Inhoud

Voorwoord

De afgelopen jaren heb ik mij, als docent ICT, gespecialiseerd in digitale beveiliging. De reden was mijn eerdere betrokkenheid bij de opleiding forensische ICT en pure persoonlijke belangstelling voor het onderwerp. De gedachte om een specialisme voor het MBO te ontwikkelen vloeit voort uit de enorme belangstelling voor dit onderwerp. Zowel vanuit de beroepsgroep als collega's en vooral ook de studenten blijkt er behoefte te zijn aan deze kennis. Het boek *Security in systemen en netwerken* is direct gerelateerd aan de opleidingen ICT en Netwerkbeheer. Toch zal blijken dat de securityspecialist met een andere, soms zelfs volledig afwijkende, zienswijze naar dezelfde digitale infrastructuur kijkt. Ik werk vrijwel wekelijks samen met security-experts uit het bedrijfsleven, wat ertoe geleid heeft dat het voorliggende boek een brede basis biedt op het gebied van security.

Deze eerste druk is tot stand gekomen in nauwe samenwerking met Henk Pel en de niet aflatende steun van mijn vrouw. Gezien de voortsnellende ontwikkelingen op het securitygebied ligt een vervolg voor de hand.

Mijn dank gaat uit naar de experts Michael Tong Sang, Alain Rees en Erik van Veen, die met hun scherpe blik en professionalisme mijn visie op security hebben verdiept en aangescherpt. Ook wil ik met name Peter Rong, Ben Visscher en Jacco van de Ven bedanken die binnen onze organisatie mij, vanuit hun functie en enthousiasme, zeer hebben gesteund.

Hoofdstuk 1
De principes van digitale beveiliging

Inleiding

In dit hoofdstuk leer je wat de basisprincipes van digitale beveiliging zijn. Je maakt kennis met de wijze waarop informatie geheim wordt gehouden (vertrouwelijkheid, paragraaf 1.1). Daarnaast leer je hoe fouten tijdens invoer, opslag en versturen van data voorkomen kunnen worden (integriteit, paragraaf 1.2). Tenslotte krijg je inzicht in de wijze waarop netwerkgebruikers op het juiste moment en op de juiste wijze bij hun data kunnen (beschikbaarheid, paragraaf 1.3). Je krijgt in paragraaf 1.4 een overzicht van de functies die binnen een bedrijf of organisatie een rol spelen bij de toepassing en uitvoering van security-maatregelen.

Leerdoelen

- Je maakt kennis met de CIA Triad, in het Nederlands de BIV genaamd.
- Je maakt kennis met de functies die in de security-wereld veelvuldig voorkomen.

