte informatie te filteren, zoals wachtwoorden of betaalgegevens, waardoor een aanvaller snel toegang krijgt tot waardevolle data. Geavanceerdere keyloggers gaan verder en kunnen niet alleen toetsaanslagen onderscheppen, maar ook klembordinhoud uitlezen of screenshots maken op cruciale momenten, bijvoorbeeld bij het invoeren van authenticatiegegevens. Dit verhoogt de kans op succesvolle diefstal van gevoelige informatie en kan beveiligingsmechanismen zoals wachtwoordmanagers omzeilen.

Een keylogger draait doorgaans als een achtergrondproces en probeert detectie door

beveiligingssoftware te vermijden. Sommige varianten gebruiken versleutelde communicatie om de gestolen gegevens onopgemerkt naar de aanvaller te versturen of verwijderen zichzelf automatisch na een bepaalde periode om sporen uit te wissen.

Indien een aanvaller er niet in slaagt om een gebruiker te overtuigen om spyware te installeren, maar wel fysieke toegang heeft tot een systeem, kan hij een *hardware keylogger* gebruiken. Dit is een fysiek apparaat dat tussen het toetsenbord en de computer wordt geplaatst en alle toetsaanslagen registreert zonder dat detectiesoftware dit kan opmerken. Dergelijke apparaten nemen vaak de vorm aan van een kleine adapter in de bekabeling of een USB-apparaat en kunnen, eenmaal geplaatst, langdurig onopgemerkt blijven.

MISBRUIK VAN PASSWORD RESET

Indien een aanvaller niet in staat is om het wachtwoord rechtstreeks te kraken, kan hij proberen gebruik te maken van de functionaliteit voor het resetten van wachtwoorden. Hoewel het inlogproces in veel gevallen goed beveiligd is, bevat het resetproces mogelijk wel kwetsbaarheden.

Vroeger was het gebruik van veiligheidsvragen om een wachtwoord te resetten populair, maar met de opkomst van sociale media bleken de antwoorden op de meeste van die vragen eenvoudig te achterhalen. Vandaag werken de meeste resetprocessen anders, maar kunnen er toch nog kwetsbaarheden in zitten, afhankelijk van hoe de resetlogica is opgebouwd.

Sommige systemen kunnen kwetsbaar zijn voor zogenaamde *host header poisoning*. Dit betreft een techniek waarbij een aanvaller de

website manipuleert, zodat de gegenereerde wachtwoordresetlink wijst naar een domein onder zijn controle. Op deze manier kan de aanvaller toegang krijgen tot de geheime tokens die nodig zijn voor het resetten van wachtwoorden, waarmee hij vervolgens de accounts van gebruikers kan overnemen. Ook maken applicaties soms gebruik van bepaalde parameters om resetlinks te genereren, die door de gebruiker beïnvloed kunnen worden. Dit vergroot de kans dat een aanvaller de resetlink kan aanpassen.

Wanneer resettokens geen vervaldatum hebben, verhoogt de kans dat een gelekt token misbruikt kan worden. Tokens kunnen op verschillende manieren gelekt worden, bijvoorbeeld door het per ongeluk delen van tokens via de *referer header* in HTTP-verzoeken. Daarom heeft een wachtwoordresettoken doorgaans een beperkte geldigheidsduur. Naast die geldigheidsduur, speelt ook de complexiteit van de tokens een belangrijke rol. Als een token niet voldoende willekeurig is, kan een aanvaller het mechanisme achter de generatie van tokens achterhalen en andere geldige tokens creëren. Tokens moeten dus voldoende willekeur bevatten om dit soort aanvallen te voorkomen.

3 MULTIFACTOR-AUTHENTICATIE

Multifactorauthenticatie, of kortweg MFA, is een authenticatiemethode die vereist dat gebruikers meer dan één vorm van verificatie bieden voordat ze toegang krijgen tot een systeem. Het doel van MFA is om de afhankelijkheid van enkel een wachtwoord te verminderen. Bij MFA wordt gebruikgemaakt van meerdere factoren om de identiteit van een gebruiker te verifiëren, wat doorgaans kan bestaan uit iets wat de gebruiker weet (zoals een wachtwoord), iets wat de gebruiker heeft (zoals een smartphone of hardwaretoken) en iets wat de gebruiker is (zoals biometrische gegevens). Op die manier biedt MFA een robuustere beveiliging aan door meerdere lagen van bescherming te combineren.

DE VERSCHILLENDE VORMEN VAN MFA

Multifactorauthenticatie kan op verschillende manieren geïmplementeerd worden, elk met specifieke voor- en nadelen. Een veelgebruikte methode is het gebruik van eenmalige authenticatiecodes (OTP's) die via sms of *authenticator-apps* worden verstrekt. Sms-berichten zijn gemakkelijk te versturen en vereisen geen extra applicaties of hardware langs de kant van de gebruiker, waardoor het een aantrekkelijke optie is voor veel bedrijven. Toch wordt het gebruik van sms-gebaseerde MFA afgeraden. Doordat sms-berichten niet versleuteld zijn, kunnen ze eenvoudig onderschept worden als een aanvaller toegang krijgt tot de telecommunicatie-infrastructuur. Dit werd recentelijk nog aangetoond door een aanval op de Amerikaanse telecomsector, waarbij hackers, gelieerd aan de Chinese overheid, in staat waren om sms-berichten te onderscheppen. Maar ook minder-geavanceerde methodes, zoals SIM swapping, kunnen gebruikt worden om sms-gebaseerde MFA te omzeilen. Ondanks deze kwetsbaarheden biedt sms nog altijd een hoger beveiligingsniveau dan alleen een wachtwoord.

Authenticator-apps, zoals Google Authenticator of Authy, zijn een alternatief voor sms-berichten. Deze apps genereren een tijdelijke code die slechts enkele seconden geldig is. Dit is veel veiliger dan sms, omdat de codes lokaal op het apparaat van de gebruiker worden gegenereerd en niet via een netwerk kunnen worden onderschept. Het gebruik van authenticator-apps wordt dan ook als een van de veiligere vormen van MFA beschouwd.

Een andere vorm van MFA gebruikt pushmeldingen. Hierbij ontvangt de gebruiker een melding op een mobiel apparaat, waarin hij eenvoudig op een knop kan klikken om de inlogpoging goed te keuren. Dit maakt de authenticatie snel en gebruiksvriendelijk, terwijl het toch een extra laag van veiligheid toevoegt.

