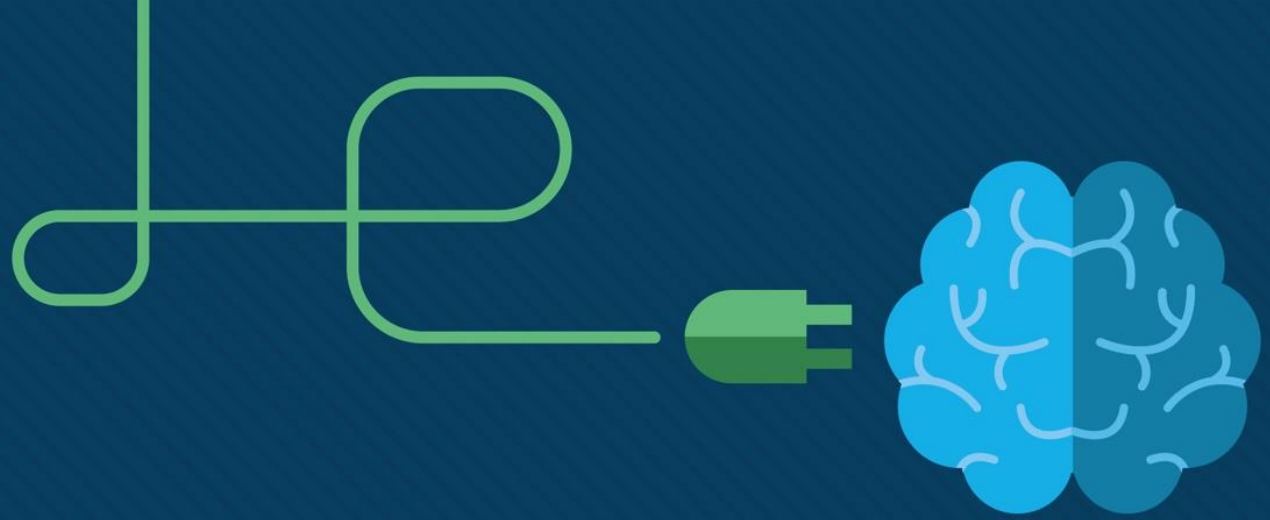


Webinar: Cybersecurity, identity & access management

Een samenwerking tussen de Cisco Networking Academy, KIVI en Stysec

20 mei 2020

Dr. Rob van der Staaij CISSP CCSP CISA CISM CRISC CEH CPT

rstaaij@gmail.com

Wat is identificatie?

- Verifiëren van de identiteit van een subject (meestal een persoon, maar applicatie of apparaat kan ook) ten behoeve van
  - Registratie
  - Genereren of uitgeven van authenticatiemiddelen en andere toegangshulpmiddelen
- Meestal eenmalig proces
- Voorwaarde voor authenticatie
- Bepaald betrouwbaarheidsniveau nodig
  - Afhankelijk van het risicoprofiel van de informatie die met de authenticatiemiddelen kunnen worden benaderd

KIVI Engineering Society

Networking Academy

Stysec

Wat is identificatie?

- Voorbeelden
  - Indiensttreding bij organisatie
  - Openen bankaccount
  - Registratie bij identity provider
  - Registratie bij webshop
  - Registratie bij nieuwe smartphone
- eIDAS voorziet in regulering over betrouwbaarheidsniveaus
  - Laag
  - Substantieel
  - Hoog

KIVI Engineering Society

Networking Academy

Stysec

Wat is authenticatie?

- Verifiëren van de identiteit ten behoeve van het verkrijgen van toegang
  - Subject biedt een of meer authenticatiemiddel(en) aan bij het informatiesysteem of faciliteit waartoe toegang gewenst wordt
  - Authenticatie volgt altijd na identificatie met bijbehorende registratie en de uitgifte of het genereren van authenticatiemiddelen; zonder een authenticatiemiddel is het verkrijgen van toegang immers niet mogelijk
- Meestal herhaald proces
- Voorwaarde voor autorisatie
- Net als bij identificatie is bepaald betrouwbaarheidsniveau nodig
  - Afhankelijk van het risicoprofiel van de informatie die met de authenticatiemiddelen kunnen worden benaderd

KIVI Engineering Society

Networking Academy

Stysec

Enkelvoudige authenticatie

- Bij het authenticatieproces wordt slechts één bewijsfactor ter verificatie aangeboden ter verificatie van de identiteit
  - In verreweg de meeste gevallen is dit nog altijd een combinatie van gebruikersnaam (identiteit) en een wachtwoord (bewijsfactor)
- Andere voorbeelden
  - Verkrijgen van toegang tot diensten van service provider met OAuth token
  - Verkrijgen van toegang tot fysieke ruimte met proximity card
  - Verkrijgen van toegang tot de smartphone met vingerafdrukscan

