TLP: CLEAR

Toepassing phishing resistente MFA

Ervaringen van Z-CERT met FIDO2 hardware key

De Nederlandse zorg digitaal veilig

versienummer 1.1 - februari 2026

Phishing resistente MFA

Z-CERT benoemt in haar jaarlijkse dreigingsbeeld Adversary-in-the-Middle (AitM) phishing als belangrijke nieuwe dreiging [1]. Zogenaamde “Phishing resistente MFA” zou de oplossing zijn om deze dreiging tegen te gaan. Z-CERT heeft dat zelf inmiddels ingericht en wil met deze publicatie haar ervaringen delen.

Dit doen we door eerst de gebruikte techniek toe te lichten. Daarna bekijken we vanuit verschillende perspectieven de nieuwe manier van MFA: het IT beheer perspectief, het security perspectief, het perspectief van de gebruiker en tenslotte het perspectief van een hacker. We zijn niet de eerste die ervaringen deelt, lees bijvoorbeeld ook een andere Engelstalige publicatie [2] die vooral ingaat op het in gebruik nemen van hardware keys.

Hoe werkt phishing resistente MFA

Phishing-resistente MFA is een vorm van inlogbeveiliging waarbij een aanvaller, zelfs als hij je gebruikersnaam, wachtwoord of tijdelijke inlogcode weet, geen toegang kan krijgen tot de systemen die hiermee zijn beveiligd. De techniek werkt op basis van een methode die cryptografisch bewijs levert dat je als gebruiker je aanmeldt bij de juiste dienst en niet bij bijvoorbeeld een nepwebsite. De belangrijkste technieken hierachter zijn: FIDO2/WebAuthn gebaseerd op security-keys of biometrie, of PKI gebaseerd op smartcards of certificaten.

Tijdens het inlogproces met een resistente MFA-token, stuurt de website of applicatie waarop je inlogt een unieke cryptografische uitdaging (challenge). Je sleutel ondertekent deze uitdaging alleen als het domein of de applicatie waar de challenge vandaan komt klopt. Phishing resistente MFA-keys onderscheiden zich van klassieke MFA doordat de sleutel waarmee je de challenge ondertekent niet door te geven is aan andere gebruikers en domeinen, zoals wel het geval bij bijvoorbeeld een beveiligingscode, sms of push bericht vanuit een app die een code levert. De applicatie stuurt een challenge naar de browser van de gebruiker, hierin staat de “relying party id”, vervolgens is een actie van de gebruiker nodig om de authenticatie in gang te zetten zoals het aanraken van de key of het in de camera kijken in het geval van biometrie.

[1] https://z-cert.nl/actueel/nieuws/dreigingsbeeld2024

Beheerperspectief

Naast de beveiligingsaspecten gaat het voor de beheerorganisatie om drie thema's: kosten, beheeruren en mogelijkheden bieden voor gebruikers.

Kosten en licenties

Bij het gebruik van security keys is de aanschaf van de fysieke keys de enige kostenpost. Er zijn geen aanvullende licenties of abonnementen nodig. In vergelijking met een authenticator-app op een smartphone betekent dit dat er per gebruiker extra kosten ontstaan.

Beheerlast

Naast de financiële kant neemt ook de beheerlast iets toe. Een key is een fysiek apparaat dat moet worden geregistreerd in de CMDB, inclusief het serienummer. Het wordt gekoppeld aan een specifieke gebruiker. Dit brengt extra handelingen met zich mee bij verlies, beschadiging of wanneer een medewerker uit dienst gaat. Denk hierbij aan het deactiveren van de key en het eventueel uitgeven van een nieuwe.

We raden aan om de authenticator-app uit te schakelen voor gebruikers die met een key werken. Alleen dan is het risico op AitM-aanvallen voor deze accounts volledig weggenomen. Gebruikers kunnen dit zelf instellen, maar het is ook mogelijk om dit centraal te beheren voor groepen gebruikers.

Gebruiksvragen en compatibiliteit

Gebruikers stellen weinig vragen over de keys. De tot nu toe enige terugkerende vraag gaat over het gebruik op apparaten zonder USB-C aansluiting, zoals sommige smartphones. In dat geval werkt de key via NFC-technologie. Niet iedereen blijkt daarmee bekend te zijn.

Uitrolstrategie

Bij de uitrol van de keys kun je kiezen voor een volledige implementatie onder alle medewerkers, of juist een gefaseerde aanpak waarbij bijvoorbeeld eerst alleen beheerders worden uitgerust met een key. Een andere optie is om bepaalde groepen, zoals externe

inhuur, gastaccounts of tijdelijke medewerkers, uit te sluiten van het gebruik van keys. Zij blijven dan gebruikmaken van de authenticator-app.

Extra functionaliteit

Beheerders kunnen met één key te authentiseren voor zowel hun reguliere account als hun beheeraccount.

Dit soort keys is geschikt voor multi-factor authenticatie (MFA) binnen Linux-omgevingen.

