dhs addsecurity Authentication

Dienstbeschrijving

Auteur(s): Sander van der Post

Datum: 02 november 2021
Kenmerk: DB_addsec_AaaS_v2_1
Status: Definitief

dhs informatisering
Kanaalstraat 12b
5347 KM Oss
Nederland

0412-653800
info@dhs.nl
www.dhs.nl
kvk 16052550

btw NL008180349B01
Rabobank
iban NL64 RABO 0140440062
swift RABONL2U

adding value

1 Inhoudsopgave

2 Authentication-as-a-Service

2.1 Introductie

Het is niet de vraag of dat een gebruikersaccount gehacked kan worden, het is meer de vraag wanneer het gebeurt. Het nieuws staat er vol van: Accountgegevens worden met de duizenden tegelijk gestolen en publiekelijk verkocht.

De reden dat deze handel zo levendig is, is eenvoudig. Het is voor de gemiddelde hacker enorm eenvoudig om accountgegevens te achterhalen. Enerzijds kan dit door het stelen van deze accountgegevens op websites welke slecht beveiligd zijn. Anderzijds door het achterhalen van gebruikersnamen en wachtwoorden door "phishing", social hacking of andere slimme methodes. Deze gegevens worden vervolgens verkocht en gebruikt voor identiteitsfraude, data diefstal of andere illegale bezigheden.

Het is vervelend als iemand zijn Facebook account wordt gehacked, maar wat als iemand met accountgegevens van uw medewerkers zich toegang verschaft tot uw bedrijfsdata? En om hier toegang tot te krijgen, hoeft de hacker helemaal niet uw systemen te hacken. Uw medewerkers gebruiken in veel gevallen wachtwoorden welke zij ook privé gebruiken, of zij gebruiken de identieke combinatie van gebruikersnaam en wachtwoord voor websites van leveranciers of klanten. Wanneer een (populaire) openbare website gehacked wordt, liggen in veel gevallen de accountgegevens van uw medewerkers al voor het oprapen.

Het is eenvoudig; een gebruikersnaam en wachtwoord zijn niet meer voldoende om uw gegevens te beschermen. Dit wordt al enige tijd erkend door marktleiders zoals Apple, Google en Microsoft. Zij verplichten steeds vaker om Multi Factor Authenticatie toe te voegen aan gebruikersaccounts van bijvoorbeeld icloud.com, Facebook, etc. Naast een gebruikersnaam en wachtwoord, is er dan altijd nog een extra stap nodig om toegang te verkrijgen tot de website.

Hoogste tijd dat ook de zakelijke markt deze extra laag van beveiliging op grote schaal introduceert in haar technische infrastructuur. Of dat het nu gaat om de toegang te beschermen tot Remote Working oplossingen, Microsoft 365 of VPN verbindingen; alle extern benaderbare ingangen tot zakelijke data moeten beschermd worden met meer dan alleen een gebruikersnaam en wachtwoord.

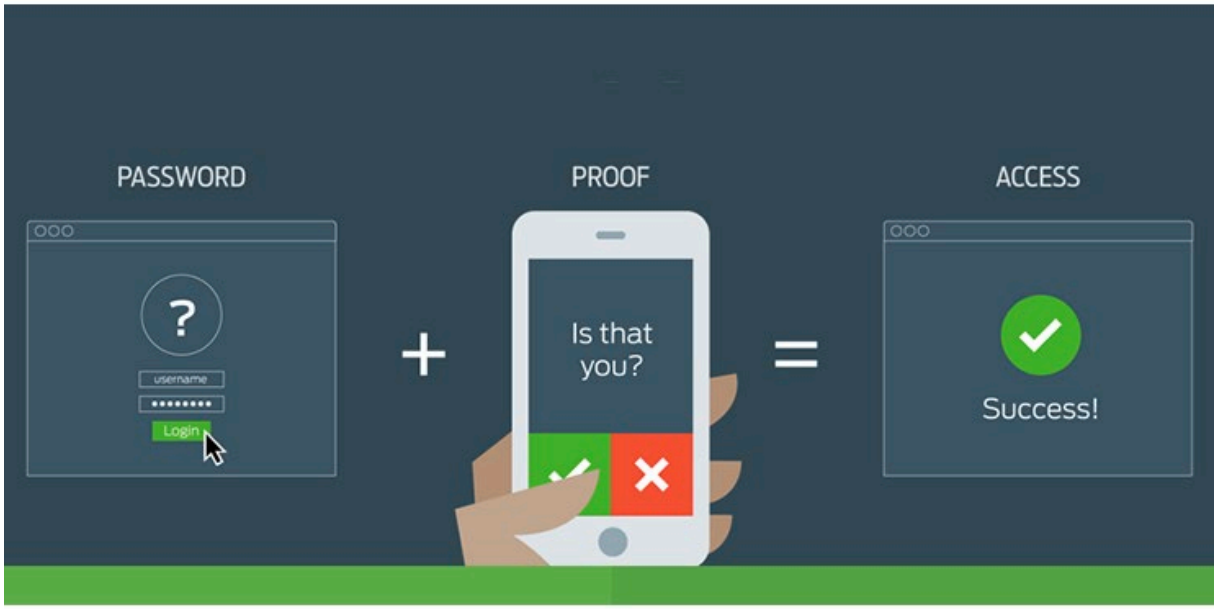
2.2 Hoe werkt Multi Factor Authenticatie

