



TECHNISCHE CYBER SECURITY

Boom beroepsonderwijs
info@boomberoepsonderwijs.nl
www.boomberoepsonderwijs.nl

Auteur: Jan Dolphijn

Eindredactie: Jan Hoeve

Titel: Technische cyber security

ISBN: 978 90 372 6257 5, maakt deel uit van pakket 978 90 372 6256 8

Bronvermelding: ViaDennis International BV, FBI, Shutterstock.com: PhatTai;
JHVEPhoto; Jan van der Wolf; PitPictures.

Eerste druk/tweede oplage
© Boom beroepsonderwijs 2022

Behoudens de in of krachtens de Auteurswet gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever.

Voor zover het maken van reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (www.reprorecht.nl). Voor het overnemen van (een) gedeelte(n) uit deze uitgave in bijvoorbeeld een (digitale) leeromgeving of een reader in het onderwijs (op grond van artikel 16, Auteurswet 1912) kan men zich wenden tot Stichting Uitgeversorganisatie voor Onderwijslicenties (Postbus 3060, 2130 KB Hoofddorp, www.stichting-uvo.nl).

De uitgever heeft ernaar gestreefd de auteursrechten te regelen volgens de wettelijke bepalingen. Degenen die desondanks menen zekere rechten te kunnen doen gelden, kunnen zich alsnog tot de uitgever wenden.

Door het gebruik van deze uitgave verklaart u kennis te hebben genomen van en akkoord te gaan met de specifieke productvoorwaarden en algemene voorwaarden van Boom beroepsonderwijs, te vinden op www.boomberoepsonderwijs.nl

INHOUD

	Inleiding	5
Hoofdstuk 1	Dreiging en risicoanalyse	9
	Dreigingsactoren	11
	Dreiging	19
	Ransomware	24
	Webapplicaties en -services	24
	Phishing en spam	26
	DDoS-aanvallen	31
	Identiteitsdiefstal	36
	Data breaches en botnets en de insider threat	38
	Security-incidenten	41
	Risicoanalyse	43
	Kwantitatieve risicoanalyse: de ALE	53
	Kwalitatieve risicoanalyse	55
	Samenvatting	62
	Begrippen	63
Hoofdstuk 2	Privacy en recht	65
	Privacy	68
	Recht en privacy	70
	Rechten van betrokkenen	76
	Recht en wetten	78
	Wetsartikel 161sexies Computervredebreuk	81
	Wetsartikel 350ab De SQL-injectie	83
	Wetsartikel 139cd Sniffen, aftappen	85
	Samenvatting	86
	Begrippen	87
Hoofdstuk 3	Frameworks en standaardisatie	89
	Frameworks en standaardisatie	90
	Toepassing BIO	91
	Securitystandaards	93
	Frameworks: Cyber Security Framework NIST	98
	Framework profiles	108
	De ISO-standaardisatie serie 27001 en 27002	117
	Samenvatting	121
	Begrippen	122

Hoofdstuk 4	Pentesten en social engineering	123
	Pentesten en social engineering	125
	Waarom pentesten?	129
	Vorbereiding op de test	132
	Social engineering	144
	Social Engineering Attack Cycle	145
	Social Engineering Attack Framework	146
	Overtuigen van het doelwit	150
	Social engineering-aanval opzetten	153
	Samenvatting	157
	Begrippen	158
 Hoofdstuk 5	 Controls	 161
	Securitymaatregelen	163
	Fysieke maatregelen	167
	Barrières	168
	Biometrie	170
	Detectieve fysieke maatregelen	173
	Afsluiting detectieve fysieke maatregelen	175
	Certificaten	180
	SSL-certificaat	181
	Correctieve technische maatregelen	185
	Organisatorische maatregelen	186
	Samenvatting	192
	Begrippen	193
	 Index	 195

INLEIDING



Digitale leeromgeving

In de kantlijn staat in deze uitgave regelmatig een icoontje in de vorm van een wereldbol. Dat verwijst naar extra informatie op Boom Digitaal. De informatie kan een video, een internetverwijzing, een tekstbron, een audiobron of andersoortige digitale informatie zijn. Om hier te komen ga je naar digitaal.boomonderwijs.nl/beroepsonderwijs.

Eerste keer inloggen in de digitale omgeving

Voordat je de digitale leeromgeving kunt gebruiken, moet je je licentie activeren.

- Overleg met je docent welk type account je gebruikt.
- Ga naar www.boomberoepsonderwijs.nl/licentie.
- Bekijk de instructiefilm of lees het stappenplan.
- Volg de stappen.

Daarna kun je aan de slag!

