Ethical hacking en Auditing

ISACA Round table

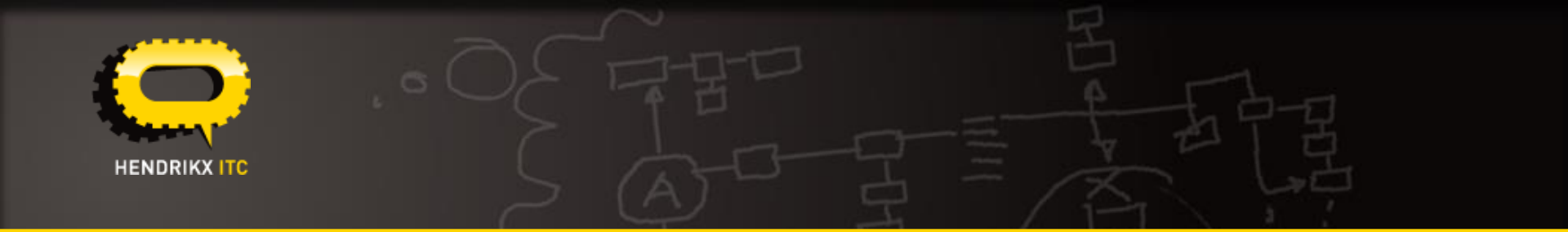
11 juni 2018

Van der Valk Hotel - Eindhoven

HENDRIKX ITC

Programma

- Even voorstellen
- Demo CloudHRM
- Een aantal begrippen
- Ethical hacking als onderdeel van een audit
- Demo beveiligingsonderzoek (optioneel)
- Vragen?



Even voorstellen

Even voorstellen

- Ing. Jan Hendrikx MSc RE CISSP CISA CISM CRISC
- Ethical hacker
- IT-auditor
- Ondersteun organisaties met NEN7510 / ISO27001 / ISAE3402 readyness
- Trainer en gastdocent

