Inhoud

Practica

Voorwoord

Welkom bij de uitgave *ICT Security*. Soms kunnen dingen raar lopen. Bij toeval kwam ik in contact met Brinkman Uitgeverij. Vrijwel onmiddellijk hebben wij besloten dat er een boek moest komen over ICT Security. Vanaf het eerste gesprek tot het schrijven van de laatste bladzijde is er altijd een duidelijke focus geweest: wij hebben niet alleen een goed lesboek willen maken, maar vinden ook dat het onderwerp een integraal onderdeel moet uit gaan maken van de bagage van elke ICT professional. Dit boek biedt dan ook elke ICT professional, beginnend of doorgewinterd, een uitgebreide ondergrond om zijn of haar kennis verder uit te breiden op het gebied van veiligheid. Het boek is zodanig opgebouwd dat je stap voor stap het security gebied gaat verkennen. Aan het einde van het boek zal je een groot aantal beveiligingsprincipes kennen en weten hoe je deze toe moet passen. Je zult zelfs in staat zijn om een Intrusion Detection System te installeren en configureren. Ik ben ervan overtuigd dat wij onze visie vast hebben kunnen houden en hoop dat jullie dat ook zo ervaren.

Een boek komt nooit tot stand zonder hulp van enkele bijzondere mensen. In mijn geval gaat mijn dank vooral uit naar mijn vrouw Liane en onze prachtige kinderen: Finn, Tara en Odin. Zij hebben mij avond op avond, dag na dag, maandenlang, volledig gesteund.

Uiteraard ben ik erg benieuwd naar ieders ervaringen en nodig elke lezer dan ook van harte uit om te reageren via de website www.ict-security-boek.nl.
Tot slot wens ik iedereen een leerzame ervaring toe en heel veel plezier.

Boris Sondagh
juli 2008

Voorwoord bij de vierde, herziene druk

De derde druk is tussentijds, via de website www.ict-security-boek.nl, geactualiseerd. Deze aanpassingen zijn inmiddels zo omvangrijk dat een nieuwe druk niet alleen gerechtvaardigd is, maar voor het overzicht ook noodzakelijk. In deze nieuwe druk zijn versie Windows 8.1 en Windows Server 2012 R2 het uitgangspunt.

Ook van de meeste tools zijn er inmiddels actuelere versies dan die uit de derde druk. In sommige situaties moest zelfs een nieuwe tool worden gekozen. Op de website staat een overzicht van de gebruikte versies van deze tools. De aanpak om, aansluitend op de nieuwe druk, de actualiseringen op de website te publiceren zullen we dan ook in de toekomst hanteren.

We hopen met deze nieuwe druk en de voortdurende aanpassingen dat de bijzonder positieve ontvangst van deze uitgave ook voor de komende tijd bij nieuwe studenten is gewaarborgd.

Boris Sondagh
juli 2015

Voorwoord bij de vijfde druk

In de vijfde druk is een nieuw hoofdstuk (hoofdstuk 13) over het beveiligen van mobiele devices toegevoegd.

Boris Sondagh
augustus 2018

Hoofdstuk 1

Inleiding

1.1
Welkom

Welkom bij het (doe)boek *ICT Security — praktische beveiliging van computersystemen, digitale media en netwerkverbindingen*. Door dit boek te lezen, en vooral door veel te doen, zul je aan het einde van dit boek in staat zijn om:

- ▷ verschillende beveiligingsprincipes uit te leggen,
- ▷ beveiligingsoplossingen te installeren en configureren,
- ▷ ICT-beveiligingen te herkennen en onderscheiden.

Dit boek kun je op verschillende manieren lezen, je kunt bijvoorbeeld bij bladzijde 1 beginnen en zo één voor één alle bladzijden doorlezen en doorwerken tot de laatste bladzijde. Door de opzet van dit boek is het ook mogelijk om te beginnen bij een hoofdstuk dat je op dat moment nodig hebt of interessant vindt. Wanneer je bijvoorbeeld je harde schijf wilt versleutelen dan kun je direct beginnen bij hoofdstuk 12 — Beveiligen van datadragers. Op welke manier je het boek ook leest, één ding is zeker: wanneer je het uit hebt zul je een heel eind op weg zijn naar een volwaardige ICT Security professional.