Multifactor-authenticatie

- Bij het authenticatieproces worden minimaal twee bewijsfactoren (uit verschillende categorieën) aangeboden ter verificatie van de identiteit
- Bewijsfactoren zijn traditioneel afkomstig uit volgende categorieën
  - Iets wat het subject weet (wachtwoord, pincode, antwoord op geheime vraag)
  - Iets wat het subject heeft (smartcard, token, smartphone)
  - Iets wat het subject is (irispatroon, vingerafdruk, gelaatspatroon, wijze van typen)
- Steeds vaker wordt de context als aanvullende factor bij het authenticatieproces betrokken
  - Locatie
  - Tijdstip
  - Type apparaat

Standaarden

- FIDO Alliance
- Heeft als doelstelling om wachtwoorden de wereld uit te helpen
- Geadopteerd door belangrijke marktpartijen (bijv. Google, Microsoft)
- FIDO2 is de meest recente standaard
- Twee subspecificaties
  - WebAuthn: API die multifactor-authenticatie mogelijk maakt tussen client en server
  - CTAP (Client To Authentication Protocol): API die het mogelijk maakt om externe authenticator (bijv. hardware token) met de client te verbinden
- Alle specificaties van FIDO werken op basis van digitale certificaten

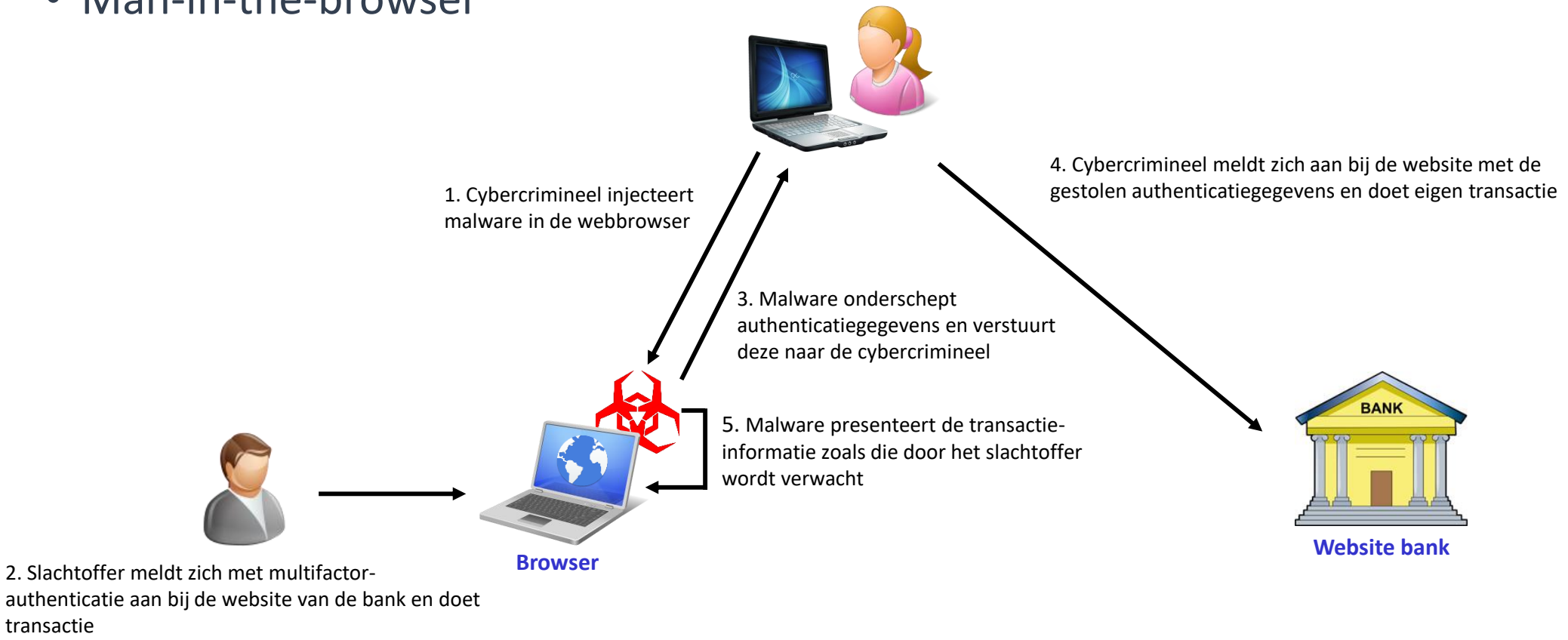
KIVI Engineering Society

Networking Academy

Stysec

Aanvallen op multifactor-authenticatie blijven mogelijk

- Man-in-the-browser



KIVI Engineering Society

Networking Academy

Stysec

Risicogebaseerde authenticatie

- Dynamisch evalueren van risico's tijdens de sessie, op basis van
  - Gevoeligheid van de informatie
  - Locatie waarvandaan informatie wordt benaderd
  - Type gebruiker dat de informatie wil benaderen
- Bij een laag risiconiveau is enkelvoudige authenticatie voldoende
- Bij een hoog risiconiveau wordt opgeschaald naar multifactor-authenticatie
- Opschalen is tijdens dezelfde sessie mogelijk (step-up)