Security keys bieden aanvullende mogelijkheden, zoals inloggen zonder wachtwoord en het gebruik als smartcard. Voor dat laatste is het wel noodzakelijk om elk apparaat afzonderlijk te configureren, wat extra inspanning vraagt van de IT-afdeling.

Security perspectief

Hoewel security-keys een sterke vorm van beveiliging bieden, kan het beheren van security keys voor grote organisaties veel beheerlast opleveren. Biometrische authenticatie oplossingen die de security key unlocken, bieden hier een alternatief: ze kunnen niet fysiek kwijtraken en zijn daardoor eenvoudiger te beheren. Daarbij maken moderne oplossingen gebruik van een veilige authenticatiestroom. De applicatie stuurt een challenge naar de browser van de gebruiker, inclusief een *relying party ID*. Als een onbekend domein een challenge probeert te starten, weigert de browser deze automatisch.

Daarnaast zijn de zogenaamde *scoped credentials* altijd gekoppeld aan de vooraf geaccepteerde relying party. Dit versterkt de beveiliging aanzienlijk, omdat alleen vertrouwde domeinen toegang krijgen.

Voor organisaties die werken met **BYOD-devices** kan biometrische authenticatie een belangrijke stap zijn. Het combineert gebruiksgemak voor de medewerker met striktere controle voor de organisatie.

Voor zowel de hardware matige security-keys als biometrische authenticatie gelden twee security voordelen:

- de tokens zijn gekoppeld aan domein en gebruiker
- de fysieke/biometrische controle zorgt dat inlogpogingen door bijvoorbeeld bots zullen falen.

Gebruikersperspectief

Onze collega's waren snel gewend aan de key. Ook de niet-security specialisten. Een instructie en korte handleiding hielpen daarbij. Juist door hen wordt het gebruik makkelijker gevonden dan een authenticator-app: daar wilden de schermpjes wel eens op de achtergrond verschijnen, ongeveer tegelijkertijd meerdere tokens gevraagd worden enz.

Vooraf waren er vooral vraagtekens over het gebruik op een telefoon zonder USB-C ingang. Het is dus relevant om dat in de instructie mee te nemen.

Door de key te bewaren bij de andere toegangsmiddelen voor het kantoorpand is er weinig extra risico op het vergeten ervan. Overweeg dan zorgvuldig of het niet tot andere veiligheidsrisico's leidt om alle toegangsmiddelen bij elkaar te bewaren. Dat kan eigenlijk alleen als er geen naam en/of adresgegevens op staan.

Het is belangrijk om na te denken over verlies: dat moeten gebruikers om beveiligingsreden melden. Dat moeten ze dus wel weten… Als je bij herhaaldelijk verlies kosten in rekening wilt brengen behoor je de gebruikers van de key daar vooraf op wijzen.

Verder is het nuttig om een proces in te richten en te communiceren (!) over hoe je in kunt loggen als je toch de key vergeten bent. De eerste weken na de implementatie is het handig om de oude manier van MFA nog actief te houden als back-up.

Hackersperspectief

Klassieke MFA als enige mitigatie is in de praktijk onvoldoende gebleken om kwaadwillenden buiten de deur te houden. Niet alleen zijn aanvallers bekend met het reguliere MFA-proces, maar ze weten ook hoe ze gebruikers kunnen misleiden. Gebruikers zijn inmiddels erg bekend met de authenticator-apps en de verzoeken die ze ontvangen voor toegang tot applicaties vanuit deze apps.

Dit heeft methodes zoals MFA-bombing zeer effectief gemaakt. Bij MFA-bombing krijgen gebruikers in korte tijd veel verzoeken tot toegang, wat de kans vergroot dat een gebruiker een keer op "toestaan" drukt. Deze klassieke vorm van MFA is vatbaar voor AitM phishing of te omzeilen met transparante proxies en Man-in-the-Middle (MiTM) aanvallen.

MFA is dus geen enorm obstakel meer voor hackers. Met wat voorkennis van een organisatie en goede reconnaissance is het goed mogelijk om phishingaanvallen op te zetten die voor een gebruiker niet van echt te onderscheiden zijn.

Phishing-resistente MFA is hierin complexer. Met deze nieuwe MFA technieken is het voor aanvallers een stuk lastiger gemaakt om toegang te krijgen. Social enigneering wordt met deze nieuwe authenticatie methodieken bemoeilijkt. Doordat dit een nieuwe methode is, ontstaat er ook een nieuw bewustzijn bij gebruikers om alerter te zijn op het proces.

Omdat de authenticatiestroom niet volledig online plaatsvindt, zijn er minder mogelijkheden voor een aanvaller om met bekende aanvalsmethodieken authenticatiesleutels af te vangen.

Toch blijft het ook bij phishing-resistente MFA van belang om deze beveiliging te combineren met Conditional Access. Dit maakt het voor kwaadwillenden in de meeste gevallen veel moeilijker om zichzelf toegang te verschaffen tot de infrastructuur van jouw organisatie.