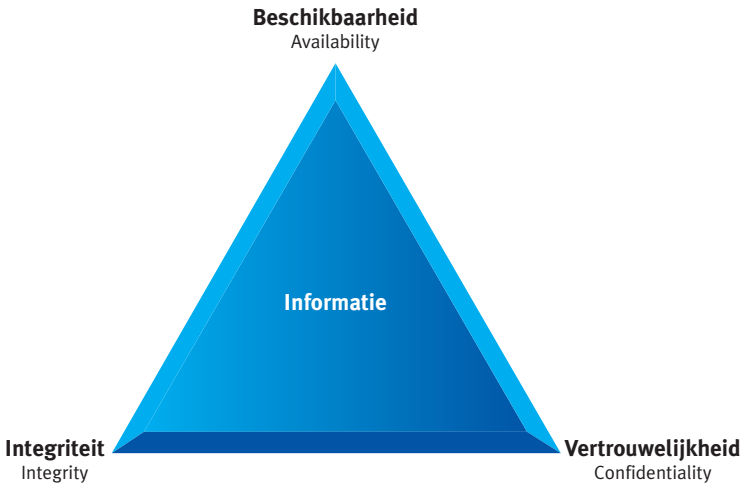
Termen

Beschikbaarheid	Het tijdig en continu beschikbaar zijn van data.
Beschikbaarheidsketen	Een reeks geschakelde apparaten die elkaar versterken of verzwakken in termen van beschikbaarheid.
Classificatie	Een indeling van informatie op basis van vertrouwelijkheid.
Cryptografie	Methode om informatie dusdanig te versleutelen dat alleen degene met de sleutel de informatie kan lezen.
Digitale handtekening	Een waarde die absoluut uniek is voor een bepaald stuk informatie, hiermee wordt de integriteit van informatie gegarandeerd.
Ethiek	Ethiek is nadenken over hoe je goed en fout kunt handelen in concrete situaties
Integriteit	Het voorkomen van gewilde of ongewilde fouten of wijzigingen in data.
MD5-waarde	Een methode om een digitale handtekening van digitale informatie te kunnen berekenen.
Onbeschikbaarheid	De uitval van een informatiesysteem.
Sleutel	Een reeks geheim te houden tekens waarmee encryptie kan worden opgeheven.
SHA	Een moderne methode om een digitale handtekening van digitale informatie te kunnen berekenen. Deze is krachtiger dan de MD5-waarde vanwege veel langere sleutels.
Vertrouwelijkheid	Het principe dat informatie alleen gelezen kan worden door degene voor wie deze bedoeld is.

De CIA Triad

De overbekende afkorting CIA heeft naast 'Central Intelligence Agency' nog een betekenis. Het verwijst ook naar de principes waarop alle security is gebaseerd. In dat geval betekent het Confidentiality, Integrity en Availability. In het Nederlands klinkt het een stuk minder spannend, namelijk BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid).

We beginnen met een uitgebreide beschrijving van deze begrippen.



1.1 Vertrouwelijkheid – alleen de persoon waarvoor het bedoeld is

Recht op privacy heeft meestal betrekking op personen. Een wijs man noemde ooit 'vertrouwelijkheid' de privacy van data. Het betekent dat informatie alleen mag worden gelezen door degene waar deze voor bedoeld is. Als jij een mail stuurt naar iemand in Australië, dan heb je geen idee wat er onderweg met die informatie gebeurt. Is er misschien iemand die onderweg een verbinding afluistert en stiekem je mail leest? Je wilt natuurlijk 100% zeker weten dat dat niet kan.

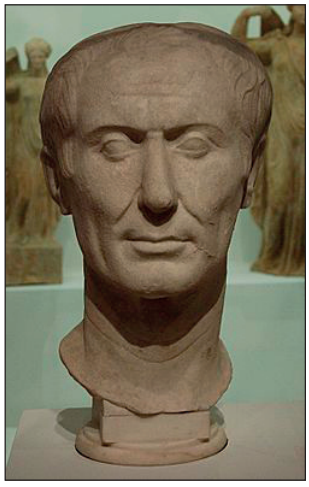
Confidentiality (vertrouwelijkheid) heeft te maken met wie er bij de informatie kan. Informatie mag niet bewust of onbewust gelezen kunnen worden door iemand waarvoor deze informatie niet bedoeld is. Documenten van de directeur van een bedrijf mogen niet door iedereen gelezen worden. Die bestanden wil je goed beveiligen zodat alleen de juiste personen ze kunnen lezen. Dit geldt ook voor bijvoorbeeld mail die je verstuurt of een WhatsApp-uitwisseling. Bestanden die zijn opgeslagen kun je vertrouwelijk maken door de toegang goed te organiseren (wie kan er bij?). In de praktijk wordt vertrouwelijkheid vooral bereikt door cryptografie toe te passen. Ook is de classificatie van data een belangrijke methode om vertrou-

welijkheid te kunnen garanderen. In paragraaf 1.1.1 wordt cryptografie en in 1.1.2 classificatie van informatie besproken.

1.1.1 Cryptografie

Stel je voor dat je een boodschap wilt versturen waarvan je 100% zeker wilt zijn dat deze niet door anderen kan worden gelezen, hoe pak je dat aan? Je stuurt een brief, maar die kan worden onderschept. Je stuurt een mail, maar die kan ook worden opgevangen. Dan misschien een telefoongesprek, dat kan worden afgeluisterd. Er is eigenlijk maar één manier om een boodschap volledig geheim over te brengen en dat is in geheimschrift, die alleen jij en de ontvanger kunnen lezen.