Ook hardwaretokens bieden een effectieve vorm van beveiliging, en worden al jarenlang gebruikt

voor sterke authenticatie in bankapplicaties. Deze fysieke apparaten genereren een tijdelijke code bij elke inlogpoging, die de gebruiker vervolgens moet invoeren. Sommige varianten werken in combinatie met een bankkaart, waarbij de gebruiker de kaart in het apparaat steekt en een pincode invoert om een code te genereren.

MFA HEEFT OOK PROBLEMEN

Het invoeren van MFA brengt grote beveiligingsvoordelen met zich mee, maar gaat tegelijk gepaard met een aantal moeilijkheden. Het gebruik van MFA is natuurlijk complexer dan het hanteren van enkel een wachtwoord. Sommige gebruikers vinden het gebruik ervan dan ook te moeilijk, wat kan leiden tot weerstand. Daarnaast kunnen bepaalde vormen van MFA bijkomende kosten met zich meebrengen, bijvoorbeeld voor het versturen van eenmalige wachtwoorden via sms of de aanschaf van hardware tokens.

Bovenop de kosten brengt MFA ook administratieve uitdagingen met zich mee. Naast het beheer van vergeten wachtwoorden moeten IT-afdelingen zich voorbereiden op scenario's waarin gebruikers hun tokens of smartphones verliezen, of waarin dergelijke apparaten worden gestolen. Dit leidt tot extra ondersteuningsvragen en kan de operationele belasting van IT-teams verhogen.

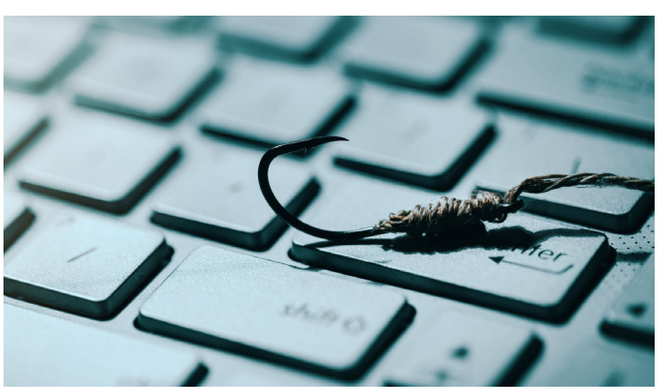
Op beveiligingsgebied is MFA een significante verbetering ten opzichte van wachtwoorden, maar het is zeker geen definitieve oplossing voor alle beveiligingsproblemen. Aanvallers beschikken namelijk over methoden om MFA te omzeilen. Een veelvoorkomende techniek die ze gebruiken is *MFA-fatigue*. Hierbij stuurt een aanvaller herhaaldelijk MFA-verificatieverzoeken naar het apparaat van een gebruiker, met de bedoeling de gebruiker te overstelpen met meldingen. Dit kan ertoe leiden dat de gebruiker uit frustratie of onoplettendheid uiteindelijk een verzoek goedkeurt, waardoor de aanvaller toegang krijgt. Deze techniek is bijzonder effectief en wordt frequent waargenomen in gerichte aanvallen: in 2023 rapporteerde Microsoft dat hun klanten gemiddeld 6000 *MFA-fatigue-aanvallen* per dag ondervonden.

Een tweede methode die wordt toegepast om MFA te omzeilen, is het gebruik van een MFA-proxy. Hierbij maakt een aanvaller een tussenlaag tussen de gebruiker en de legitieme authenticatieservice. De gebruiker wordt via een phishingpagina verleid om in te loggen, waarna de aanvaller zowel de inloggegevens als de gegenereerde MFA-code onderschept. Hierdoor kan de aanvaller zich in real-time authenticeren bij de echte dienst zonder dat de gebruiker zich daarvan bewust is. Deze techniek is een vorm van een *adversary-in-the-middle (AiTM)-aanval*.

PHISHING-RESISTENTE MFA

Verschillende vormen van MFA bieden verschillende niveaus van beveiliging. Een aantal van de beveiligingsproblemen die in de vorige sectie werden besproken, kunnen opgelost worden door te kiezen voor een sterkere MFA-variant, zoals *phishing-resistente MFA*.

Phishing-resistente MFA is ontworpen om aanvallen zoals phishing, man-in-the-middle-aanvallen en credential stuffing te voorkomen door het gebruik van gedeelde codes—zoals authenticator codes—te vermijden en een sterke binding tussen de gebruiker en de authenticator te garanderen. Phishing-resistente MFA maakt gebruik van cryptografische sleutelpaarmechanismen waarbij een unieke private sleutel op een veilig apparaat wordt opgeslagen en niet exporteerbaar is. De bijbehorende publieke sleutel wordt gedeeld met de dienstverlener, waardoor die de gebruiker kan verifiëren wanneer die inlogt. Daarnaast wordt de authenticiteit van authenticatieverzoeken gegarandeerd, waardoor gebruikers niet per ongeluk inloggegevens kunnen verstrekken aan frauduleuze websites. Bovendien vereist deze vorm van authenticatie expliciete actie



van de gebruiker om in te loggen, zoals het drukken op een knop of het goedkeuren via een vingerafdruk.

Een veelgebruikte standaard die phishing-resistente MFA implementeert, is FIDO2. Dit open authenticatiekader, ontwikkeld door de FIDO Alliance, bestaat uit twee componenten: *WebAuthn* en het *Client-to-Authenticator Protocol* (CTAP). WebAuthn is een webstandaard die door browsers en online diensten wordt ondersteund, waardoor gebruikers zich kunnen authenticeren met beveiligingssleutels of ingebouwde authenticators op hun apparaten. CTAP maakt communicatie mogelijk tussen externe authenticators, zoals hardwaretokens of mobiele apparaten, en de cliëntapparaten waarop de authenticatie plaatsvindt.

Een concrete en gebruiksvriendelijke implementatie van FIDO2 is *Passkeys*. Passkeys maakt gebruik van dezelfde onderliggende cryptografische principes, maar is ontworpen om de gebruikerservaring te optimaliseren door naadloze synchronisatie en herstelopties te bieden binnen het ecosysteem van een gebruiker. Door de combinatie van sterke beveiliging en gebruiksgemak wordt Passkeys beschouwd als een belangrijke stap in de brede adoptie van phishing-resistente MFA.

