Recommended Practice

Voorkom datalekken met MFA

Knowledge Article

Jaarlijks ontstaan veel datalekken in de categorie hacking, malware of phishing waarbij geen multifactorauthenticatie (MFA) als beveiligingsmaatregel is doorgevoerd.

MFA had waarschijnlijk de impact van deze datalekken kunnen beperken en veel datalekken zelfs kunnen voorkomen.

Daarnaast geldt dat MFA in veel gevallen een essentiële en daarmee verplichte maatregel is om aan de eisen te voldoen uit de Algemene Verordening Gegevensbescherming (AVG). Het niet toepassen van MFA kan leiden tot een overtreding van de AVG. De Autoriteit Persoonsgegevens zal dan ook strenger gaan toezien op het gebruik van MFA. Het juist toepassen van MFA speelt ook een belangrijke rol in het voldoen aan de NTA 7516[1].

Dit document beschrijft wat een MFA is, waarvoor je deze inzet en waarom de juiste toepassing van een MFA zo belangrijk is. Daarnaast worden er een aantal MFA-oplossingen genoemd die we in de markt veelal gebruikt zien worden en leggen we de relatie met de NTA 7516.

Daarmee biedt het handvatten voor CISO, FG en systeem- of werkplekbeheerder voor het bepalen van de juiste strategie rondom de toepassing van MFA binnen de organisatie.

1. https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf

Wat is een MFA?

MFA staat voor Multi-factor Authentication. Een MFA betekent dat je jezelf op verschillende manieren authenticeert om in te loggen.

De bekendste vorm van een MFA is een 2FA, oftewel een Two-factor Authentication. Je authenticeert jezelf dan op 2 manieren, om in te loggen of om ergens toegang toe te krijgen. Een pinpas is een voorbeeld van een 2FA die we regelmatig gebruiken. Je hebt twee dingen nodig om toegang tot je bankrekening te krijgen: je pinpas (iets dat je hebt) en de bijbehorende pincode (iets dat je weet).

Een gebruikersnaam en wachtwoord is overigens geen 2FA, omdat het beide dingen zijn die je weet. We zien een gebruikersnaam en wachtwoord daarom als één manier om jezelf te authenticeren[2].

Er zijn dus verschillende manieren om jezelf te authenticeren. Deze verdelen we onder in de volgende categorieën:

Iets wat je weet

Een gebruikersnaam en een wachtwoord, een pincode of het antwoord op een beveiligingsvraag. Dit zijn allemaal vormen van iets dat je weet en waarmee je je kan authenticeren.

Iets dat je hebt

Een pinpas of een unieke inlogcode ontvangen per sms. Maar ook een code die wordt gegenereerd door een token. Er zijn hardware tokens zoals de RSA SecurID. En er zijn software tokens, zoals een Authenticator App op je mobiele telefoon of MobilePASS. Deze tokens genereren meestal een Time-Based One-Time Password (TOTP). Oftewel een eenmalige inlogcode die continu verandert in de tijd. Mobilepass daarentegen genereert een Event-Based One-Time Password (HOTP).

Iets dat je bent

Hieronder vallen biometrische gegevens die uniek zijn voor ieder persoon. Denk aan een vingerafdruk of je gezicht t.b.v. gezichtsherkenning. Met Microsoft Windows Hello kan je biometrische gegevens inzetten MFA binnen jouw organisatie[3].

Locatie

Vaak kan je een applicatie alleen gebruiken als je bent ingelogd op een thuiswerkomgeving of als je bent verbonden via een VPN-verbinding. Daarmee is de toegang tot de applicatie beperkt tot de (digitale) locatie van jouw organisatie. Je locatie is daarmee een manier om jezelf te authenticeren.

Tijd

De toegang tot een applicatie kan tijdsgebonden zijn. Je kan dan alleen binnen een bepaalde periode inloggen.

Waarvoor gebruik je een MFA?

Een inlognaam en wachtwoord beschermen je account niet voldoende. Het is lastig om een echt sterk wachtwoord te bedenken. Eisen voor een lang of complex wachtwoord werken daarbij een zwak wachtwoord gemakkelijk in de hand[4].