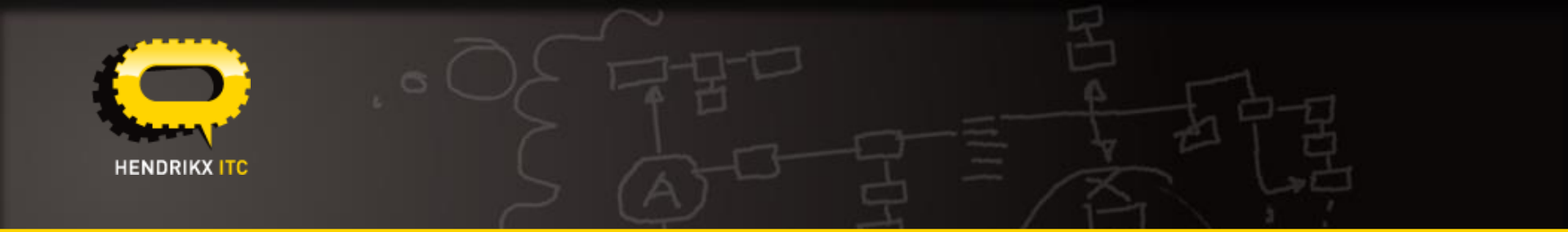
HENDRIKX ITC

Demonstratie CloudHRM

HENDRIKX ITC

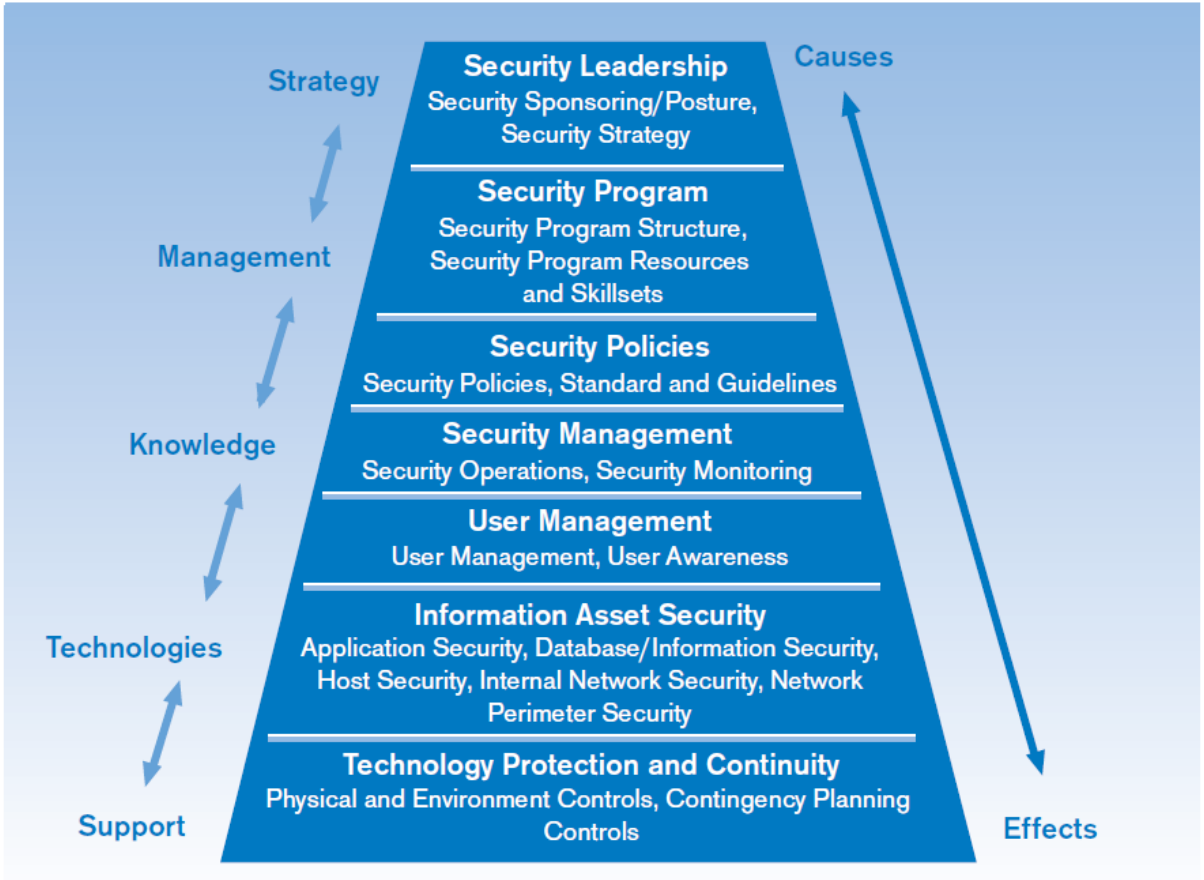
Demonstratie CloudHRM

- Fictieve SAAS-oplossing
- Bedoeld om declaraties af te handelen
- Onderliggende database bevat gegevens van verschillende organisaties
- En bevat een beveiligingslek…



Een aantal begrippen

Informatiebeveiliging



Bron: KPMG

HENDRIKX ITC

Ethical hacking

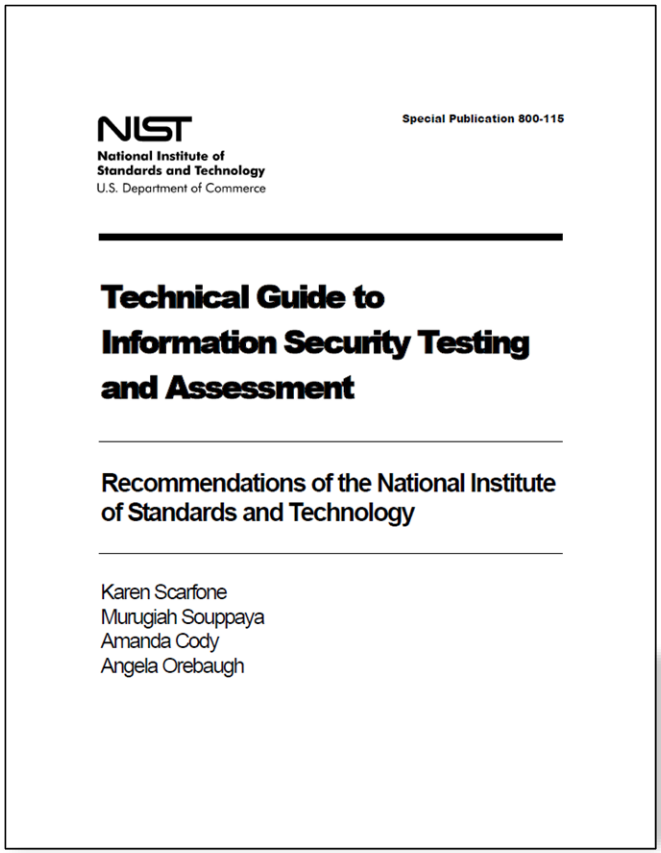
- Het proberen te doorbreken van (technische) beveiligingsmaatregelen op een gecontroleerde wijze
- Toont vaak alleen de symptomen aan van eventuele problemen
- Momentopname
- “Out of the box” / Creatief denken