In de huidige tijd is geheimschrift vervangen door cryptografie: de techniek van het versleutelen van gegevens. Dit is de enige echt betrouwbare manier om je data veilig te houden. Alle data die jij *veilig* over het internet verstuurt worden versleuteld. Alleen jij en de ontvanger kennen de sleutel en kunnen zo op een slimme manier een onleesbare boodschap weer leesbaar maken. Het versleutelen van informatie of 'coderen' is een zeer belangrijke manier om gegevens geheim te houden. Dit versleutelen van informatie op basis van een bepaald algoritme wordt ook wel encryptie genoemd. In die zin is encryptie een toepassing van cryptografie. Beide termen worden door elkaar gebruikt.



Het begin van de cryptografie wordt vaak bij Julius Caesar (links), een Romeinse keizer, geplaatst. Hij leefde zo'n 100 jaar voor Christus en bedacht de zogenaamde *Caesar-versleuteling*. Hij schoof de letters in het alfabet een eindje op. Als hij 1 letter opschoof dan werd de a de b, de b de c enzovoort.

Eén letter opschuiven werkt zo:

HALLO CAESAR HOE GAAT HET MET JOU
wordt IBMMP DBFTBS IPF HBBU IFU NFU KPV

Haal de spaties weg en het bericht wordt onleesbaar:
IBMMPDBFTBSIPFHBBUIFUNFUKPV

Deze versleutelde boodschap werd naar de ontvanger gestuurd. Mocht iemand de boodschap onderscheppen, dan kon hij de boodschap niet lezen. De ontvanger kon de boodschap wel lezen, door de vooraf afgesproken verschuiving (de sleutel) toe te passen. Hij kon de letters terugschuiven in het alfabet. Voor die tijd was deze manier veilig, bijna niemand kon nog lezen, laat staan een cryptografische versleuteling oplossen.

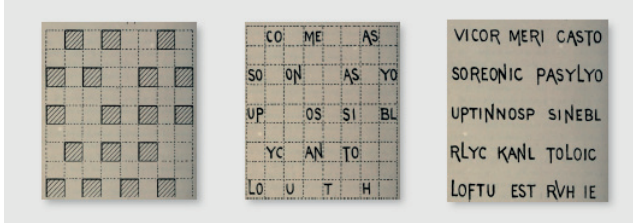
Opdracht 1.1 Vertrouwelijkheid: Caesar-verschuiving

Welke verschuiving is hieronder toegepast?
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
E F G H I J K L M N O P Q R S T U V W X Y Z A B C D

Ontsleutel met deze verschuiving de volgende zin:
GSRXEGXTIVWSSRMWNERLEVMKYMX IHI

Opdracht 1.2 Vertrouwelijkheid: Grille en Porta-tabel

Hieronder zie je twee oude vormen van encryptie. De eerste wordt een Grille genoemd en bestaat uit drie stukken papier. Beschrijf hoe deze manier van versleuteling werkt.



Hieronder zie je een tweede vorm van encryptie uit ongeveer 1560, de Porta-tabel, een manier om data vertrouwelijk te houden. Beschrijf de wijze waarop de data worden versleuteld.

A	B	a	b	c	d	e	f	g	h	i	j	k	l	m
		n	o	p	q	r	s	t	u	v	w	x	y	z
C	D	a	b	c	d	e	f	g	h	i	j	k	l	m
		z	n	o	p	q	r	s	t	u	v	w	x	y
E	F	a	b	c	d	e	f	g	h	i	j	k	l	m
		y	z	n	o	p	q	r	s	t	u	v	w	x
G	H	a	b	c	d	e	f	g	h	i	j	k	l	m
		x	y	z	n	o	p	q	r	s	t	u	v	w
I	J	a	b	c	d	e	f	g	h	i	j	k	l	m
		w	x	y	z	n	o	p	q	r	s	t	u	v
K	L	a	b	c	d	e	f	g	h	i	j	k	l	m
		v	w	x	y	z	n	o	p	q	r	s	t	u
M	N	a	b	c	d	e	f	g	h	i	j	k	l	m
		u	v	w	x	y	z	n	o	p	q	r	s	t
O	P	a	b	c	d	e	f	g	h	i	j	k	l	m
		t	u	v	w	x	y	z	n	o	p	q	r	s
Q	R	a	b	c	d	e	f	g	h	i	j	k	l	m
		s	t	u	v	w	x	y	z	n	o	p	q	r
S	T	a	b	c	d	e	f	g	h	i	j	k	l	m
		r	s	t	u	v	w	x	y	z	n	o	p	q
U	V	a	b	c	d	e	f	g	h	i	j	k	l	m
		q	r	s	t	u	v	w	x	y	z	n	o	p
W	X	a	b	c	d	e	f	g	h	i	j	k	l	m
		p	q	r	s	t	u	v	w	x	y	z	n	o
Y	Z	a	b	c	d	e	f	g	h	i	j	k	l	m
		o	p	q	r	s	t	u	v	w	x	y	z	n