1.2
Wat is ICT Security?

Om de vraag te beantwoorden wat er bedoeld wordt met ICT Security, moeten we eerst de begrippen ICT en Security duidelijk krijgen.

Bij ICT, voluit informatie- en communicatietechnologie, denken de meeste mensen vaak aan 'iets met computers'. Als we dit proberen wat duidelijker te omschrijven kunnen we volgens de vrije encyclopedie, Wikipedia[1], de volgende definitie hanteren: *'Informatie- en Communicatietechnologie (ICT) is een vakgebied dat zich met informatiesystemen, telecommunicatie en computers bezighoudt.'*

Wanneer we praten over Security, of beveiliging, dan hebben we het over 'dingen veilig houden'. Of nog iets specifieker: *'dingen waar we waarde aan toekennen met bepaalde middelen preventief veilig houden'*. Als we bepaalde dingen waardevol vinden en we denken dat die op dat moment niet veilig zijn, gaan we deze dingen beveiligen.

1 'Informatie- en Communicatietechnologie.' Wikipedia, de vrije encyclopedie, jan. 2008.

Twee voorbeelden:
Wanneer we onze auto waardevol vinden en we laten deze elke nacht gewoon op straat staan, dan is het handig om deze te beveiligen. Dit doen we door middel van een slot op de deur, een slot om de auto te starten en soms ook met een alarm. Security gaat dus ook over middelen zoals sloten en alarmsystemen.
Wanneer een heel waardevol schilderij is gestolen dan is het niet mogelijk om dit achteraf te beveiligen. We zullen dus nog vóórdat we het schilderij ophangen na moeten denken over de beveiliging ervan. Security is dus een preventief begrip.

Wanneer we de twee termen samenvoegen krijgen we iets als 'computers veilig houden' of specifiek 'informatiesystemen, telecommunicatie en computers met bepaalde middelen (tools) preventief veilig houden'.

Omdat de meeste informatiesystemen, telecommunicatie en computers niet preventief beveiligd zijn, of maar een klein beetje, zul je bij het beveiligen vooral gebruik moeten maken van de juiste middelen (tools).

1.3 Voor wie is dit boek?

Dit boek is geschreven voor iedereen die wil leren hoe ICT Security werkt en hoe je dit moet toepassen. Het boek sluit aan op de basis ICT-kennis zoals deze op de verschillende mbo ICT-opleidingen wordt gegeven.

Heel specifiek zijn de opdrachten en kennis geschikt om te gebruiken tijdens of na de volgende mbo-opleidingen:
- Medewerker ICT,
- Medewerker beheer ICT,
- ICT-beheerder,
- Netwerk- en mediabeheerder.

Bovenstaande opleidingen zijn geen vereiste om dit boek te kunnen gebruiken. Je hebt wel ICT-basiskennis nodig om de opdrachten in dit boek te kunnen uitvoeren. Zo moet je de volgende begrippen in ieder geval kunnen omschrijven, toelichten en enkele voorbeelden kunnen geven:
- besturingssysteem,
- bestandssysteem,
- netwerk,

- protocol,
- informatiesysteem,
- datadrager.

Een gezonde hoeveelheid ICT-kennis is erg handig bij het doorwerken van dit boek. Maar er is één ding dat nog handiger is dan ICT-kennis: dat je ICT Security leuk vindt!