STERKE ALTERNATIEVEN VOOR MFA

MFA wordt vaak voorgesteld als een noodzakelijke beveiligingsmaatregel, maar een sterke beveiliging kan ook zonder MFA worden gerealiseerd. Het probleem dat MFA oplost, ligt vooral in het gebruik van wachtwoorden. Enkelvoudige authenticatie-mechanismen waar geen wachtwoorden aan te pas komen, kunnen dus perfect veilig zijn.

Biometrische authenticatie wordt vaak gepresenteerd als een alternatief voor wachtwoorden. Methoden zoals vingerafdrukken, gezichtsherkenning en irisscans kunnen een gebruiker uniek identificeren. Echter, niet alle biometrische kenmerken bieden dezelfde mate van beveiliging, aangezien de entropie per methode kan variëren. Sommige vingerafdrukscanners, bijvoorbeeld, gebruiken slechts een beperkt aantal

herkenningspunten, waardoor de kans op een *false positive* groter wordt. Daarnaast brengt biometrische authenticatie inherente risico's met zich mee. Waar een wachtwoord gemakkelijk gewijzigd kan worden, is een gestolen biometrisch kenmerk permanent gecompromitteerd. Biometrische kenmerken zijn dus niet geheim en kunnen in bepaalde omstandigheden zelfs op afstand gestolen kunnen worden. Zo slaagde een spreker op het Chaos Communication Congress erin om de vingerafdruk van de Duitse minister van defensie te klonen aan de hand van hoge-resolutie foto's.

Een robuust alternatief voor een wachtwoord is het gebruik van cryptografische sleutels. SSH-sleutels zijn een goed voorbeeld van een wachtwoordloos authenticatiemechanisme en worden vaak gebruikt voor de beveiliging van externe servertoegang. In plaats van een wachtwoord wordt een asymmetrisch sleutelpaar gebruikt, waarbij de privésleutel op een veilige locatie wordt bewaard en de publieke sleutel op de server wordt geïnstalleerd.

Bepaalde hardwaretokens die eenmalige codes genereren, zoals FIDO2-beveiligingssleutels, bieden eveneens een veilige vorm van authenticatie zonder noodzakelijkerwijs als MFA te worden geclassificeerd. Sommige van deze tokens vereisen geen PIN-code of biometrische bevestiging, maar genereren een cryptografisch bewijs dat de gebruiker in bezit is van het fysieke apparaat. Hierdoor wordt een aanzienlijk hoger beveiligingsniveau bereikt dan met wachtwoorden, zonder dat een tweede verificatiefactor noodzakelijk is.

WACHTWOORDLOZE AUTHENTICATIE

MFA heeft zich de afgelopen jaren ontwikkeld uit noodzaak om de tekortkomingen van traditionele wachtwoorden te compenseren. De huidige generatie MFA-methodes, waar het wachtwoord vaak nog een prominente rol speelt, is echter een tussenstap op weg naar een veiligere en gebruiksvriendelijkere authenticatie-infrastructuur. In de toekomst zullen wachtwoorden helemaal verdwijnen om uiteindelijk te komen tot wachtwoordloze authenticatie.

De verschuiving naar wachtwoordloze authenticatie is vandaag al zichtbaar in verschillende technologieën. De smartphone speelt hierin een centrale rol en heeft een fundamentele impact gehad op hoe gebruikers zich aanmelden bij digitale diensten. Dit toestel ontvangt sms-codes, draait authenticator-apps en fungeert als een hardware token in FIDO2-implementaties. Daarnaast hebben geïntegreerde biometrische methoden, zoals vingerafdruk- en gezichtsherkenning, de noodzaak voor handmatige invoer van authenticatiegegevens grotendeels overbodig gemaakt. Hierdoor kan een gebruiker zich aanmelden zonder ooit een wachtwoord in te voeren.

De evolutie richting een infrastructuur zonder wachtwoorden wordt actief ondersteund door grote technologiebedrijven. Microsoft moedigt bijvoorbeeld zijn gebruikers expliciet aan om wachtwoorden te verwijderen en over te stappen op alternatieve authenticatiemethoden. Met de implementatie van sterke gestandaardiseerde oplossingen zoals passkeys zal deze overgang enkel nog versnellen.

4 FUNDAMENTEN VOOR EEN AUTHENTICATIE-INFRASTRUCTUUR

De beveiliging van bedrijfskritische systemen en gegevens steunt op een doordachte authenticatie-infrastructuur. In deze sectie worden verschillende technologieën besproken die een rol spelen binnen die infrastructuur, om zo tot een effectieve en alomvattende oplossing voor het toegangsbeheer binnen de bedrijfsomgeving te komen.

IDENTITEITSBEHEER MET LDAP

Het *Lightweight Directory Access Protocol* (LDAP) is een gestandaardiseerd protocol dat wordt gebruikt voor het benaderen van zogenaamde *directoryservices*, waarin gestructureerde gegevens zoals gebruikers en groepen worden opgeslagen. LDAP is platformonafhankelijk en wordt breed ingezet binnen bedrijfsomgevingen als onderdeel van de authenticatie- en autorisatie-infrastructuur.

LDAP werd in 1993 ontwikkeld als een lichtere versie van het X.500-directoryprotocol en groeide al snel uit tot de standaard voor directorytoegang. De huidige meest gebruikte versie is LDAPv3, zoals gedefinieerd in RFC 4510.

LDAP werkt volgens een client-servermodel waarbij een LDAP-client verbinding maakt met een LDAP-server om gegevens op te vragen of aan te passen. De server kan op zichzelf staan of deel uitmaken van een hiërarchische structuur met meerdere servers die informatie synchroniseren. LDAP biedt een gestandaardiseerd schema voor gegevensopslag en maakt gebruik van het *Directory Information Tree-model*, waarbij de gegevens in een boomstructuur worden georganiseerd. De hoogste niveaus van deze boom vertegenwoordigen algemene organisatorische eenheden, terwijl de lagere niveaus individuele gebruikers, apparaten en andere netwerkentiteiten bevatten.

Het protocol is gebaseerd op vier kernmodellen: het informatiemodel, het naamgevingsmodel, het functionele model en het beveiligingsmodel.

Het informatiemodel definieert hoe gegevens in de directory worden gestructureerd met behulp van objectklassen en attributen. Elke directory-entry bestaat uit een reeks attributen, zoals naam, e-mailadres en wachtwoord. Het naamgevingsmodel bepaalt hoe entries uniek worden geïdentificeerd via *distinguished names*, die de hiërarchische positie van een entry in de directory aangeven. Het functionele model beschrijft de bewerkingen die op de directory kunnen worden uitgevoerd, zoals zoeken, toevoegen, wijzigingen of verwijderen. Ten slotte biedt het beveiligingsmodel mechanismen voor authenticatie en autorisatie.