Introductie

Deze uitgave is geschreven voor iedereen die zich wil bekwamen om binnen een organisatie de digitale beveiliging vorm te geven. Alle organisaties, commercieel en niet commercieel maken gebruik van digitale middelen om informatie te verwerken. Het beveiligen van de bedrijfsinformatie heeft in vrijwel alle bedrijven een hoge prioriteit. In dit boek leer je op een praktische manier hoe je digitale beveiliging toepast door middel van beveiligingsmaatregelen. In het eerste hoofdstuk leer je dreiging en kwetsbaarheden kennen en het mogelijke risico te analyseren. Hoofdstuk twee gaat in op de wetgeving op het gebied van cybercriminaliteit en privacy aan de hand van een aantal casussen. Hoofdstuk drie beschrijft de organisatie van cybersecurity door de belangrijkste frameworks te beschrijven. In hoofdstuk vier leer je een penetratie test voor te bereiden en uit te voeren, in hoofdstuk 5 tenslotte pas je beveiligingsmaatregelen toe om bedrijf kritische informatie te beschermen.

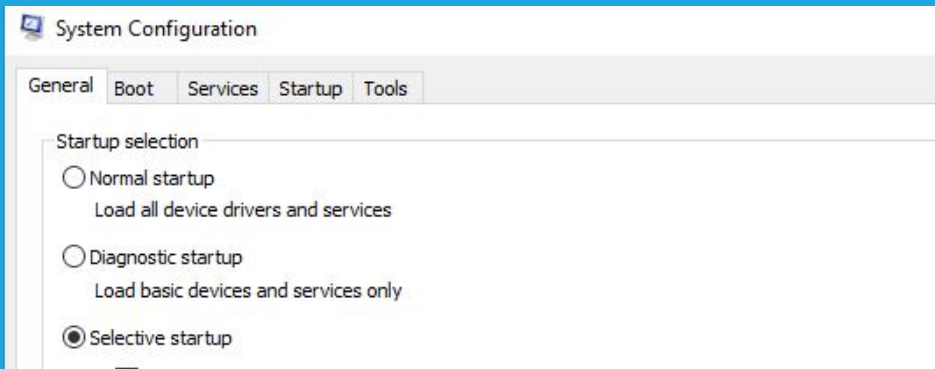
Alle hoofdstukken combineren theorie met praktische opdrachten die inzicht geven in de manier waarop cybersecurity wordt toegepast anno 2022.



Deze 'gevaren' staan in de wereld van de **cyber security** bekend als **dreigingen**. In dit gedeelte leer je de meest voorkomende dreigingen herkennen en maatregelen treffen om de negatieve gevolgen van een dreiging te voorkomen. In het tweede gedeelte van dit hoofdstuk leer je een inschatting maken van welke dreigingen het meest urgent zijn en waar je de bedrijfsmiddelen tegen dient te beschermen. Vaststellen welke middelen je tegen welke dreiging beschermen doe je door middel van een **risicoanalyse**.

Ken jij je systeem? Als je een Windows-systeem hebt, doe je het volgende:

Klik op zoek, typ **msconfig** in en klik dan op enter.



Msconfig op een Windows 10-systeem.

Kijk op het tabblad waar startup staat. Hier staan alle programma's die op jouw computer automatisch worden gestart als je Windows opstart. Ken je ze allemaal? Weet je zeker dat niet elke keer als je je computer aanzet een programma draait waarvan jij geen weet hebt? Tenslotte is elk gestart programma een mogelijke kwetsbaarheid. Is de lijst leeg? Heel goed. Al haal je al deze programma's weg, je ziet rechtsonder in je scherm allerlei programma's die gestart zijn (bij de datum- en tijdaanduiding). Blijkbaar is het niet zo simpel. Welkom in de wereld van dreiging en risico.

Leerdoelen

1. Je ontwikkelt kennis van de belangrijkste bedreigingen van netwerken, systemen, gebruikers, software en/of devices.
2. Je kent de belangrijkste dreigingsactoren.
3. Je kent de belangrijkste dreigingen.
4. Je kent de belangrijkste aanvalsvectoren.
5. Je kunt een kwantitatieve risicoanalyse uitvoeren.
6. Je kunt een kwalitatieve risicoanalyse uitvoeren.
7. Je ontwikkelt kennis van wetgeving op het gebied van privacy en cybercriminaliteit.
8. Je ontwikkelt globale kennis van de AVG.
9. Je krijgt globale kennis van cyber gerelateerde wetsartikelen.
10. Je leert wat het belang is van BIO.
11. Je leert kennis over de securitystandaards.
12. Je leert wat het belang is van Framework profiles.
13. Je leert wat het belang is van ISO-standaardisatie 27001 en 27002.
14. Je kunt technieken toepassen voor het opsporen en evalueren van beperkingen en kwetsbaarheden in netwerken, systemen, gebruikers, software en/of devices.
15. Je kent de opbouw van een social engineering-aanval.
16. Je kent de technieken, tactieken en motivatie van een social engineering-aanvaller.
17. Je kent de opbouw van een penetratietest.
18. Je kunt een penetratietest uitvoeren met de juiste tooling.
19. Je leert specialistische kennis van de belangrijkste preventieve en repressieve maatregelen voor de beveiliging van netwerken, systemen, gebruikers, software en/of devices.
20. Je kunt technieken toepassen voor het opsporen en evalueren van beperkingen en kwetsbaarheden in netwerken, systemen, gebruikers, software en/of devices.
21. Je kent de belangrijkste fysieke, technische en organisatorische controls.
22. Je kunt incidenten opsporen en de belangrijkste processen monitoren.