Porta's tabel uit 1563

Je neemt een tekst, bijvoorbeeld 'bad', en de sleutel, bijvoorbeeld 'KAT'. Dit levert op 'wnu'.

Zie je hoe het werkt?

Opdracht 1.3 Vertrouwelijkheid: Je eigen cryptosysteem

Hieronder volgt een voorbeeld dat je kunt gebruiken om zelf een cryptosysteem te maken om je data vertrouwelijk te houden.

Vereist is dat de boodschap alleen uit blokletters en spaties (niet meer dan 30 tekens) bestaat. Kies vervolgens een geheel getal onder de 10 (voor de eenvoud niet te groot). Wij kiezen hier 4.

Versleutelen

- Schrijf een boodschap.
- Verwijder de leestekens en spaties als die er zijn.
- Verdeel je tekst in blokjes van 4 letters.
- Schrijf de tekst per blokje achterstevoren op.
- Voeg alle blokjes weer bij elkaar tot één lange tekst.
- Bijvoorbeeld: amsterdam wordt **amst erda m** dan **tsma adre m** dan **tsmaadrem**.
- Pas nu de Caesar-verschuiving van 4 toe en het wordt: **xwpeehvip**

Ontsleutelen

- Pas de Caesar-verschuiving van 4 toe (letters schuiven terug in het alfabet).
- Verdeel de tekst in blokjes van lengte vier.
- Schrijf de tekst per blokje achterstevoren op.
- Voeg de blokjes samen tot één lange tekst.
- Lees de tekst goed door en voeg spaties toe (in dit voorbeeld is er maar één woord).

Je eigen systeem

- Schrijf een bericht dat bestaat uit blokletters en spaties.
- Kies een getal (de sleutel) en versleutel de boodschap op de manier zoals jij dat wilt.
- Je kunt gebruikmaken van de Caesar-verschuiving of van de tekstblokjes zoals hierboven. Ook een combinatie is mogelijk.
- Beschrijf je methode zoals in het voorbeeld hierboven.
- Je eerste cryptografische systeem is een feit.

Je hebt hier kennisgemaakt met cryptografie als methode om data geheim te houden. Je leerde hoe data kunnen worden versleuteld en alleen via een sleutel weer gelezen kunnen worden.

Practicum 1.1 Klassieke cryptografie

In het practicum komen nog enkele vormen van klassieke encryptie aan bod, onder andere uit de Eerste en Tweede Wereldoorlog.

1.1.2 Classificatie van informatie

Soms is het wenselijk dat sommige personen bepaalde documenten mogen lezen en andere personen niet.

Er zijn vele documenten waar in meerdere of mindere mate vertrouwelijke informatie in is verwerkt, bijvoorbeeld jouw medisch dossier of iemands strafblad. In een groot bedrijf waar dagelijks honderden documenten worden gemaakt kan het heel lastig zijn om bij te houden wie wel en wie niet bepaalde informatie mag lezen. Een goede indeling van informatie naar vertrouwelijkheid is hierbij erg behulpzaam. Deze indeling van de vertrouwelijkheid van informatie noemt men *classificatie*.

Vervolgens beveilig je de data al naar gelang de belangrijkheid van de inhoud. De bekendste classificatie is waarschijnlijk wel 'Top Secret' die in iedere spionnenfilm wel een keer voorkomt. Dat soort documenten ligt in een grote kluis, terwijl de reclamefolders gewoon op de deurmat liggen. Die folders hebben als classificatie 'publiek', iedereen kan er bij.

Het classificeren van informatie bepaalt welke informatie wel of niet van groot belang is binnen een bedrijf. Een nieuwsbrief of een reclamefolder heeft over het algemeen een lage classificatie, een document waarin staat vermeld wie er volgende week ontslagen wordt, heeft juist een hoge classificatie.