1.4 Hoe is het boek opgebouwd?

Na de eerste twee hoofdstukken beginnen we met het echte werk. Vanaf hoofdstuk 3 is elk hoofdstuk als volgt opgebouwd:

1. Inleiding — een korte toelichting van het onderwerp van het hoofdstuk.
2. Leerdoelen — wat je zou moeten kunnen en weten na het doorwerken van dit hoofdstuk.
3. Vereiste voorkennis — welke kennis je zou moeten hebben om dit hoofdstuk goed te kunnen begrijpen.
4. De bedreiging — welke bedreiging er bestaat met betrekking tot het onderwerp, de reden waarom we gaan beveiligen.
5. De oplossing — welke methodes en tools er bestaan om de bedreiging te minimaliseren of zelfs op te heffen.
6. Het practicum — het uitvoeren van de oplossing. Er zijn soms meerdere practica bij een oplossing.
7. Samenvatting — het hele hoofdstuk nog even op een rijtje.

De punten 4, 5 en 6 staan er meestal een aantal keer in, aangezien er vaak meerdere bedreigingen en oplossingen zijn bij één onderwerp.

1.5 Benodigdheden

Er zijn nogal wat zaken die je nodig hebt om de opdrachten in dit boek uit te kunnen voeren:

- een pc met de volgende minimale hardware-eisen:
  - processor van 1 Ghz,

  - geheugen 1 GB (32-bit) of 2 GB (64-bit),
  - 16 GB (32-bit) of 20 GB (64-bit) schijfruimte,
  - Grafisch DirectX 9-apparaat met stuurprogramma WDDM 1.0 of hoger
- eventueel een virtualisatieproduct (bijvoorbeeld Microsoft Virtual PC, VMware Workstation of VirtualBox, zie ook 1.7),
- een Office pakket,
- een internetverbinding,
- een ondersteunende website: www.ict-security-boek.nl. Deze bevat onder andere:
  - de werkbladen,
  - bestanden die nodig zijn voor de practica,
  - tools (vaak zijn de tools op het internet wel nieuwer),
  - instructievideo's,
  - vingerafdrukken/hashwaarden van de bestanden.

1.6 Toolselectie

Voor de verschillende oplossingen die in dit boek worden genoemd zijn vaak meerdere tools beschikbaar. Er is daar waar mogelijk gekozen voor de tool welke als marktleider beschouwd wordt. Er zijn twee uitzonderingen: wanneer de standaardtool significant minder effectief is dan een andere tool en wanneer de standaardtool niet als gratis of testversie beschikbaar is.

Wanneer we met security te maken krijgen, komt al snel de discussie van Open Source tegenover Closed Source ter sprake. Vaak is er ook sprake van een discussie over Microsoft tegen Linux. In de securitywereld wordt bij menige oplossing gekozen voor een Open Source oplossing, dan wel een Linux oplossing. Op de vraag wat het beste platform is kan geen eenduidig antwoord gegeven worden. Over dit onderwerp op zich kan een boek worden geschreven. In dít boek is er geen voorkeur voor een bepaald platform. Er is steeds uitgegaan van de marktleider. Als er goede alternatieven zijn voor de gebruikte tools in dit boek, dan worden deze benoemd.

1.7
Werken met Virtualbox

Zoals aangegeven bij de benodigdheden kunnen we gebruikmaken van een virtualisatieproduct. Je kunt zelf kiezen om op een echt besturingssysteem te werken of in een gevirtualiseerde omgeving. Het voordeel van een gevirtualiseerde omgeving is dat we fouten kunnen maken zonder dat we data kwijtraken. Ook kunnen we sneller opnieuw beginnen als we iets verkeerd hebben gedaan. Het nadeel is dat er behoorlijk wat werkgeheugen nodig is om redelijk snel te kunnen werken. Virtual PC heeft geen USB-support (in tegenstelling tot de meeste overige virtualisatieproducten) en draadloze netwerkkaarten worden gezien als fysieke netwerkkaarten (ze zijn onhandig bij de security-analyse van draadloze netwerken).

In dit boek kan gebruik worden gemaakt van Virtualbox, maar andere virtualisatieproducten kunnen net zo goed gebruikt worden.

Virtualbox-installatie
Tijdsduur: ± 5 minuten.

