maart 2023

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Volwassen authenticeren

Is uw organisatie voldoende beschermd tegen phishing middels authenticatie?

Wat is volwassen authenticeren?

Met authenticatie bepaalt u de identiteit van een gebruiker. Het wachtwoord is de meest gebruikte vorm. Maar daar zitten diverse nadelen aan; wachtwoorden zijn niet gebruiksvriendelijk waardoor mensen makkelijk te achterhalen wachtwoorden kiezen, en wachtwoorden kunnen worden gestolen door bijvoorbeeld phishingaanvallen.

Er zijn nu nieuwe, wachtwoordloze technieken voor authenticatie die het voor gebruikers makkelijker maken, en voor de organisatie veiliger. Het volwassenheidsmodel voor authenticatie helpt om gebruikersaccounts beter te beschermen en in de toekomst beschermd te houden. Phishing wordt daarmee nagenoeg onmogelijk. Zo blijft u de aanvallers een stap voor.

Waarom volwassen authenticeren?

Uw werk stilgelegd door een ransomware-aanval; uw data op straat door datadiefstal; uw bedrijfsgeheimen gestolen door digitale spionage. Veel verschillende digitale aanvallen beginnen met de diefstal van één wachtwoord via phishing. Nu steeds meer organisaties tweefactorauthenticatie toepassen wordt ook die tweede factor steeds vaker gestolen bij een phishingaanval. Het is belangrijk om de aanvallers écht een stap voor te blijven met volwassen authenticatietechnieken.

Hoe maakt u uw organisatie klaar voor volwassen authenticatie?

Stappenplan volwassen authenticatie

Stap 1
Inventariseer al uw gebruikersaccounts:
- Intern en extern (medewerkers en klanten)
- Lage en hoge autorisatie (gebruikers en beheerders)

→

Stap 2
Bepaal per groep de impact van aanvallen op die accounts

→

Stap 3
Geef prioriteit aan de accounts met de hoogste impact

→

Stap 4
Beveilig (op termijn) alle accounts met phishingbestendige authenticatie

Volwassenheidsmodel

U kunt nu uw organisatie indelen in onderstaand volwassenheidsniveau. Bij een niveau lager dan 2 raden wij aan tot actie over te gaan. Hoe meer autorisaties, des te groter de impact.

Niveau 0:
- O Geen inventarisatie van low-, medium- en high-impact accounts.
- O Accounts alleen beveiligd met gebruikersnaam en wachtwoord.

Niveau 1:
- O Inventarisatie van low-, medium- en high-impact accounts.
- O Tweefactorauthenticatie voor medium- en high-impact accounts.

Niveau 2:
- O Inventarisatie van low-, medium- en high-impact accounts.
- O Phishingbestendige authenticatie op high-impact accounts.
- O Tweefactorauthenticatie op low- en medium-impact accounts.

Niveau 3:
- O Inventarisatie van low-, medium- en high-impact accounts.
- O Phishingbestendige authenticatie op medium- en high-impact accounts.
- O Tweefactorauthenticatie op low-impact accounts.

Maak uw organisatie klaar voor volwassen authenticatie.

In de factsheet *Volwassen Authenticeren* leest u welke afwegingen u kunt maken bij het bepalen van een geschikte authenticatiemethode voor de accounts en systemen binnen uw organisatie.

Factsheet Volwassen authenticeren *(ncsc.nl)*