Een lang wachtwoord is namelijk pas sterk als het complex is. Maar daarmee wordt het lastig om te onthouden. Om aan de de minimale lengte van een wachtwoord te voldoen, worden daarom soms delen van het wachtwoord herhaald. Door deze herhaling is een lang wachtwoord niet veiliger dan een kort wachtwoord.

Ook de eis voor een complex wachtwoord leidt zelden tot een sterk wachtwoord. Dit komt doordat bijna iedereen complexe wachtwoordeisen op dezelfde manier toepast. Bijvoorbeeld door een i te vervangen door een 1 en een a te vervangen door een @. Hackers weten dit en spelen daar dan ook op in.

Daarnaast lekken wachtwoorden regelmatig uit. Op dit moment zijn er al meer dan 613 miljoen wachtwoorden wereldwijd uitgelekt. De kans is groot dat hier een wachtwoord tussen zit die in jouw organisatie wordt gebruikt.

Een inlognaam en wachtwoord beschermt je account dus niet genoeg. Door MFA te gebruiken los je dit probleem op. Of het nou gaat om het beveiligen van je privé-mailbox of het beheerdersaccount van Microsoft Exchange. Een MFA gebruiken is altijd een goed idee.

2. https://www.informatiebeveiligingsdienst.nl/product/handreiking-2-factor-authenticatie-2fa-voor-gemeenten/
3. https://docs.microsoft.com/nl-nl/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise
4. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984

Wat is geen MFA?

Zoals eerder is aangegeven is een inlognaam en wachtwoord geen vorm van MFA, omdat het beide dingen zijn die je weet. We zien een gebruikersnaam en wachtwoord daarom als één manier om jezelf te authenticeren.

Verder zien we in de praktijk dat het feit dat je op het bedrijfsnetwerk bent ingelogd, als een MFA wordt gebruikt. Je kunt immers alleen inloggen op het bedrijfsnetwerk als je fysiek toegang hebt tot een werkplek op kantoor. De fysieke toegang tot (een werkplek met toegang tot) het bedrijfsnetwerk is daarmee een vorm van jezelf authenticeren op basis van de locatie.

Dit kan inderdaad als MFA worden gebruikt, mits de toegang tot de werkplekken goed beveiligd is. Bijvoorbeeld doordat de toegang tot een werkplek in het kantoorgebouw alleen toegankelijk is middels een personeelspas.

Daarnaast moet ook de digitale toegang tot het bedrijfsnetwerk via een VPN-verbinding beveiligd zijn met een MFA. Anders staat de spreekwoordelijke achterdeur alsnog open.

Houd er echter rekening mee dat er vaak geen daadwerkelijke fysieke toegang noodzakelijk is om op het bedrijfsnetwerk te geraken. De noodzaak om een personeelspas in te zetten (MFA op basis van locatie) komt daarmee te vervallen. Er zijn gevallen bekend waarbij de Autoriteit Persoonsgegevens hoge boetes heeft uitgedeeld, omdat organisaties geen MFA hadden toegepast binnen de muren van het gebouw5.

De Europese eIDAS-verordening6 beschrijft wat wel en wat niet als een MFA wordt gezien. Daarnaast beschrijft deze verordening ook verschillende betrouwbaarheidsniveau's. Lees hier verderop meer over in de sectie Welke betrouwbaarheidsniveau's bestaan er voor MFA?

Waarom is een 2FA voor Zivver belangrijk?

Jouw organisatie gebruikt (of start binnenkort met) Zivver om gevoelige gegevens veilig te delen met de hele wereld. Om deze gegevens goed te beschermen past Zivver asymmetrical zero-knowledge-encryption toe en wordt je Zivver-account standaard beveiligd met een 2FA7. Zo zijn de gevoelige gegevens optimaal beveiligd.

Als jouw organisatie een MFA-oplossing gebruikt, dan is de 2FA-oplossing van Zivver niet meer noodzakelijk. Zivver vraagt een gebruiker bij het inloggen dan niet langer om een 2FA. Daarvoor moet de gebruiker inloggen in Zivver via Single Sign-On (SSO). De Identity Provider (IdP) van jouw organisatie authenticeert de gebruiker in dat geval middels een MFA.

Kijk op docs.zivver.com hoe je een SSO-koppeling met Zivver opzet en daarbij aangeeft dat de 2FA-oplossing van Zivver niet meer noodzakelijk is.