Binnen bedrijfsomgevingen wordt LDAP vaak gebruikt als basis voor identiteitsbeheer en toegangscontrole. Een van de meest voorkomende implementaties is Microsoft Active Directory, een directorydienst die LDAP als onderliggend protocol gebruikt, maar daarnaast extra functionaliteiten biedt zoals groepsbeleidbeheer en integratie met Windows-domeinen. Active Directory wordt voornamelijk gebruikt in omgevingen die draaien op een Microsoft-infrastructuur.

FEDERATED AUTHENTICATION

Met *federated authentication* kunnen gebruikers met een enkele set inloggegevens toegang krijgen tot meerdere applicaties en domeinen, zelfs wanneer deze zich in verschillende organisaties bevinden. Dit concept speelt een fundamentele rol in moderne IT-infrastructuren waar bedrijven steeds vaker gebruikmaken van cloudgebaseerde diensten en externe applicaties. De kern van federated authentication ligt in het vertrouwen tussen een *identity provider* (IdP) en een of meerdere *service providers* (SP). De IdP beheert en verifieert de identiteit van gebruikers, waarna deze informatie wordt gedeeld met de aangesloten SP's.

Federated authentication kan gebruikt worden voor scenario's waar LDAP niet voor ontworpen is. LDAP werkt uitstekend binnen de grenzen van een organisatie, maar het is minder geschikt wanneer werknemers veilige toegang nodig hebben tot diensten buiten de organisatie, zoals cloudapplicaties.

Federated authentication zorgt voor een scheiding tussen het authenticatieproces enerzijds en de applicaties zelf anderzijds. In plaats van dat elke afzonderlijke service eigen authenticatiemechanismen beheert, wordt de validatie uitbesteed aan de centrale IdP. Dit biedt vele voordelen, zoals verbeterde beveiliging, minder administratieve overhead en een naadloze gebruikerservaring. Daarnaast maakt het gecentraliseerde beheer van identiteiten het eenvoudiger om toegang te verlenen of in te trekken.

Verschillende protocollen ondersteunen federated authentication. De meest gebruikte zijn *Security Assertion Markup Language* (SAML) en *OpenID Connect* (OIDC).

SAML is een XML-gebaseerd protocol dat veilige communicatie mogelijk maakt tussen de IdP en de SP door middel van zogenaamde *assertions*, die informatie over de gebruiker en hun toegangsrechten bevatten. Wanneer een gebruiker een applicatie probeert te openen, wordt een authenticatieverzoek naar de IdP gestuurd. Indien de gebruiker reeds is geauthenticeerd, genereert de IdP een SAML-respons en stuurt deze naar de SP, die vervolgens toegang verleent. SAML wordt veel gebruikt in enterprise-omgevingen en bij cloudapplicaties die compatibiliteit vereisen met oudere systemen.

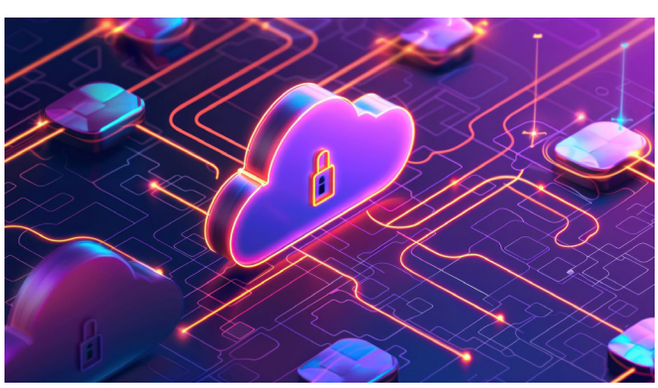
OIDC is een modernere standaard die is gebaseerd op het OAuth 2.0 protocol en daar een identiteitslaag aan toevoegt. Waar OAuth primair gericht is op autorisatie voegt OIDC authenticatiefunctionaliteit toe, waardoor een applicatie de identiteit van een gebruiker kan verifiëren. Dit protocol is het meest gangbaar in hedendaagse federated authentication-oplossingen en vormt de basis voor populaire diensten zoals Google Login en Facebook Login.

AUTHENTICATION AS A SERVICE

Een logische evolutie van federated authentication heeft geleid tot de opkomst van een nieuwe industrie: *authentication as a service* (AaaS). Dit model biedt bedrijven de mogelijkheid om authenticatieprocessen uit te besteden aan gespecialiseerde dienstverleners.

Authentication as a service is een cloudgebaseerde oplossing waarbij authenticatiefunctionaliteiten extern worden beheerd. Dit betekent dat organisaties niet langer verantwoordelijk zijn voor het onderhouden, upgraden en beveiligen van eigen authenticatie-infrastructuur. In plaats daarvan wordt gebruikgemaakt van een schaalbare en gestandaardiseerde dienst. AaaS-oplossingen ondersteunen verschillende authenticatiemethoden, waaronder multifactorauthenticatie en biometrische verificatie, en kunnen eenvoudig geïntegreerd worden in bestaande IT-omgevingen.

De overstap naar AaaS wordt gedreven door verschillende factoren. Enerzijds zorgt de digitalisering van bedrijfsprocessen voor een



toenemende vraag naar efficiënte en veilige authenticatiemethoden. Anderzijds brengt het onderhoud van een eigen authenticatiesysteem bepaalde operationele uitdagingen met zich mee, zoals de noodzaak om gespecialiseerde IT-medewerkers in dienst te hebben en regelmatige investeringen te doen in hardware en software.

Ook voor gebruikers brengt AaaS voordelen met zich mee: ze krijgen gestroomlijnde toegang tot applicaties en systemen, waardoor het gebruiksgemak verbetert en de beveiliging verhoogt.

SINGLE SIGN-ON

Gebruikers in een bedrijfsomgeving moeten vaak meerdere keren per dag inloggen op verschillende systemen en applicaties, wat soms kan leiden tot frustratie, tijdsverlies en een verhoogd risico op het gebruik van zwakke wachtwoorden. *Single Sign-On* (SSO) biedt hiervoor een oplossing door gebruikers na een eenmalige authenticatiestap toegang te geven tot meerdere systemen.