HENDRIKX ITC

Soorten beveiligingsonderzoeken

- Blackbox
- Greybox
- White / Crystalbox
- Pentest
- Social engineering

Leestip – NIST 800-115



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-115

Technical Guide to Information Security Testing and Assessment

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
Murugiah Souppaya
Amanda Cody
Angela Orebaugh

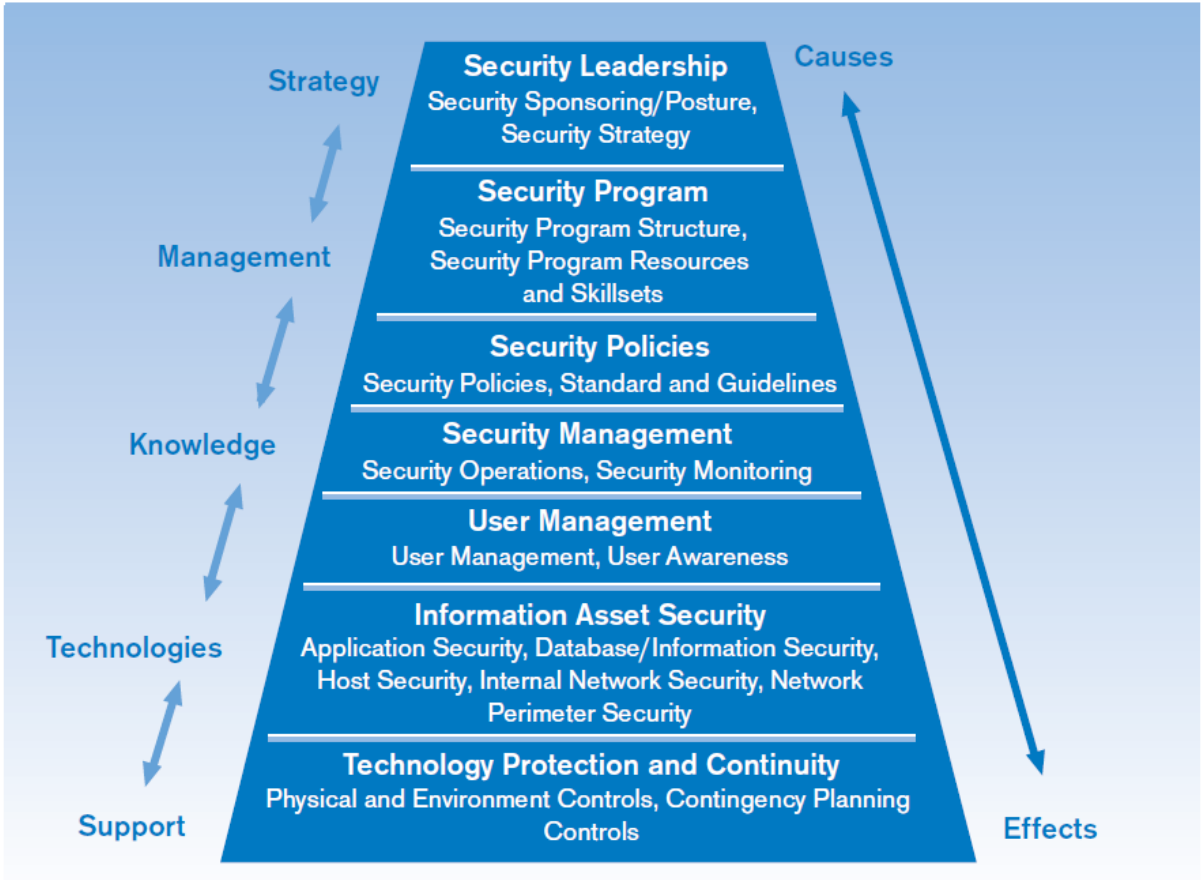
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