Zivver zet een 2FA niet alleen in om de toegang tot Zivver-accounts te beveiligen. Ook de toegang tot een bericht kan eventueel met een 2FA worden beveiligd. Zo weet je zeker dat alleen de beoogde ontvanger het bericht kan lezen.

Autoriteit Persoonsgegevens: blik op MFA

In de Jaarrapportage meldplicht datalekken 2020 dat op 1 maart 2021 werd gepubliceerd, is er uitgebreid aandacht voor MFA.

De AP maakt zich zorgen over de blijvende stijging van het aantal meldingen naar aanleiding van hacking, malware of phishing-incidenten. Daarom heeft de AP ervoor gekozen om in deze rapportage extra aandacht te besteden aan MFA. De AP merkt op dat vooral bij dit type datalek MFA de impact van het datalek had kunnen beperken of zelfs had kunnen voorkomen. Naar schatting van de AP waren in 2020 minimaal 600.000 en maximaal 2.000.000 personen (mogelijk) betrokken bij een (gemeld) datalek dat voorkomen had kunnen worden met MFA. Meer over MFA is terug te lezen in het rapport vanaf pagina 7.

Welke MFA-oplossingen zien we in de markt?

Als jouw organisatie geïnteresseerd is in een MFA-oplossing, dan is onderstaand overzicht een goed startpunt:

- Microsoft Windows Hello for Business
- Microsoft Azure AD (Office 365)
- Okta
- OneLogin
- Tools4Ever HelloID
- Ping Identity
- Entrust Solutions SMS Passcode
- Net IQ / MicroFocus
- RSA SecurID® Access

De Informatiebeveiligingsdienst (IBD) heeft de Handreiking 2-Factor authenticatie (2FA) voor gemeenten[8] opgesteld, met daarin een stappenplan voor als jouw organisatie een MFA wilt implementeren. Ondanks dat de IBD zich richt op gemeenten kan het stappenplan uiteraard ook in andere sectoren worden toegepast.

4. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/your-pa-word-doesn-t-matter/ba-p/731984
5. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ziekenhuis-olvg-beboet-om-onvoldoende-beveiliging-medische-dossiers en https://autoriteitpersoonsgegevens.nl/nl/nieuws/haga-beboet-voor-onvoldoende-interne-beveiliging-pati%C3%ABntendossiers
6. https://www.rijksoverheid.nl/onderwerpen/inloggen-in-de-europese-unie-eidas/alles-wat-u-moet-weten-over-eidas
7. https://www.zivver.com/nl/whitepaper-encryptie-privacy-by-design
8. https://www.informatiebeveiligingsdienst.nl/product/handreiking-2-factor-authenticatie-2fa-voor-gemeenten/

Welke betrouwbaarheidsniveau's bestaan er voor MFA?[9]

In de Europese verordening genaamd eIDAS zijn criteria vastgelegd om te bepalen of een oplossing een MFA is. Deze eIDAS-verordening is op 29 september 2018 ingegaan. Vanaf dat moment moeten publieke organisaties en private organisaties met een publieke taak het mogelijk maken dat je als burger kan inloggen met een inlogmiddel die erkend veilig is.

eIDAS onderscheidt drie betrouwbaarheidsniveau's: laag, substantieel en hoog.

De NTA 7516 vereist (in overeenstemming met het type gegevens) dat voor het authenticeren van een verzender en ontvanger een MFA wordt gebruikt met minimaal betrouwbaarheidsniveau substantieel. Als het gaat om gegevens waarop het wettelijk beroepsgeheim van de professional rust, dan is betrouwbaarheidsniveau hoog vereist[10 11].

Niveau 1: eIDAS laag

Een middel met éénfactorauthenticatie volstaat. Denk bijvoorbeeld aan een combinatie van een gebruikersnaam en wachtwoord of een unieke code die de gebruiker ontvangt van een vertrouwde partij.

De doelstelling van eIDAS laag is om het risico van misbruik of wijziging van de identiteit te verkleinen. Dit gebeurt door vast te stellen dat de gebruiker een uniek identificeerbare persoon is [...]. Maar voor toepassing in digitale diensten geldt een beperkte mate van vertrouwen. Het is niet helemaal zeker dat de persoon die zich in de elektronische dienst meldt echt degene is waar u als dienstverlener de identiteit van krijgt doorgegeven. DigiD (basis) is een voorbeeld van een middel op het niveau eIDAS laag.