Bij traditionele authenticatieprotocollen zoals LDAP moet elke applicatie die LDAP gebruikt rechtstreeks authenticeren bij de directoryservice, wat leidt tot een versnipperd beheer van sessies en toegangsrechten. SSO lost deze beperkingen op door een tussenlaag in te voeren die fungeert als centrale authenticatiedienst. Wanneer een gebruiker zich eenmaal aanmeldt, wordt een sessie aangemaakt en worden toegangsrechten beheerd via gestandaardiseerde protocollen, waaronder Kerberos, SAML en OIDC.

BEHEER VAN GEPRIVILIGEERDE ACCOUNTS EN SYSTEMEN

Binnen bedrijven bestaan grote verschillen in toegangsrechten tussen individuele accounts. In het bijzonder vormen accounts met uitgebreide privileges, zoals beheerdersaccounts, een risico en moeten daarom gepast beschermd worden. Wanneer dergelijke accounts onvoldoende beveiligd worden, kan dat leiden tot ernstige beveiligingsincidenten. *Privileged Access Management* (PAM) en *Privileged Identity Management* (PIM) zijn

twee beveiligingsmechanismen die kunnen helpen bij het beheer en de bescherming van deze accounts.

PAM richt zich op het beheren en controleren van toegang tot kritieke systemen en gevoelige gegevens. PAM-oplossingen beperken de toegang van gebruikers en processen tot het absolute minimum dat nodig is om hun functie uit te voeren. Dit wordt bereikt door het afdwingen van het principe van *least privilege*, waarbij gebruikers alleen de noodzakelijke rechten krijgen. Bovendien omvat een PAM-oplossing vaak functies zoals sessiemonitoring, waarbij een continue bewaking van de activiteiten van gebruikers sneller toelaat verdachte activiteiten te detecteren.

Naast PAM is er PIM, dat zich specifiek richt op het beheer van accounts met verhoogde rechten. PIM-oplossingen zorgen voor tijdsgebonden en goedkeuringsgebaseerde rolactivatie, waarbij verhoogde rechten alleen worden verleend voor een beperkte periode en onder toezicht van geautoriseerde personen. Dit voorkomt dat accounts met uitgebreide rechten continu beschikbaar zijn en potentieel misbruikt kunnen worden.

Door het beperken en controleren van privileges wordt de kans op misbruik sterk verkleind. Dit is vooral relevant in het kader van geavanceerde aanvallen waarbij aanvallers proberen beheerstoegang te verkrijgen. PAM en PIM helpen bedrijven om deze risico's te minimaliseren door overbodige of ongebruikte rechten te elimineren en de toegang tot gevoelige systemen dynamisch te regelen. Daarnaast kunnen PAM en PIM ondersteuning bieden bij compliance audits. Door middel van logging en monitoring kunnen bedrijven aantonen wie op welk moment toegang had tot specifieke systemen en welke handelingen zijn uitgevoerd.

ZERO TRUST

Waar PAM en PIM inzetten op het controleren van geprivilegieerde accounts en systemen, gaat het concept van *zero trust* nog een stapje verder. In zero trust wordt het principe van least privilege toegepast op de volledige IT-omgeving, inclusief niet-geprivilegieerde gebruikers en systemen. Het uitgangspunt van zero trust is dat een inbraak onvermijdelijk is of reeds heeft plaatsgevonden. Het is dus een kwestie om ervoor te zorgen dat de impact van een aanval geminimaliseerd wordt.

Traditionele netwerkbeveiligingsmodellen vertrouwden op het onderscheid tussen interne en externe gebruikers, waarbij interne gebruikers impliciet als betrouwbaar werden beschouwd. Dit wordt vaak vergeleken met het *castle and moat*-model, waarbij de nadruk lag op het versterken van de buitenste verdedigingslinie, terwijl binnen het netwerk minder strenge beveiligingsmaatregelen golden. Dit model is met de huidige IT-infrastructuur achterhaald: veel bedrijfskritische systemen bevinden zich in hybride of volledig cloudgebaseerde omgevingen, buiten de klassieke netwerkperimeter.

Zero Trust elimineert het concept van vertrouwde interne gebruikers en implementeert authenticatie en autorisatie op meerdere niveaus binnen de infrastructuur. Dit betekent dat gebruikers, apparaten en applicaties voortdurend geverifieerd worden, ongeacht hun locatie of eerdere authenticatie. Hierdoor wordt de laterale bewegingsvrijheid van een eventuele aanvaller in het netwerk sterk beperkt.

CONTINUOUS AUTHENTICATION

Traditionele authenticatiemethodes verifiëren gebruikers doorgaans slechts één keer bij het inloggen, of—bij zero trust—één keer per operatie. Zodra de initiële verificatie is voltooid, blijft de sessie actief zonder verdere authenticatiecontroles. Om de beveiliging verder aan te scherpen, kan gebruik gemaakt worden van *continuous authentication*.

Hierbij wordt de toegang van de gebruiker gedurende de volledige sessieduur voortdurend opnieuw geëvalueerd. Dit beperkt de impact van gestolen inloggegevens, sessiekaping en andere aanvalstechnieken.

Continuous authentication maakt gebruik van een combinatie van gedragsanalyse, biometrische gegevens en contextuele signalen om de identiteit van een gebruiker te valideren. Dit gebeurt zonder merkbare onderbrekingen, tenzij een afwijking van het normale gedrag wordt gedetecteerd. Op basis van een risicoscore, die in real time wordt berekend, kan het systeem beslissen om aanvullende authenticatie te vereisen of de sessie te blokkeren.

Er bestaan verschillende vormen van continuous authentication. Gedragsbiometrie analyseert hoe een gebruiker het apparaat bedient, zoals de manier van typen of hoe de muis beweegt. Fysiologische biometrie, zoals gezichtsherkenning of stemidentificatie, kan ook continu worden gemonitord. Daarnaast kunnen contextuele factoren zoals de locatie, het netwerk waarmee een gebruiker verbonden is, en de gebruikte hardware in overweging worden genomen. Een combinatie van deze methoden verhoogt de betrouwbaarheid van het authenticatieproces.

LEGACY SYSTEMEN

Veel bedrijven maken nog steeds gebruik van legacy systemen die niet compatibel zijn met de meest recente authenticatiestandaarden. Desondanks is het belangrijk om ook deze systemen op een veilige manier te integreren in het bredere authenticatiekader van de organisatie. Een eerste stap in dit proces is het in kaart brengen van alle aanwezige legacy systemen en de bijbehorende authenticatiemechanismen. Dit omvat niet alleen het identificeren van de gebruikte methodes, maar ook het evalueren van mogelijke alternatieve mechanismen die in deze software (eventueel met beperkte aanpassingen) kunnen worden ingezet.