Elk hoofdstuk bestaat uit:

- *Theorie, begrippen en opdrachten*

Hierbij leer je over en oefen je met de praktijk.



HOOFDSTUK 1

DREIGING EN RISICOANALYSE

Het ligt voor de hand dat een dreiging schade kan aanrichten aan de digitale systemen van een bedrijf. Onverlaten kunnen het bedrijfsnetwerk ontoegankelijk maken, geheimen stelen, computers besmetten met malware of valse informatie rondsturen. Dreigingen komen in vele vormen. Evenals de onverlaten die je systemen aanvallen. Toch vormt een dreiging op zich nog geen risico. Als een nieuwe vorm van ransomware zich richt op Windows Servers en tracht daar schade aan te richten, is sprake van een dreiging. Als een bedrijf echter alleen Linux-servers heeft of alleen uit macOS (Apple)-computers bestaat, heeft deze dreiging geen effect bij dat bedrijf.

Als er een dreiging is waar een systeem of netwerk wél gevoelig voor is, wordt dit een **kwetsbaarheid** genoemd. Pas als er een reële dreiging is én een systeem wat kwetsbaar is voor die dreiging, is sprake van **risico**. Een bedrijf neemt maatregelen om de bedrijfsmiddelen te beschermen door risico te verminderen. Een securityprofessional weet hoe kwetsbare systemen te beschermen zijn tegen aanvallen. De professional herkent risicofactoren (waar dreiging en kwetsbaarheid elkaar raken) en past de juiste maatregelen toe om risico te verminderen.

Leerdoelen

1. Je leert specialistische kennis van de belangrijkste bedreigingen van netwerken, systemen, gebruikers, software en/of devices.
2. Je kent de belangrijkste dreigingsactoren.
3. Je kent de belangrijkste dreigingen.
4. Je kent de belangrijkste aanvalsvectoren.
5. Je kunt een kwantitatieve risicoanalyse uitvoeren.
6. Je kunt een kwalitatieve risicoanalyse uitvoeren.

Dreigingsactoren

Personen die een dreiging vormen voor de juiste werking van een digitaal systeem of een geautomatiseerd proces, worden **dreigingsactoren** genoemd. De Nederlandse overheid heeft een organisatie opgericht, het **Nationaal Cyber Security Centrum (NCSC)**, die onderzoek doet naar mogelijke dreigingen voor diensten van de overheid. In Nederland is volgens het NCSC sprake van een permanente dreiging. Dit betekent continue aandacht voor de digitale weerbaarheid in ons land. Voor bedrijven geldt dit natuurlijk ook. Permanente digitale waakzaamheid is een vanzelfsprekendheid geworden.

Het Nationaal Cyber Security Centrum (NCSC) verdeelt de actoren op drie manieren. Ten eerste de intentie van de actor: waarom doen de actoren wat zij doen? Daarnaast worden de actoren ingedeeld op basis van capaciteit; de mate van deskundigheid waarmee aanvallen worden uitgevoerd. Ten derde de activiteit van de actor: hoe vaak en op welke schaal is de actor actief?

Bij **intentie** gaat het om de vraag of een actor wordt gemotiveerd door bijvoorbeeld een financieel, politiek of idealistisch doel om informatiesystemen aan te vallen.

Capaciteit bestaat uit de middelen die een actor ter beschikking heeft om een aanval uit te voeren. Middelen bestaan uit de hoeveelheid financiering, de gespecialiseerde mankracht en de moderniteit van de technologie.

De **activiteit** van een actor wordt bepaald door de mate waarin concrete digitale aanvallen zijn waargenomen en uitgevoerd door die actor in het verleden of door wat de actor in het heden uitvoert.

Tussen de verschillende groepen zijn grote verschillen in capaciteit: de mate van organisatie (werkomstandigheden en financiën), technologie (beschikbaarheid van middelen) en specialisme (professionele mankracht). Ten slotte is een actor wel of niet actief in het uitvoeren van aanvallen.

Een combinatie van de mate van intentie, capaciteit en activiteit bepaalt de dreiging van een actor richting (informatie)systemen. De actoren worden onderverdeeld in zes groepen, die hierna kort beschreven worden. Voor een securityspecialist is het noodzakelijk te weten wie een aanval uitvoert. Dit geeft een beter idee van hoe de aanval verloopt en hoe de mate van dreiging moet worden ingeschat.

De volgende groepen worden toegelicht:

- staatondersteunde groepen
- cybercriminelen
- hacktivists
- terroristen
- script-kiddies
- insiders.