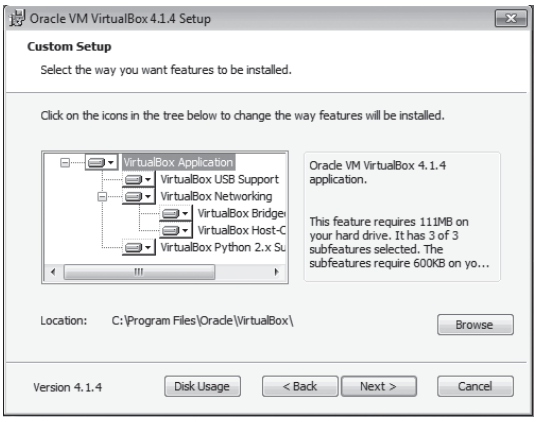
1. Open je favoriete internetbrowser en ga naar: http://www.ict-security-boek.nl/tools, download VirtualBox via de link naar de site www.VirtualBox.org.

2. Voer de gedownloade setup uit (bij publicatie boek is dit VirtualBox-4.1.4-74291-win.exe).

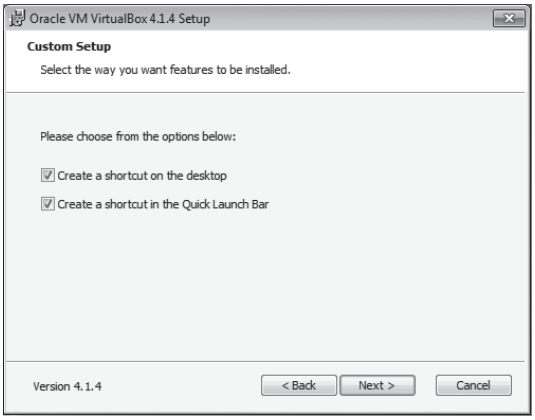
3. Het Wizardscherm Welcome to Oracle VM VirtualBox verschijnt. Klik *Next >*.

4. Het wizardscherm *Custom Setup* verschijnt (figuur 1-1). Standaard zijn alle benodigde onderdelen geselecteerd. Klik op *Next >* om de installatie te vervolgen.
   In dit boek zul je veel gaan werken met VirtualBox. Geef daarom de setup de opdracht om een snelkoppeling op het bureaublad en in de Snelstart balk aan te maken (figuur 1-2).

5. Om het mogelijk te maken dat de Virtuele machines met het internet kunnen communiceren dienen de VirtualBox Network Interfaces geïnstalleerd te worden (figuur 1-3). Klik daarom *Yes* in het venster *Warning: Network Interfaces*.



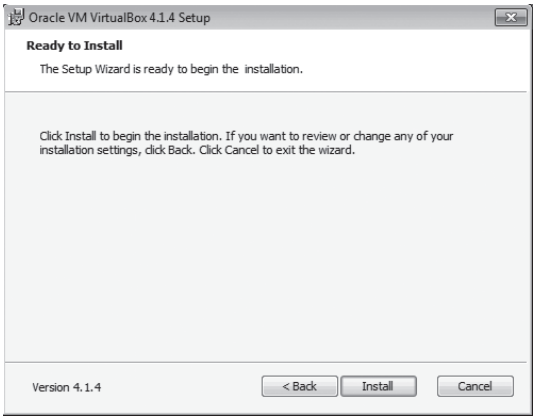
FIGUUR 1-1 *Custom Setup*



FIGUUR 1-2 *Aanmaken Snelkoppelingen*

FIGUUR 1-3 *Installatie Netwerkkoppeling*

6. Klik Install in het scherm Ready to install (figuur 1-4). VirtualBox wordt nu op de PC geïnstalleerd. Het kan zijn dat tijdens de installatie het beeld even knippert en de netwerkverbindingen voor korte tijd wegvallen. Dit komt door de installatie van de virtualisatiecomponenten. Dit kan geen kwaad. Na de installatie van VirtualBox zal de PC werken als voorheen.



FIGUUR 1-4 *Installatie Starten*

7. Na afronding van de installatie kan indien gewenst VirtualBox gestart worden (figuur 1-5).

FIGUUR 1-5 *Installatie voltooid*