De overheid

Een bekend classificatiesysteem dat vooral door regeringen wordt gebruikt, komt van de Amerikaanse regering. Hoe gevoeliger de informatie in een document is, hoe hoger de classificatie.

Top Secret (zeer geheim): Informatie kan in verkeerde handen grote schade kan toebrengen aan een heel land.

Secret (geheim): Informatie kan in verkeerde handen grote schade toebrengen aan de nationale veiligheid.

Confidential (vertrouwelijk): Informatie kan in verkeerde handen schade toebrengen aan de nationale veiligheid. Hieronder een gelekt document met die classificatie (Wikileaks-website).

DUTCH EU PRESIDENCY: THE VIEW FROM THE HAGUE

Date:	2004 July 2, 14:45 (Friday)	Canonical ID:	04THEHAGUE1670_a
Original Classification:	CONFIDENTIAL	Current Classification:	CONFIDENTIAL
Handling Restrictions	-- Not Assigned --	Character Count:	13058
Executive Order:	-- Not Assigned --	Locator:	TEXT ONLINE
TAGS:	EU - Europa Island | NL - Netherlands	Concepts:	-- Not Assigned --

Sensitive but unclassified (gevoelig maar niet geclassificeerd): Deze informatie kan in verkeerde handen nadelige gevolgen hebben voor de nationale veiligheid.

Unclassified (niet geclassificeerd): Deze term wordt gebruikt voor informatie die geen schade aanricht in verkeerde handen.

NIGERIA: 2009 INVESTMENT CLIMATE STATEMENT

Date:	2009 January 16, 06:45 (Friday)	Canonical ID:	09ABUJA88_a
Original Classification:	UNCLASSIFIED	Current Classification:	UNCLASSIFIED
Handling Restrictions	-- Not Assigned --	Character Count:	50585
Executive Order:	-- Not Assigned --	Locator:	TEXT ONLINE
TAGS:	ECON - Economic Affairs--Economic	Concepts:	-- Not Assigned --

Op de indeling is 'need to know' van toepassing: iemand die een als Secret geclassificeerd document mag lezen, heeft *niet* automatisch recht op alle Secret documenten.

Bedrijven en private sector

Voor gebruik in doorsneebedrijven is de bovenstaande indeling behoorlijk overdreven. De meeste bedrijven en organisaties gebruiken vaak de volgende indeling:

Openbaar: Mag door iedereen gelezen worden (een reclamefolder), richt geen schade aan bij openbaarmaking.
Bedrijfsvertrouwelijk: Alleen voor medewerkers (informatie over klantbehandeling), richt enige schade aan bij openbaarmaking.
Vertrouwelijk: Bijvoorbeeld dossiers van personeelszaken, kan flinke schade aanrichten aan het bedrijf. Als de directeur een gokprobleem blijkt te hebben kan dit het bedrijf schade berokkenen.
Geheim: Bijvoorbeeld overnameplannen, die alleen toegankelijk zijn voor wie ze zijn bedoeld. Overtreding van deze classificatie kan zeer grote schade toebrengen.

De kwalificatiecriteria

Als je documenten of andere digitale informatie wilt classificeren, hoe bepaal je dan de waarde? Meestal wordt gebruik gemaakt van drie criteria:

Waarde: De geldwaarde van informatie wordt het meest gebruikt om die informatie te classificeren. Een grote klantendatabase is hier een goed voorbeeld van. Als die in verkeerde handen valt, kun je veel klanten kwijtraken.
Leeftijd: Hoe ouder de informatie is, hoe lager de classificatie. Oude geheimen zijn vaak niet belangrijk meer. De aandelenkoersen van vijf jaar geleden bijvoorbeeld hebben geen waarde meer.
Nut: Als informatie niet langer nuttig is, daalt de classificatie. Voorbeeld is een medisch dossier van een werknemer die ergens anders is gaan werken.

Opdracht 1.4 Vertrouwelijkheid: classificatie

Met deze opdracht werk je als security-beheerder op een school. Op deze school zijn directie, managers, docenten en deelnemers actief. Aan jou wordt de vraag gesteld om een classificatiesysteem te maken voor documentatie binnen de school. Je neemt als uitgangspunt dat momenteel iedere werknemer op een afdeling bij alle documenten kan die bij die afdeling horen, maar bij geen enkel document van een andere afdeling.