Lager dan eIDAS laag

Veel authenticatiemiddelen voldoen niet aan de eisen voor eIDAS laag. Het zijn niveau 1-middelen volgens STORK en ISO29015 . Een voorbeeld is een e-mail met daarin een verificatielink die de aanvrager slechts hoeft aan te klikken om het authenticatiemiddel in gebruik te nemen.

9. Bron: https://www.forumstandaardisatie.nl/sites/default/files/BFS/4-basisinformatie/publicaties/fs-handreiking-betrouwbaarheidsniveus-v4_0.pdf
10. Bron: NTA 7156:2019
11. Brief van AP aan minister over patientauthenticatie

Niveau 2: eIDAS substantieel

Voor eIDAS substantieel zijn striktere methoden voor de identiteitsverificatie nodig. Als een gebruiker dit middel aanvraagt, moet daadwerkelijk vastgesteld worden dat hij een geldig, officieel document bezit met dezelfde identiteitsgegevens die gecontroleerd kunnen worden in een basisregistratie. Deze controle mag worden uitbesteed of op afstand plaatsvinden. De controle moet een substantiële mate van vertrouwen bieden.

Als type middel is 2FA vereist. Het middel moet zo ontworpen zijn dat het alleen onder controle van de gebruiker gebruikt kan worden. Het mag niet mogelijk zijn dat het per ongeluk of ongemerkt door een ander kan worden gebruikt.

Ten slotte geldt voor eIDAS substantieel een eis voor het authenticatiemechanisme zelf. Er moet sprake zijn van dynamische authenticatie: de (cryptografische) gegevens voor de authenticatie veranderen bij ieder gebruik, ook wel Time-based One Time Password (TOTP) genoemd. Dit biedt extra bescherming tegen fraudeurs die gegevens willen stelen en hergebruiken.

Een voorbeelden van een middel op het niveau van eIDAS substantieel is SMS-verificatie met inachtneming van het feit dat het gebruikte telefoonnummer geverifieerd is, zoals hierboven beschreven.

Niveau 3: eIDAS hoog

Voor eIDAS hoog moet de gebruiker bij de identiteitsverificatie in aanvulling op de eisen bij niveau substantieel ten minste eenmaal fysiek verschijnen.

Verder moet het middel goed beschermd zijn tegen misbruik door anderen. Denk bijvoorbeeld aan een cryptografisch token, dat echter ook nog een PIN-code vereist, voordat het gebruikt kan worden. Deze PIN-code biedt een extra bescherming tegen misbruik door derden.

Betrouwbaarheidsniveaus en de NTA 7516

In overeenstemming met het type gegevens dat in de NTA 7516 veilig kan worden uitgewisseld (persoonlijke gezondheidsinformatie), moet een passend betrouwbaarheidsniveau voor authenticatie van mensen worden vastgesteld. In de terminologie van de eIDAS-verordening wil dit zeggen dat bij authenticatie minimaal niveau substantieel vereist is. Als het gaat om gegevens waarop het wettelijk beroepsgeheim van de professional rust, is het betrouwbaarheidsniveau hoog vereist[12 13].

Context waarbinnen MFA vereist is

6.1.5 Herkomstbevestiging en 6.1.7. Onweerlegbaarheid verzender

Deze criteria beschrijven dat het aantoonbaar moet zijn dat de verzender daadwerkelijk degene is die zich als zodanig uitgeeft en dat de verzending van een bericht niet kan worden ontkend door de verzender.

In de praktijk betekent dit dat de verzender zich moet authenticeren middels 2FA conform het betrouwbaarheidsniveau substantieel. De authenticatie hoeft niet op de veilige communicatietoepassing te worden toegepast. De professional kan zich ook, bijvoorbeeld met een dergelijk betrouwbaarheidsniveau op een computersysteem aanmelden waarbinnen de veilige communicatietoepassing wordt gebruikt. In dit laatste geval is het uiteraard wel belangrijk dat het wel herleidbaar is (in logging) op welke manier een verzender was geauthenticeerd op het moment van het verzenden van een e-mail. Let op dat dit ook geldt voor het gebruik van mobiele of web clients.