HENDRIKX ITC

Auditing

- Het geven van een bepaalde mate van zekerheid over het object van onderzoek
- Is breder dan alleen informatiebeveiliging
- Op basis van een afgestemd normenkader
- Probeert inzicht te verschaffen in de oorzaak van eventuele problemen
- Kijkt naar dit moment en naar het verleden
- Vaak bekeken vanuit het proces

Informatiebeveiliging

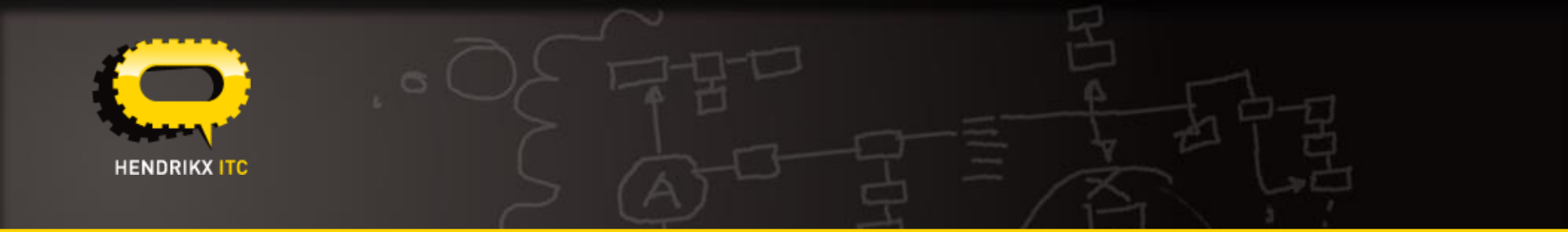


Bron: KPMG

HENDRIKX ITC

Overeenkomsten

- Vaak uitgevoerd door een onafhankelijke partij
- Kunnen zowel intern als extern zijn
- Bevindingen zijn onderbouwd met bewijs
- Vinden beiden iets van het object van onderzoek
- Zijn beiden belangrijk voor het verbeteren van de informatiebeveiliging binnen een organisatie



Ethical hacking als onderdeel van een audit

HENDRIKX ITC

Ethical hacking als onderdeel van een audit

- Wanneer er zekerheid gegeven te worden over (technische) beveiligingsmaatregelen
- Soms vanuit wet & regelgeving (DigiD-audit, ENSIA, etc.)
- Als onderdeel van de Check-fase binnen de ISO27001 / NEN7510 / BIR / BIG, etc.

Fases beveiligingsonderzoek

- Fase 1: Voorbereiding
- Fase 2: Beveiligingsonderzoek
- Fase 3: Rapportage
- Fase 4: Afronding

HENDRIKX ITC

Fase 1: Voorbereiding

- Bepaal het type onderzoek dat noodzakelijk is voor het verkrijgen van de benodigde zekerheid (pentest / security test)
- Verstrek de juiste gegevens op tijd aan de onderzoeker
- Neem een aantal onderzoeksvragen op in de opdrachtomschrijving waar tenminste op getest dient te worden
- Stem een referentiekader af waartegen getest dient te worden (optioneel)

Leestip - MG Update Zomer 2009

- https://www.secura.com/pathtoimg.php?id=376

HENDRIKX ITC

Onderzoeksvragen

At least the following threats apply to the solution and should be taken into account during the pentest:

- Ability for an unauthenticated user to read / modify financial transaction information in the system;
- Ability to create new users (with access to financial transaction information);
- Ability to obtain access to the file repository or database tables with transaction information;
- Ability to upload false transaction information through API / SFTP;
- Ability to alter system configuration;
- Ability to illegally alter roles / permissions for any webapplication user;
- Ability as a user to access financial transaction information not part of the scope of the respective webapplication user;
- Ability to alter any financial transaction information;
- Ability to alter aggregate information for other webapplication users;
- Ability to disable/remove/destroy all audit trails such as (system/application/security) logs;

HENDRIKX ITC

Leestip - Referentiekaders

- OWASP testing guide / top 10
- NCSC Richtlijnen / Whitepapers
- Certified Secure Checklists
- https://www.forumstandaardisatie.nl

HENDRIKX ITC

Fase 2: Beveiligingsonderzoek

- Laat je aan het einde van iedere dag informeren over de vorderingen
- Stuur eventueel bij op hoofd- en bijzaak
- Zorg dat je bereikbaar bent voor eventuele vragen
- Zorg voor een technisch contactpersoon om technische problemen op te kunnen vangen

Fase 3: Rapportage

- Zorg voor een managementsamenvatting met de belangrijkste bevindingen
- Zorg dat bevindingen worden voorzien van een technische onderbouwing
- Vraag bij bevindingen om een technische risico inschatting inclusief oplossingstermijn
- Zorg dat de rapportage alleen wordt verstrekt aan de juiste mensen

Voorbeeld rapportage CloudHRM

Voorbeeld beveiligingsonderzoek:
CloudHRM webapplicatie

In opdracht van: Cloudservices B.V.

Door: ing. J.H.J. Hendrikx MSc RE CISSP CISA CISM

Datum: 16 januari 2018

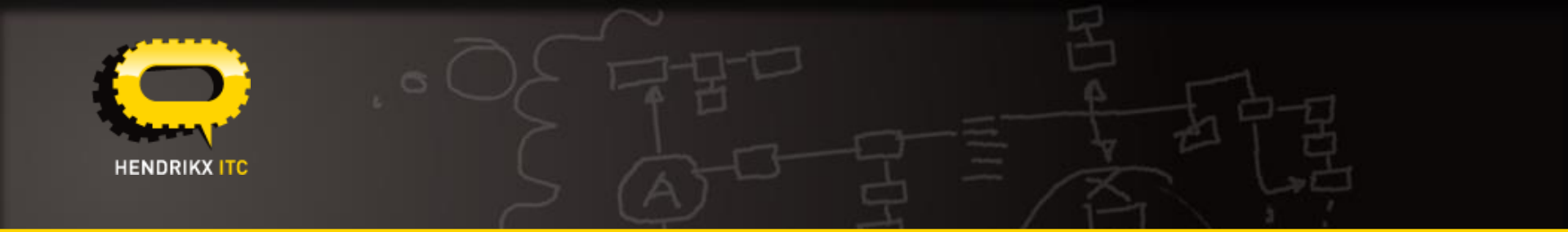
HENDRIKX ITC

Fase 4: Afronding

- Bespreek de rapportage met de onderzoeker
- Vraag ook naar eventuele andere opvallende zaken
- Vertaal de technische risico's naar risico's voor de organisatie
- Neem het rapport op in het auditdossier
- Overweeg een hertest / audit

Red teaming

- Gedacht vanuit de aanvaller
- Geen vast testplan of vaste scope
- Maakt gebruik van verschillende aanvalsscenario's over een langere periode
- Maakt de weerbaarheid / veerkracht (cyber resilience) van de organisatie inzichtelijk