De **directie** maakt drie soorten documenten:

a Financiële plannen (welke afdeling of opleiding krijgt hoeveel geld voor komend jaar?)
b Organisatorische plannen (welke opleiding wordt uitgebreid, komen er gebouwen bij?)

c Personele plannen (wat gaat er volgend jaar gebeuren, moet misschien personeel ergens anders gaan werken, hoeveel gaat iedereen volgend jaar verdienen?)

De **managers** schrijven documentatie over:

d Deelnemersaantallen (hoe meer deelnemers hoe meer geld en personeel)
e Onderwijsindeling (welke vakken worden gegeven en door wie, bij welk vak horen welke middelen en welk lokaal?)
f Personele plannen (welke docenten doen het goed of juist niet, welke docenten worden bijgeschoold en waarom?)

De **docenten** schrijven documenten over:

g Deelnemers (welke deelnemers doen het goed en welke niet?)
h Lesmateriaal (hoe worden de lessen gegeven en wat leren we deelnemers?)
i Examens (de toetsen en examens die door de deelnemers worden gemaakt en cijferlijsten)

De **deelnemers** schrijven documentatie over:

j Lessen die zij volgen en opdrachten die zij maken
k Klachten en problemen die zij hebben met andere deelnemers of docenten
l Examens die zij maken

Je maakt een overzicht van de documentatie en kiest een classificatie. Om de documenten te kunnen beoordelen kijk je naar degene die het heeft geschreven (welke functie). Dan deel je de documenten in op basis van de criteria die hierboven zijn vermeld.

We voeren een analyse uit om een classificatie te maken. We doen het volgende.
We schatten de *waarde* in: onbelangrijk = 1, belangrijk = 2 en zeer belangrijk = 3
We schatten de *leeftijd* in: onbelangrijk = 1, belangrijk = 2 en zeer belangrijk = 3
We schatten het *nut* in: onbelangrijk = 1, belangrijk = 2 en zeer belangrijk = 3

We maken eerst een tabel met daarin de documenten, kennen een score toe en vermenigvuldigen dan de scores met elkaar. Een aantal waardes is al ingevuld, jij vult de ontbrekende waardes in op basis van je eigen inschatting.

Plannen	Waarde	Leeftijd	Nut	Totaal
DIRECTIE				
a Financiële plannen	3	2	3	18
b Organisatorische plannen				
c Personele plannen				

Plannen	Waarde	Leeftijd	Nut	Totaal
MANAGEMENT				
d Deelnemers aantallen				
e Onderwijsindeling				
f Docenten plannen	2	2	3	
DOCENTEN				
g Deelnemers beschrijven	3	1	3	
h Lesmateriaal				
i Examens				
DEELNEMERS				
j Lessen				
k Klachten	1	1	3	3
l Examenresultaten				

Nu maken we een nieuwe tabel en maken een inschatting bij welke score welke classificatie hoort. De laagste score is 1 (1 * 1 *1) en de hoogste is 27 (3 * 3 * 3).

Bij welke laagste en hoogste waarde behoort een document in welke klasse? Hoe zou jij dit indelen? Vul de overige waarden in.

Classificatie	Ondergrens	Bovengrens
Openbaar	1	
Bedrijfsvertrouwelijk		
Vertrouwelijk		
Geheim		27

Je hebt nu je eigen classificatiesysteem gemaakt, een goede manier om informatie vertrouwelijk te houden.

Samenvatting vertrouwelijkheid

Vertrouwelijkheid vormt een van de pijlers waarop security is gebaseerd, de geheimhouding van informatie komt op vele gebieden terug. Zowel de gegevens van nucleaire raketten als van een dagboek is informatie die men geheim wil houden. De manier om geheimhouding te garanderen is de gegevens te versleutelen, je maakt later in het boek nog uitgebreid kennis met cryptografie. Voorlopig is het voldoende om te begrijpen dat 100% vertrouwelijkheid absoluut noodzakelijk is voor een goede toepassing van beveiligingsmaatregelen. We kunnen rustig stellen: zonder vertrouwelijkheid geen beveiliging. Dit geldt ook voor het onderwerp van de volgende paragraaf, integriteit.