KIVI Engineering Society

Networking Academy

Stysec

Continue authenticatie

- Authenticatie vindt gewoonlijk alleen plaats aan het begin van de sessie
- Continue authenticatie voorziet in het doorlopend verifiëren van de identiteit
- Hiermee kunnen belangrijke risico's worden gemitigeerd
  - Session hijacking
  - Man-in-the-middle-aanvallen
  - Weggrissen van notebook of smartphone
- Technieken
  - Doorlopend scannen van biometrische kenmerken (bijv. gezichtsscan, wijze van typen of swipen)
  - Doorlopend controleren van de context (bijv. GPS-locatie)

KIVI Engineering Society

Networking Academy

Stysec

Wat is autorisatie?

- Toestemming, bevoegdheid of machtiging om een bepaalde handeling te mogen verrichten
- Bijvoorbeeld het bewerken van digitale informatie
  - Creëren (create)
  - Lezen (read)
  - Wijzigen (update)
  - Wissen (delete)
- Volgt altijd op authenticatie; eerst moet toegang tot het informatiesysteem zijn verkregen alvorens de handelingen kunnen worden verricht

KIVI Engineering Society

Networking Academy

Stysec

Autorisatieprincipes

- De gegevenseigenaar bepaalt wie zijn of haar gegevens mag bewerken
- Daarbij moeten altijd de volgende principes worden gehanteerd
  - Need-to-know: alleen toegang tot die informatie die nodig is om je taken te kunnen verrichten
  - Least privilege: alleen die autorisaties die nodig zijn om je taken te kunnen doen
  - Segregation (separation) of duties (SoD): riskante handelingen kunnen niet door één individu worden voltooid
- Autorisaties liggen onder het vergrootglas van de toezichthouder
- Wet- en regelgeving (bijv. AVG, BIO) vereist dat autorisaties correct zijn

KIVI Engineering Society

Networking Academy

Stysec

Enkele autorisatiemethoden

- Mandatory access control (MAC)
  - Toegang tot informatie wordt door de beheerder gecontroleerd
  - Klassieke vorm is gebaseerd op security labels
- Discretionary access control (DAC)
  - Toegang tot informatie wordt gecontroleerd door de eigenaar ervan
- Role-based access control (RBAC)
  - Toegang tot informatie is gebaseerd op rollen (bijv. arts, beheerder)
- Attribute-based access control (ABAC)
  - Toegang tot informatie is gebaseerd op attributen (bijv. leeftijd van de gebruiker)

Accountability

- Afleggen van verantwoording, in dit geval voor het verrichten van bepaalde handelingen ofwel uitoefenen van autorisaties
- Volgt op autorisatie
- Nodig om achteraf te kunnen controleren of autorisaties zijn uitgeoefend zoals die vooraf zijn bedoeld en bepaald
- Zeer belangrijk in het kader van risicomanagement en het voldoen aan wet- en regelgeving
- Logging is meest voor de hand liggende maatregel

KIVI Engineering Society

Networking Academy

Stysec

Fysieke toegangscontrole

- Controleren wie wat voor type toegang verkrijgt tot fysieke faciliteiten zoals locaties, gebouwen, ruimtes
- Ook de fysieke toegang tot informatiesystemen moet er onder worden verstaan
  - Wel of niet in staat zijn om een USB-stick in een computersysteem te stoppen
  - Wel of niet in staat zijn een computersysteem uit te schakelen
- Ten slotte fysieke toegang tot IoT-omgevingen
  - Bruggen, sluizen, gemalen
  - Smart city
  - Smart building

KIVI Engineering Society

Networking Academy

Stysec

Fysieke toegangscontrole

- Afhankelijk van het risicoprofiel van de organisatie en de situatie zijn meerdere vormen van fysieke toegangsmechanismen mogelijk
- Via IT-infrastructuur en IoT-platform
- Directe toegang tot fysieke faciliteit
  - Smartcard, proximity card, token
  - Toegangscode, biometrische scan
  - Mantrap, tourniquet


CISCO