///Phishing Resistant Multifactor-authenticatie

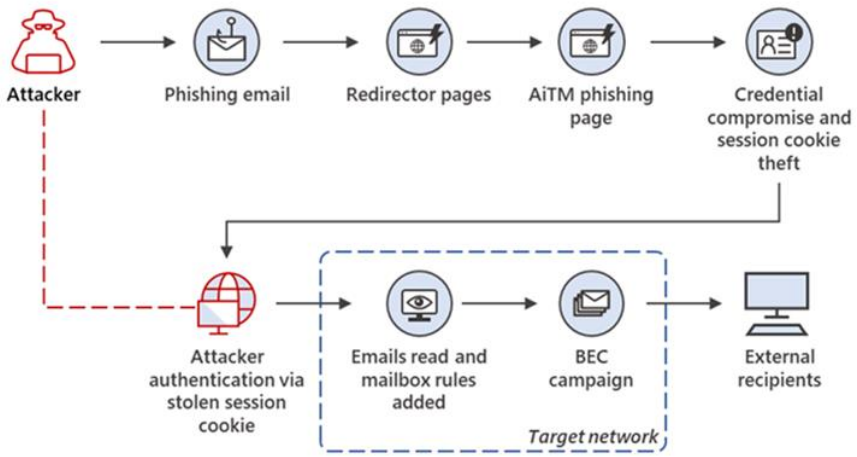
1 INTRODUCTIE

Phishing staat met stip op nummer één als het gaat over de oorzaken van cyberveiligheidsincidenten. Om beter bestand te zijn tegen phishing aanvallen, wordt dringend aangeraden om multifactor-authenticatie (MFA) te implementeren binnen uw lokaal bestuur. Met het veranderende dreigingenlandschap is normale MFA echter niet genoeg om bestand te zijn tegen cybercriminelen.

Cybercriminelen maken steeds vaker gebruik van 'adversary-in-the-middle' aanvallen. Dit type cyberaanval is een geavanceerde vorm van traditionele phishing waarbij een geautoriseerde cookie (bijv. de cijferreeks die uw multifactor-authenticatie applicatie genereert) verkregen wordt. Eenmaal dat cybercriminelen dit cookie hebben, kunnen zij deze gebruiken op een ander toestel om zo toegang te krijgen tot hetzelfde account.

Afhankelijk van de permissies van het gehackte account en de mogelijkheden van de cybercrimineel om binnen uw netwerk toegang te krijgen tot andere accounts of data kan de impact van een dergelijke aanval variëren.

Afbeelding 1: De 'adversary-in-the-middle' aanval



Bron:https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

2 AANBEVELINGEN

Om 'adversary-in-the-middle' aanvallen te voorkomen, is het noodzakelijk om af te dwingen dat multifactor-authenticatie op basis van phishing-resistant tokens wordt afgedwongen. Dit betekent dat de tokens die uw MFA-applicatie genereert slechts één keer gebruikt kunnen worden of tijdsgebonden (bijv. 30 seconden) zijn.

In de praktijk betekent dit voor u als lokaal bestuur dat uw MFA-authenticaties via een FIDO2 token, Windows Hello for Business of Certificate-based authentication dienen te lopen.

Concrete voorbeelden van FIDO2 tokens zijn o.a.:

- **Dedicated hardware keys**: Google Titan/ Yubico u2f security key
- **Device bound passkeys**: Opslag van FIDO2 tokens in de security chip op het gebruikte toestel (bv: TPM voor Windows toestellen, secure enclave voor MAC toestellen, iPhone of Android toestel)
- **Passkeys in credential managers:** Tegenwoordig ondersteunen password managers ook reeds passkeys zodat deze op verschillende toestellen gebruikt kunnen worden

Het spreekt voor zich dat elke authenticatie die via MFA verloopt een veiligere oplossing is dan enkel te authentiseren via een gebruikersnaam en wachtwoord. Afhankelijk van uw risico appetijt kan het interessant zijn om gebruik te maken van dedicated hardware keys (fysieke tokens) of te kiezen voor een meer praktische implementatie van phishing-resistant tokens (bijv. via Windowns Hello for Business).

3 MITIGATIE EN IMPLEMENTATIE

Vanuit het Cyber Response Team komt het dringende advies voor alle lokale besturen die gebruik maken van een MFA-oplossing om te controleren of er op basis van de instellingen van de authenticatiesterkte een phishing-resistant token verplicht kan worden bij de authenticatie.

Lokale besturen die gebruik maken van Entra ID als hun MFA-oplossing, vinden hier meer informatie over hoe u dit kunt inrichten.

Indien u als lokaal bestuur nog geen gebruik maakt van een MFA-oplossing, wordt er nogmaals dringend een oproep gedaan om MFA te implementeren.

4 VERKLARENDE WOORDENLIJST

Term	Verduidelijking	Link naar meer informatie
MFA	Multifactor-authenticatie is een elektronische authenticatiemethode waarbij gebruikers pas toegang krijgen tot een website of applicatie	https://www.vlaanderen.be/digitaal-vlaanderen/toegangsbeheer

	nadat gebruikers zich twee (of meer) keer geauthentiseerd hebben.	
U2F	Universal 2nd Factor is een authenticatie standaard die gebruikt maakt van een of meerdere diensten	https://www.okta.com/identity-101/u2f/

5 REFERENTIES

- Documentatie over de 'adversary-in-the-middle' aanval: https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/
- Documentatie over het kiezen van de juiste authenticatie sterkte: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/authentication-strength-choose-the-right-auth-method-for-your/ba-p/2365674
- Goede praktijken rond identiteit- en toegangsbeheer (CCB): https://cyberguide.ccb.belgium.be/nl/identiteit-toegangsbeheer
- Minimale IAM maatregelen Vlaamse Overheid: https://assets.vlaanderen.be/image/upload/v1663779254/Vo_Informatieclassificatie_-_Minimale_maatregelen_-_IAM_xle0xg.pdf