Een veelvoorkomend probleem bij *legacy* systemen is het gebruik van incompatibele of verouderde protocollen, zoals het onversleuteld verzenden van gebruikersnamen en wachtwoorden. Een ander obstakel is de beperkte ondersteuning voor moderne authenticatiemethoden, zoals multifactorauthenticatie. Een mogelijke oplossing is het inzetten van een *protocolconverter*

of *reverse proxyserver* die deze verouderde authenticatiemethoden omzet naar een veiliger alternatief, zoals OAuth 2.0 of SAML. Hiermee kan het bestaande systeem blijven functioneren terwijl het beveiligingsniveau aanzienlijk wordt verbeterd.

In sommige gevallen kan een migratiestrategie nodig zijn om legacy-systemen geleidelijk te vervangen door moderne oplossingen die wel de nodige beveiligingsstandaarden ondersteunen. Wanneer migratie niet haalbaar is, kan het beperken van de toegankelijkheid tot het systeem een potentiële mitigatiestrategie zijn. Dit kan onder andere door netwerkrestricties, zoals IP-whitelisting of verplicht VPN-gebruik, en door het minimaliseren van de beschikbare functionaliteit voor eindgebruikers.

5 HET BELEID VAN DE ORGANISATIE

Naast de technische implementatie van authenticatieprotocollen en -oplossingen moeten bedrijven ook een doordacht en consistent authenticatiebeleid ontwikkelen. Dit beleid is minstens even belangrijk als de technologische maatregelen, aangezien het de praktische toepassing en naleving van de beveiligingsprincipes binnen de organisatie bepaalt.

BEHEER VAN GEBRUIKERS

Uit onderzoek blijkt dat 75% van de *insider threats* afkomstig is van ex-werknemers die nog toegang hebben tot bedrijfssystemen of gevoelige data meenemen. Dit risico kan worden beperkt door een zorgvuldig beheer van gebruikers en hun toegangsrechten. *Identity and Access Management* (IAM) en *Identity Governance and Administration* (IGA) spelen dan ook een centrale rol binnen elk bedrijf als oplossing voor het beheer van gebruikers. IAM is de strategische aanpak die bepaalt wie toegang krijgt tot welke middelen, onder welke voorwaarden en voor welke periode. IGA gaat verder dan IAM door niet alleen te focussen op het provisioneren en authenticeren van gebruikers, maar ook meer naar het operationele aspect te kijken. Het automatiseert processen, verlaagt de bijbehorende kosten en houdt rekening met compliance-eisen.

Een gestructureerd gebruikersbeheer begint bij het administratief proces rond de levenscyclus van een gebruiker. Dit omvat het aanmaken van accounts bij aanwerving, het wijzigen van toegangsrechten bij functiewijzigingen en het onmiddellijk intrekken van toegangsrechten bij vertrek. Wanneer deze processen niet goed werken, verhoogt het risico op ongeautoriseerde toegang en gegevenslekken. Een geautomatiseerd systeem kan helpen om deze processen efficiënt te beheren om zo fouten te minimaliseren.

Het bedrijfsbeleid moet duidelijke richtlijnen bevatten over de gebruikersrechten die worden toegekend op basis van functies en verantwoordelijkheden. Dit voorkomt dat werknemers toegang hebben tot systemen die niet relevant zijn voor hun taken.

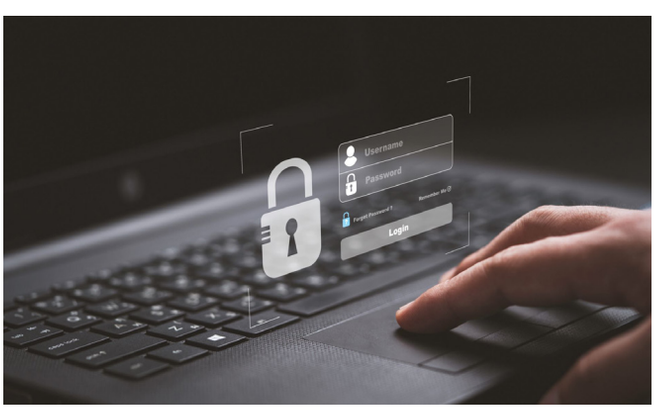
Naast het definiëren van gebruikersrollen en toegangsrechten, moet een organisatie ook inzetten op continue monitoring en periodieke herziening van deze rechten. Regelmatige audits zorgen ervoor dat toegangsrechten up-to-date blijven en dat ongebruikte accounts worden verwijderd. Dit is niet alleen een beveiligingsmaatregel, maar helpt ook bij naleving van bepaalde wetgeving en interne compliance-eisen.

WACHTWOORDBELEID

Het beveiligen van accounts begint met het instellen van een sterke authenticatiemethode. Hoewel we naar een wereld zonder wachtwoorden gaan, blijven wachtwoorden vandaag nog altijd een belangrijk onderdeel van veel authenticatie-processen. Het opstellen en handhaven van een goed wachtwoordbeleid kan garanderen dat wachtwoorden niet eenvoudig misbruikt kunnen worden.

Een betrouwbare bron voor richtlijnen op dit vlak is het National Institute of Standards and Technology (NIST). Recentelijk publiceerde NIST hun vernieuwde richtlijnen voor digitale identiteiten, waarin de best practices voor wachtwoorden beschreven staan.

Naast een aantal voor de hand liggende aanbevelingen zoals de lengte van een goed wachtwoord—bij voorkeur minstens 15 tekens—bevat het document ook enkele minder intuïtieve aanbevelingen. Zo wordt het gebruik van strikte complexiteitsregels, zoals verplichte hoofdletters, cijfers en speciale tekens, afgeraden. Dergelijke eisen maken wachtwoorden niet noodzakelijk veiliger, maar leiden er vaak toe dat gebruikers voorspelbare patronen hanteren of hun wachtwoorden opschrijven. Ook het verplicht periodiek wijzigen van wachtwoorden wordt niet langer als een best practice beschouwd. Hoewel veel bedrijven nog steeds eisen dat wachtwoorden bijvoorbeeld elke 90 dagen worden aangepast, tonen studies aan dat dit eerder een negatief effect heeft op de beveiliging. Gebruikers kiezen in dat geval vaak slechts kleine variaties op hun vorige wachtwoord, wat ze voorspelbaar maakt en dus makkelijker te kraken. In plaats daarvan adviseert NIST om wachtwoorden alleen te wijzigen wanneer er een vermoeden is dat ze gecompromitteerd zijn.