Het inloggen met uitsluitend een gebruikersnaam en wachtwoord is gebaseerd op iets dat de gebruiker weet. Omdat een gebruiker deze informatie goed moet kunnen onthouden, kiest hij of zij vaak voor hetzelfde wachtwoord of eenvoudig te achterhalen wachtwoorden. Deze informatie kan door anderen worden misbruikt, zonder dat de gebruiker hier weet van heeft.

Het aanmelden met een Multi Factor Authenticatie oplossing haalt de potentiële zwakte van het wachtwoord uit de vergelijking. Middels Multi Factor Authenticatie worden meerdere gegevens gebruikt om iemand zijn identiteit te verifiëren. Minimaal drie gegevens types moeten kloppen om de authenticatie te laten slagen. Pas hierna wordt er toegang verkregen tot de data of ICT-functionaliteiten welke gewenst zijn.

Een Multi Factor Authenticatie oplossing is dus gebaseerd op minimaal onderstaande gegevens:

- Wie je bent (gebruikernaam)
- Wat je weet (wachtwoord)
- Wat je hebt (persoonlijke Multi Factor App)



Ondanks dat mogelijk het wachtwoord van de gebruiker achterhaald of gestolen is, dan nog kan er geen toegang verschaft worden tot de data of ICT-faciliteiten. De Multi Factor App is persoonlijk, net zoals dat de App van de bank. Deze werkt alleen op de Smartphone van de gebruiker en kan niet gekopieerd of overgezet worden.

Mocht onverhoopt de smartphone van de gebruiker ook gestolen worden, dan merkt de gebruiker dit in veel gevallen direct. Hierop kunnen dan ook direct passende maatregelen genomen worden om de Multi Factor App op afstand onbruikbaar te maken.

2.3 Waarom "as-a-Service"

De voordelen van een Multi Factor Authenticatie oplossing zijn duidelijk. Er wordt een extra laag van beveiliging toegevoegd aan standaard authenticatie oplossingen welke gebaseerd zijn op alleen gebruikersnaam en wachtwoord. Naast dat deze toevoeging van beveiliging in het belang van de organisatie is, wordt het vandaag de dag ook steeds vaker geëist vanuit Data Security / AVG / GDPR oogpunt. Het beschermen van data en de toegang hiertoe is een "must" vanuit deze interne en externe richtlijnen.

dhs ziet echter ook dat veel organisaties wel gebruik zouden willen maken van een dergelijke oplossing, maar niet de kennis of investeringsmiddelen hebben om dit in te voeren. Oplossingen als Multi Factor Authentication, zeker geïntegreerd in een bedrijfsnetwerk, waren tot voorkort alleen haalbaar voor de grote Enterprises of voor hen met een aanzienlijk budget voor ICT-beveiligingsoplossingen. En heel eerlijk, het liefst geeft geen één organisatie geld uit aan dit soort oplossingen. Het is immers een "noodzakelijke" kwaad, om een nog groter kwaad te bestrijden.

dhs heeft om deze reden de Authentication-as-a-Service gelanceerd in haar dienstenportfolio. Deze dienst biedt de relaties van **dhs** een compleet state-of-the-art Multi Factor Authenticatie platform aan.