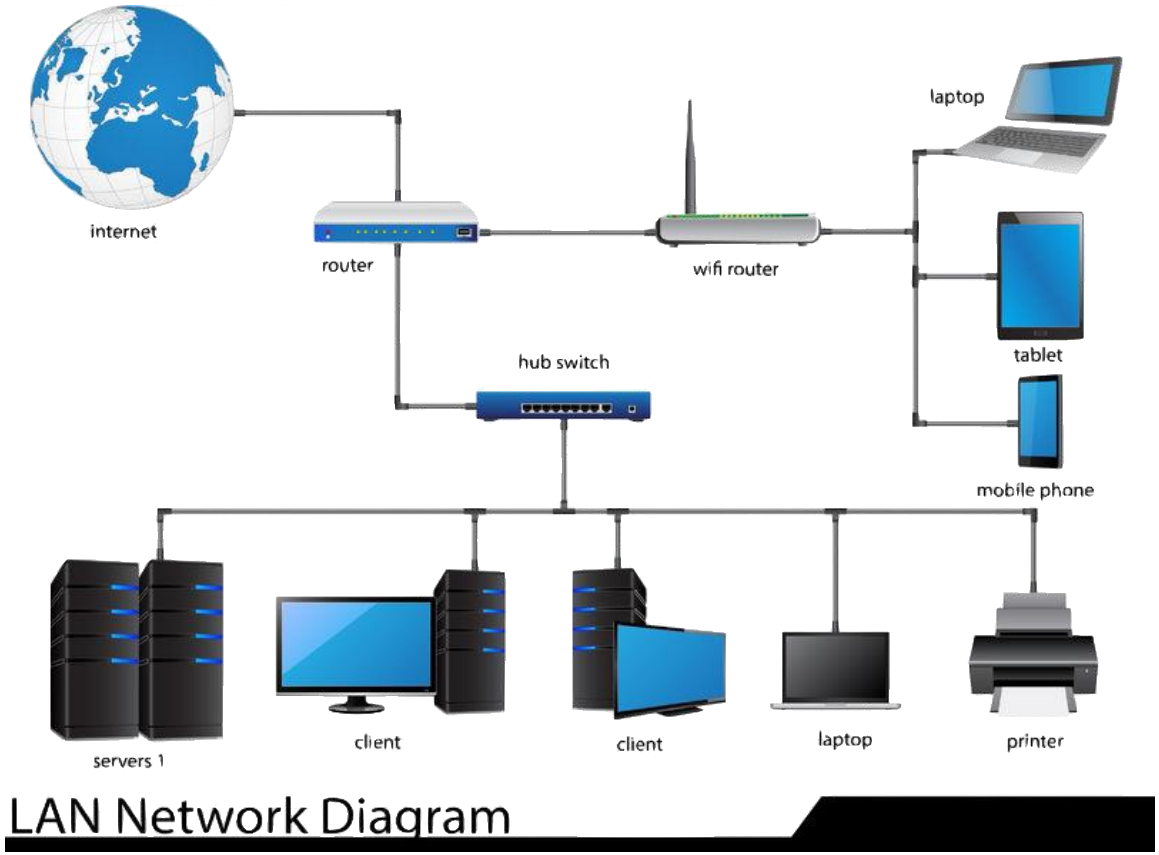


Demo beveiligingsonderzoek

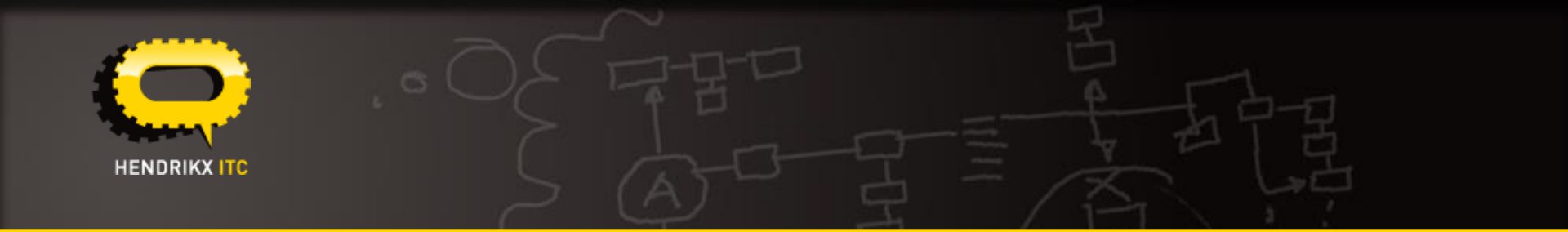
HENDRIKX ITC

Demonstratie beveiligingsonderzoek

DEMO



Bron: RF123.com



Zijn er nog vragen?

Spoorlaan 346
5038 CC Tilburg
The Netherlands
T +31 (0)6 23010199
E info@hendrikx-itc.nl
W www.hendrikx-itc.nl