VEILIGE WACHTWOORDOPSLAG

Bedrijven die zelf wachtwoorden verwerken, bijvoorbeeld omdat ze eigen ontwikkelde diensten aanbieden aan klanten, moeten zorgvuldig bekijken hoe ze deze wachtwoorden beheren. De eerste stap is nagaan of het gebruik van een bestaand authenticatiesysteem mogelijk is. Integratie met een *Authentication-as-a-Service-provider* of het inzetten van bestaande, al dan niet commerciële, bibliotheken en implementaties kan de veiligheid en onderhoudbaarheid van het authenticatieproces verzekeren. Wanneer er toch besloten wordt om zelf wachtwoorden op te slaan, dient dit met de nodige voorzorgsmaatregelen te gebeuren.

Een belangrijk risico bij het opslaan van wachtwoorden is dat een aanvaller toegang kan krijgen tot de database. In geen geval mogen wachtwoorden in leesbare tekst bewaard worden. Historisch gezien werd vaak gebruikgemaakt van eenvoudige hash-algoritmes zoals MD5 of SHA-1, maar deze bieden onvoldoende bescherming. Dergelijke algoritmes zijn ontworpen voor snelheid, waardoor aanvallers in staat zijn om met moderne hardware en grootschalige rekenkracht miljoenen hash-bewerkingen per seconde uit te voeren. Dit maakt brute force-aanvallen op gestolen hashes praktisch haalbaar.

Om dit tegen te gaan, werden later algoritmes zoals *bcrypt* geïntroduceerd, waarbij een zogenaamde *work factor* ingesteld kan worden. Deze parameter bepaalt hoe vaak een wachtwoord gehasht wordt voordat het eindresultaat wordt opgeslagen, waardoor de berekeningstijd toeneemt. Naarmate de rekenkracht van hardware toeneemt, kan de work factor verhoogd worden om het beveiligingsniveau te handhaven.

Een moderner en veiliger alternatief is PBKDF2, dat in 2010 door NIST werd gestandaardiseerd en eveneens iteratief werkt om brute-force aanvallen te bemoeilijken.

De OWASP Foundation beveelt momenteel het gebruik van Argon2id aan als de meest geschikte standaard voor veilige wachtwoordopslag. Dit algoritme maakt niet alleen de rekentijd maar ook het geheugengebruik instelbaar, en biedt bescherming

tegen zowel traditionele brute force-aanvallen als geavanceerde GPU-gebaseerde aanvallen. Argon2id minimaliseert bovendien het risico op side-channel-aanvallen door zijn gestructureerde rekenmethode en de mogelijkheid om parallelle bewerkingen te beperken.

Wanneer een bedrijf ervoor kiest om het hash-algoritme te upgraden, is het niet altijd mogelijk om gebruikers te dwingen onmiddellijk een nieuw wachtwoord te kiezen. Er zijn echter betere strategieën om bestaande (onveilige) hashes te upgraden naar veiligere varianten. Een gangbare methode is het herschrijven van de wachtwoordopslag bij elke succesvolle login. Zodra een gebruiker zich aanmeldt met een correct wachtwoord, kan dit direct opnieuw worden gehasht met een moderner algoritme en opgeslagen in de database. Gebruikers die geruime tijd niet inloggen, kunnen gedwongen worden om hun wachtwoord te resetten. Alhoewel dit toelaat de oude hash te verwijderen uit de database, is dit niet gebruiksvriendelijk. Om dit te vermijden, kan een gelaagde hashingtechniek toegepast worden, waarbij een bestaand gehasht wachtwoord wordt gebruikt als invoer voor een nieuw hash-algoritme.

DOORGEDREVEN MONITORING

Een gedetailleerde loggingstrategie is de basis voor een effectieve monitoring van authenticatiestromen en het detecteren van potentiële anomalieën. Door het systematisch vastleggen van alle relevante authenticatiegebeurtenissen kunnen verdachte activiteiten tijdig geïdentificeerd worden. Bij een beveiligingsincident dragen de logs ook bij aan de forensische analyse van de aanval, waardoor zwakke plekken in de beveiliging van het bedrijf blootgelegd kunnen worden.

Het loggen van authenticatiegebeurtenissen biedt inzicht in wie zich probeert aan te melden, wanneer dit gebeurt, vanaf welk apparaat en via welke methode. Zonder deze gedetailleerde informatie blijven belangrijke patronen onopgemerkt. Zo kan een reeks mislukte aanmeldpogingen van verschillende gebruikersnamen vanaf één IP-adres wijzen op een *password-spraying-aanval*, terwijl een aanmelding vanaf een ongebruikelijke geografische locatie kan duiden op een gecompromitteerd account. Door authenticatielogs te analyseren en te correleren met andere beveiligingsgegevens, zoals threat intelligence feeds of firewall-logs, kunnen bedrijven gerichte detectie- en responsmaatregelen implementeren.

Het is dus van belang dat bij het opzetten van monitoringmechanismen gekozen wordt om de logs voldoende gedetailleerd te maken. Naast de standaardinformatie zoals gebruikers-ID, tijdstip en authenticatiemethode, moeten logs ook contextuele gegevens registreren, zoals het bron-IP-adres, gebruikte client-applicatie en eventuele foutcodes bij mislukte inlogpogingen. Bovendien is het noodzakelijk om afzonderlijke gebeurtenissen voor succesvolle en mislukte aanmeldingen bij te houden, aangezien afwijkingen in deze statistieken kunnen wijzen op kwaadaardige activiteiten. Een plotselinge stijging in mislukte aanmeldpogingen zonder overeenkomstige succesvolle logins kan bijvoorbeeld een indicatie zijn van een lopende aanval.