2.3.1 Voordelen

De voordelen van Authentication-as-a-Service ten opzichte van een eenmalige investering in een Multi Factor Authentication oplossing zijn de volgende:

- **Kosten:** In plaats van eenmalige investeringen in een Multi Factor Authentication oplossing (Licenties, (Soft)tokens, servers, onderhoud, etc.), wordt de dienst aangeboden in een abonnementsvorm voor een bedrag per medewerker per maand. Het grote voordeel hierbij is dat organisaties naar een heldere kostenstructuur per maand gaan (OPEX) en niet geconfronteerd worden met vaak hoge eenmalige investeringen (CAPEX). Tevens kan een abonnementsvorm eenvoudig mee schalen met de ontwikkelingen van de organisatie.

- **Ultieme veiligheid:** De dienst voorziet niet alleen in het platform voor Multi Factor Authenticatie, maar biedt ook continu beheer op de deze infrastructuur. Dit houdt in dat dagelijks de omgeving bewaakt wordt of, er geen ongeautoriseerde pogingen om toegang te verschaffen zijn geweest en of dat de laatste beveiligingsupdates zijn doorgevoerd. Dit laatste is zeker in het kader van gegevensbeveiliging een "must have" voor veel organisaties, om zo zeker te zijn dat persoonlijke gegevens niet onnodig verloren gaan of in verkeerde handen terecht komen.

- **Meer mogelijkheden:** Techniek kan kostbaar zijn, zeker wanneer deze van "Enterprise" waardig niveau is. Ondanks dat organisaties baat kunnen hebben bij bepaalde functionaliteiten welke een dergelijke oplossing kan bieden, wordt vanwege de kosten in veel gevallen gekozen voor een minder functionele oplossing. Dankzij de Authentication-as-a-Service dienst van **dhs**, en haar keuze in technologie en daarmee de beschikbare functionaliteiten, kan nu iedere organisatie voor een aantrekkelijk bedrag per maand beschikken over de meest geavanceerde beveiliging en functionaliteiten. Denk hierbij aan Single Sign On, Company Application Portal, etc.

- **Schaalbaarheid / Flexibiliteit:** Wanneer de organisatie groeit in het aantal medewerkers, is het van belang dat het Multi factor Authenticatie middelen direct meegroeien in aantal. De Authentication-as-a-Service dienst kan eenvoudig uitgebreid worden met extra gebruikers, om zo de groeiende organisatie direct te ondersteunen.

Bovenstaande zijn slechts een selectie van de voordelen welke een Authentication-as-a-Service dienst kan bieden ten opzichte van een eenmalig aangekochte oplossing. Samenvattend ontzorgt **dhs** middels haar Authentication-as-a-Service dienst de organisatie als het gaat om het verhogen van de veiligheid van haar data en ICT-infrastructuren.

2.4 Inhoud van de dienst

Zoals beschreven is Authentication-as-a-Service een dienst, welke voor een maandelijks bedrag geleverd wordt aan de uw organisatie. De dienst wordt geleverd per gebruikersaccount. Om te definiëren op welke wijze Multi Factor Authenticatie in de situatie van uw organisatie ingezet kan en moet worden, wordt er initieel een inventarisatie uitgevoerd door de specialisten van **dhs**. Middels deze inventarisatie wordt helderheid verschaft in welke authenticatie methodieken toegepast kunnen worden en op welke toegang(en) tot de ICT-infrastructuur beveiligd moeten worden.

dhs biedt de volgende zaken aan binnen de dienst Authentication-as-a-Service:

1. **Multi Factor Authentication Platform**
   Het technische hart van iedere Multi Factor Authentication oplossing, is het authenticatie platform. Dit platform beheert en monitort alle toegangsverzoeken, gebruikers en uitgegeven toegangsmiddelen (Smartphone App Authenticator).

   Door gebruik te maken van **dhs** Authentication-as-a-Service, maakt u gebruik van een state-of-the-art platform, gehost door een wereldwijd erkende leverancier.

2. **Authenticator**
   Waar vroeger nog wel eens gebruik werd gemaakt van zogenaamde hardware tokens (sleutelhangers welke een code genereerde), maakt **dhs** gebruik van de meest innovatieve Smartphone App Authenticators in de markt. Voor iedere gebruiker wordt een Smartphone Authenticator App beschikbaar gesteld. Deze Authenticator App is beschikbaar voor zowel Apple IOS als Android gebaseerde devices.

   Het Multi Factor Authentication Platform zal naar de gedefinieerde gebruikers een interactieve installatie en activatie procedure sturen, waarmee de gebruiker zelf zijn Authenticator App kan instellen en direct gaan gebruiken.