6.1.10 Toegangsvertrouwelijkheid

Dit criterium beschrijft dat de inhoud van berichten uitsluitend door de beoogde ontvanger kunnen worden gelezen en/of verwerkt na het toepassen van een authenticatiemiddel van het betrouwbaarheidsniveau substantieel voor personen en hoog voor professionals.

In de praktijk betekent dit dat een professional die als verzender optreedt, het bericht met een authenticatiemiddel van het betrouwbaarheidsniveau substantieel moet beveiligen. Binnen Zivver vertaalt zich dit naar ontvangerscontrole met SMS, waarbij het telefoonnummer van de ontvanger geverifieerd is. Zie sectie: eIDAS substantieel met Zivver.

Toepasbaarheid Er wordt in de NTA 7516 veelvuldig gerefereerd aan authenticatiemiddelen met betrouwbaarheidsniveau ‘substantieel’ en ‘hoog’. Deze zijn voor de ontvanger en ook de professional nog niet breed beschikbaar. Zolang deze middelen nog niet beschikbaar zijn, moet een authenticatiemiddel worden gebruikt met het hoogst haalbare betrouwbaarheidsniveau dat breed beschikbaar is.

Wanneer de professional als ontvanger optreedt vertaalt dit criterium zich naar de toepassing van 2FA zoals beschreven onder 6.1.5 Herkomstbevestiging en 6.1.7. Onweerlegbaarheid verzender.

eIDAS substantieel met Zivver

Wanneer de professional in het kader van toegangsvertrouwelijkheid een ontvangerscontrole wil toepassen die conform betrouwbaarheidsniveau eIDAS substantieel of hoog is, dan geldt dat er te allen tijde gekozen moet worden voor de SMS-verificatie. Daarbij is het van belang dat het telefoonnummer dat daarvoor wordt ingezet geverifieerd is. Een voorbeeld hiervan is dat het telefoonnummer van een patiënt of andere potentiële ontvanger pas wordt geregistreerd na controle van een geldig identiteitsbewijs en een passende controle van de juistheid van het telefoonnummer. Bijvoorbeeld door het toesturen van een controlebericht.

Afwijken van de het vereiste betrouwbaarheidsniveau

In relatie tot eis 6.1.10 Toegangsvertrouwelijk wordt gesteld dat met name bij elektronische dienstverlening aan burgers kan het voorkomen dat de doelgroep in kwestie nog niet in voldoende mate kan beschikken over een authenticatiemiddel met een voldoende betrouwbaarheidsniveau. In het geval dat het gewenste betrouwbaarheidsniveau nog niet (in voldoende mate) beschikbaar is, gelden de volgende vuistregels:

- Kies voor elektronische dienstverlening, waarbij u het eerstvolgende lagere betrouwbaarheidsniveau verplicht, dat wèl (in voldoende mate) beschikbaar is.
- Stimuleer in dit geval tevens het gebruik van een authenticatiemiddel van het gewenste betrouwbaarheidsniveau, indien burgers hier wel over kunnen beschikken maar dit nog niet gebruiken. Zo kan een doelgroep ook geleidelijk toegroeien naar het juiste betrouwbaarheidsniveau.
- Neem compenserende maatregelen, die het extra risico acceptabel maken, dat volgt uit de keuze van het lagere betrouwbaarheidsniveau.

Let op dat er met betrekking tot eisen 6.1.5 Herkomstbevestiging en 6.1.7 Onweerlegbaarheid verzender er in de NTA 7516 geen onderscheid gemaakt tussen het toepassen van MFA bij inloggen via interne of externe netwerken[14]. Hetzelfde geldt voor het apparaat waar vanaf men omgaat met persoonlijke gezondheidsinformatie. Dit betekent dat er altijd duidelijk in kaart gebracht moet worden vanaf welke apparaten de professional toegang heeft tot de mailbox en voor ieder van deze apparaten een passend beveiligingsniveau moet worden toegepast[15].

12. Bron: NTA 7156:2019
13. Brief van AP aan minister over patientauthenticatie
14. Zie sectie Wat is geen MFA?
15. Zie sectie Welke MFA-oplossingen zien we in de markt? voor mogelijke oplossingen die toepasbaar zijn op de relevante apparaten

Zivver
Kon. Wilhelminaplein 30
1062 KR Amsterdam

085 016 0555
contact@zivver.com

www.zivver.nl