Door logs centraal te verzamelen in een SIEM-oplossing en in real-time te analyseren, kunnen bedrijven afwijkingen sneller detecteren en automatisch waarschuwingen genereren bij verdacht gedrag. Een effectieve monitoringstrategie vereist dus niet alleen dat logs worden verzameld, maar ook dat ze op de juiste manier worden gebruikt. Het opstellen van detectieregels op basis van bekende aanvalspatronen helpt bij het identificeren van potentiële bedreigingen. Daarnaast kunnen machine learning-algoritmes afwijkingen in gebruikersgedrag detecteren die mogelijk wijzen op ongeautoriseerde toegang. Regelmatige audits en het herzien van logging- en monitoringstrategieën zorgen ervoor dat het authenticatiebeleid meegroeit met evoluerende dreigingen en nieuwe ontwikkelingen.

ADAPTIEVE AUTHENTICATIE

Standaard authenticatieprocedures vragen telkens om dezelfde logininformatie, ongeacht de omstandigheden van de authenticatieaanvraag. Adaptieve authenticatie wijkt hiervan af door contextuele factoren mee te nemen in de evaluatie van een inlogpoging. Dit houdt in dat het systeem

niet enkel kijkt naar de ingevoerde gebruikersnaam en het wachtwoord, maar ook naar andere elementen zoals de locatie, het gebruikte apparaat en het tijdstip van de inlogpoging. Op basis van deze gegevens wordt een risicoprofiel opgesteld, waarna de authenticatiemethode aangepast wordt aan het berekende risico.

Adaptieve authenticatie biedt voordelen op het vlak van beveiliging en gebruikerservaring. Gebruikers zullen minder frictie ervaren bij het inloggen, aangezien zij onder normale omstandigheden minder verificatiestappen moeten doorlopen. Indien er echter afwijkingen worden vastgesteld, zoals een loginpoging vanaf een onbekend toestel of een ongebruikelijke locatie, kan het systeem aanvullende verificatie vereisen. Dit kan variëren van een extra factor, zoals een eenmalige code via een authenticator-app, tot een volledige blokkering van de inlogpoging bij een te hoog risico.

Een bijkomend voordeel van adaptieve authenticatie is de mogelijkheid om de berekende risicoscore niet alleen te gebruiken bij de initiële login, maar ook bij andere risicovolle acties binnen het systeem. Deze manier van werken wordt bijvoorbeeld in de financiële sector toegepast: een gebruiker die inlogt op de mobiele app van de bank kan slechts beperkte betalingen uitvoeren, terwijl grotere betalingen enkel na extra validatie via een hardware-token aanvaard worden.

TRAINING EN BEWUSTZIJN

Volgens een recent rapport van Verizon spelen menselijke fouten een rol in 68% van de inbraken. In veel gevallen gaat het dan over het omzeilen van authenticatiemechanismen, waarbij een aanvaller erin slaagt een gebruiker te manipuleren om inloggegevens door te geven of op een andere manier toegang tot beveiligde systemen te krijgen. Bedrijven die een effectief authenticatiebeleid willen voeren, beginnen dus best bij het opleiden van hun werknemers. Wanneer werknemers inzien dat authenticatie een fundamenteel onderdeel is van de cyberbeveiliging van het bedrijf, zullen ze niet alleen minder vatbaar worden voor aanvallen, maar zal ook hun weerstand tegen sterkere authenticatiemethoden, zoals multifactorauthenticatie, afnemen.

Een eerste stap in dit proces is het verstrekken van duidelijke richtlijnen over hoe werknemers hun inloggegevens op een veilige manier beheren. Dit omvat het kiezen van sterke en unieke wachtwoorden, het vermijden van hergebruik en het correct opslaan van inloggegevens met een wachtwoordmanager. Indien multifactorauthenticatie niet verplicht is binnen het bedrijf, moeten werknemers aangemoedigd en begeleid worden bij het activeren van deze extra beveiligingslaag. De rol van het bedrijf is hierbij niet enkel informatief, maar ook faciliterend: door laagdrempelige instructies en ondersteuning te bieden, wordt de drempel voor adoptie verlaagd.

Naast het aanleren van best practices met betrekking tot authenticatie, moeten werknemers ook getraind worden in het herkennen van aanvallen die specifiek gericht zijn op het compromitteren van inloggegevens. Zo blijft phishing de populairste manier om authenticatie te omzeilen. Werknemers moeten leren hoe ze verdachte e-mails, berichten of telefoongesprekken kunnen identificeren. Simulaties en realistische scenario's kunnen helpen om deze kennis in de praktijk te brengen en de waakzaamheid te vergroten.

Een effectief authenticatiebeleid kan echter niet bestaan zonder een open en veilige meldcultuur binnen het bedrijf. Werknemers moeten zich comfortabel voelen om verdachte activiteiten of mogelijke beveiligingsincidenten te rapporteren zonder angst voor negatieve consequenties. Dit is bijzonder belangrijk, want snelle detectie en melding van een potentieel geslaagde aanval kan de impact sterk inperken. Het moet daarom duidelijk zijn dat meldingen gewaardeerd worden en onderdeel uitmaken van een collectieve inspanning om het bedrijf veiliger te maken.

SLOT

Authenticatie blijft een essentiële pijler binnen de beveiligingsstrategie van bedrijven. Klassieke oplossingen, zoals het gebruik van enkel wachtwoorden, zijn achterhaald en vormen een belangrijk risico. Ze zijn vatbaar voor uiteenlopende aanvallen, waaronder phishing, credential stuffing en brute-force-aanvallen. Een sterkere aanpak dringt zich op, maar het bepalen van een effectieve authenticatiestrategie blijft uitdagend.

Bedrijven moeten vandaag inzetten op robuuste multifactorauthenticatie en zich voorbereiden op een overgang naar een wachtwoordloze toekomst. Daarnaast volstaat het niet om enkel extra authenticatiefactoren af te dwingen; een bredere strategie is noodzakelijk. Het beperken van gebruikersrechten volgens het principe van least privilege vermindert het risico van gecompromitteerde accounts. Daarnaast moet misbruik van authenticatieprocessen in real time gedetecteerd worden om er adequaat op te reageren.

Naast technische maatregelen is ook een doordacht beleid rond authenticatie onmisbaar. Bedrijven moeten duidelijke richtlijnen opstellen en werknemers ondersteunen in het veilig omgaan met authenticatiemiddelen. Zonder de juiste omkadering en training blijven zelfs de sterkste technische oplossingen kwetsbaar voor menselijk falen. Een integrale aanpak, waarin technologie, beleid en bewustwording hand in hand gaan, is noodzakelijk om een veilige en efficiënte bedrijfsomgeving te garanderen.

AUTEURS: Pieter Philippaerts, Wouter Joosen, DistriNet, KU Leuven

Publicatiedatum: 14.02.2025