   Het optioneel gebruiken van YubiKeys, SMS authenticatie of Emergency Access Codes worden eveneens ondersteund door het Authentication-as-a-Service platform.

3. **Beheer en onderhoud**
   Het eenmalig installeren en configureren van een authenticatie oplossing is niet afdoende. Dagelijkse beheer is benodigd om een dergelijke oplossing beschikbaar en veilig te houden. Om deze reden biedt de dienst de volgende activiteiten:

   a. **Monitoring:** Continue monitoring van het Multi Factor Authenticatie Platform, borgen de werking en potentiele gevaren (ongeautoriseerde pogingen tot aanmelden) worden hiermee direct gedetecteerd.
   b. **Patches & Updates:** Patches en updates, zeker welke nieuwe beveiligingsrisico's oplossen, worden doorgevoerd op zowel het platform als binnen de Authenticator App.
   c. **Gebruikersbeheer:** het koppelen en ontkoppelen van gebruikersaccounts aan de Multi Factor Authentication oplossing en Authenticators.
   d. **Instructie:** Zowel een interactieve als beschreven instructie wordt aangeboden aan de gebruikers om zo zelfstandig gebruik te maken van de Multi Factor Authentication oplossing.
   e. **Support:** Gebruikersvragen of problemen met betrekking tot de Multi Factor Authentication oplossing kunnen rechtstreeks gemeld worden bij de **dhs** servicedesk. Een team van professionals staan dan klaar om de gebruiker zo snel mogelijk weer op weg te helpen.

2.5 Installatie, Configuratie en Integratie

De Authentication-as-a-Service dienstverlening wordt volledig, passend bij uw organisatie haar wensen en eisen, geïnstalleerd, geconfigureerd en geïntegreerd in de huidige ICT-infrastructuur. Deze installatie dienst kent een eenmalige vaste investering op basis van de "**dhs** Standaard Installatie" definitie. De inhoudt van deze installatie procedure is als volgt:

- **Installatie**
  Installatie van Authentication Synchronization Agents op te beveiligen servers of toepassingen. Een kort overzicht van mogelijke servers / services:
  - Microsoft Windows Remote Desktop Services
  - Microsoft Active Directory Services
  - Microsoft 365 Services
  - Microsoft Azure Services
  - VMware Horizon View Services
  - Citrix NetScaler Services
  - Standaard Radius Services
  - En nog vele andere Webbased en SaaS applicaties, waaronder:
    - AFAS
    - Google Workspace
    - Salesforce
    - DocuSign

- **Configuratie**
  Binnen de Multi Factor Authenticatie oplossing worden regels (rules en policies) ingesteld welke passen bij de wensen en eisen van uw organisatie. Denk hierbij aan de noodzaak om iedere keer te autoriseren, of alleen wanneer er toegang gezocht wordt vanaf bepaalde locaties. Samen met de **dhs** specialist worden deze mogelijkheden aan u voorgelegd.

- **Integratie**
  De te beveiligen servers / services moeten in sommige gevallen aangepast worden om te begrijpen dat een extra beveiligingsmiddel is toegevoegd aan de normale gebruikersnaam / wachtwoord combinatie. Deze integratie wordt volledig voor u verzorgt.

3 Dienstverlening dhs

Voor alle diensten beschreven in dit document, als ook overige diensten geleverd door **dhs** onder de merknamen van **dhs addcloud**, **dhs addcontrol**, **dhs addwireless**, **dhs addsecurity** en **dhs addbackup**, geldt dat deze onderhevig zijn aan een onderliggende "Service Level Agreement (SLA)". Deze Master SLA is opvraagbaar bij **dhs** en/of te downloaden via de website van **dhs** (www.dhs.nl).

4 Contractduur, looptijd en verlenging

De dienst **dhs** Authenticatoin-as-a-Service wordt u aangeboden als een abonnement met een bepaalde contractlooptijd.

- Standaard wordt deze overeenkomst aangegaan voor een periode van 36 maanden;
- De overeenkomst is niet tussentijds opzegbaar;
- Opzegging dient schriftelijk en uiterlijk 2 maanden voorafgaande aan einddatum te geschieden;
- Indien geen opzegging heeft plaatsgevonden wordt de overeenkomst automatisch met periodes van 12 maanden verlengt.

Overige bepalingen en voorwaarden staan beschreven in de onderliggende Service Level Agreement.