
HO
GENT

Cybersecurity

2. De cybersecurity kubus

2. De cybersecurity kubus

2.1 De 3 dimensies van de cybersecurity kubus
2.2 De CIA-driehoek
2.3 De 3 staten van data
2.4 Beveiligingsmaatregelen
2.5 Het cybersecurity ISO model

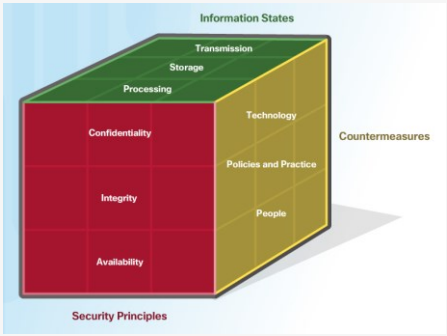
HO
GENT

2.1 De 3 dimensies van de cybersecurity kubus

HO GENT

De 3 dimensies

1. Beveiligingsprincipes
2. De staten van data
3. Beveiligingsmaatregelen

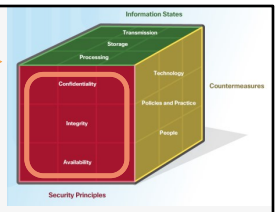


McCumber Cube

HO GENT

2.1 De 3 dimensies van de cybersecurity kubus

Volg hier mee waar we ons telkens bevinden in de cybersecurity kubus



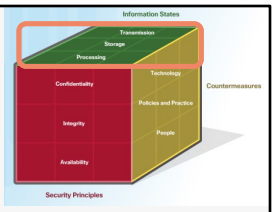
Beveiligingsprincipes

- Identificeert het doel van beveiling
- Er zijn 3 principes (de CIA-driehoek):
  - Vertrouwelijkheid (Confidentiality)
  - Integriteit (Integrity)
  - Beschikbaarheid (Availability)

- Helpen cybersecurity specialisten om prioriteiten te stellen om de cyberwereld te beveiligen

HO GENT

Staten van data

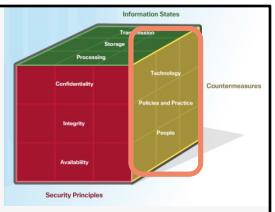


- Alles in de cyberwereld draait rond data. Cybersecurity specialisten focussen zich op het beveiligen van die data
- Data heeft 3 mogelijke staten:
  - Data in rust/opslag
  - Data tijdens het verzenden
  - Data tijdens het verwerken

HO GENT

2.1 De 3 dimensies van de cybersecurity kubus

Beveiligingsmaatregelen



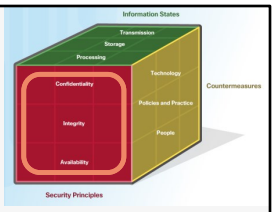
- Er zijn 3 types beveiligingsmaatregelen:
  - Technologieën
    - Toestellen en producten die gebruikt kunnen worden om informatie te beschermen en cybercriminelen af te weren.
  - Beleid en praktijken
    - Procedures en richtlijnen die de burgers van de cyberwereld veilig houden en aansporen om goede praktijken te volgen.
  - Personen
    - Men is zich bewust van en kent de gevaren van de cyberwereld.

HO GENT

2.2 De CIA driehoek

HO
GENT

De CIA-driehoek

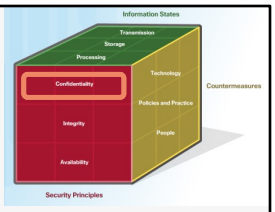


- Vertrouwelijkheid (Confidentiality)
  - Wie mag dit zien?
  - Bv. chatgesprekken, bedrijfsgeheimen, medische informatie, …
- Integriteit (Integrity)
  - Klopt dit wel?
  - Bv. financiële transacties, contracten, …
- Beschikbaarheid (Availability)
  - Kan ik er aan wanneer ik het nodig heb?
  - Bv. 112-noodcentrale, chamilo.hogent.be tijdens online examen, e-mail servers, internet-toegang, …

HO GENT

2.2 De CIA-driehoek

Vertrouwelijkheid

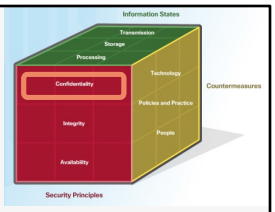


- Verhindert de bekendmaking van informatie aan onbevoegde personen, bronnen en processen
- Organisaties moeten hun personeel opleiden om zo goed mogelijk om te gaan met gevoelige informatie om zichzelf en hun organisaties te beschermen tegen aanvallen
- Vertrouwelijkheid kan verkregen worden door encryptie, authenticatie en toegangscontrole

HO GENT

2.2 De CIA-driehoek

Vertrouwelijkheid

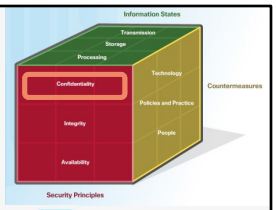


- Organisaties verzamelen enorme hoeveelheden data
  - Sommige data is publiek beschikbaar en niet gevoelig
    - Bv. telefoonnummers, namen, …
  - Andere data is wel gevoelig en wordt beschermd om personen of organisaties te beschermen
    - Bv. medische patientgeschiedenis, financiële toestand, …

HO GENT

2.2 De CIA-driehoek

Vertrouwelijkheid



German politicians targeted in mass data attack

4 January 2019

Angela Merkel, Greens leader Robert Habeck and TV satirist Jan Böhmermann have all been targeted by the attack

Hundreds of German politicians, including Chancellor Angela Merkel, have had personal details stolen and published online.

Contacts, private chats and financial details were put out on Twitter that belong to figures from every political party except the far-right AfD.

Data from celebrities and journalists were also leaked.

Intel Suffers Apparent Data Breach, 20GB of IP and Documents Leaked on to Internet

by Ryan Smith on August 6, 2020 8:45 PM EST

Posted in CPUs Intel Crime

81 Comments

+ Add A Comment

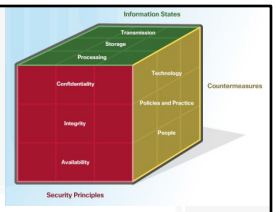
Intel today became the apparent victim of a massive internal data breach, as roughly 20 GB of various Intel documents and tools have begun showing up in a data cache uploaded to the wider internet. With materials seemingly spanning over a decade, the breach reportedly includes everything from Intel presentation templates to BIOS code and debugging tools, and would represent one of the biggest intellectual property leaks from a chipmaker in years.

HO GENT

https://www.bbc.com/news/world-europe-46757009
https://www.anandtech.com/show/15962/intel-data-breach-20gb-of-ip-leaked

2.2 De CIA-driehoek

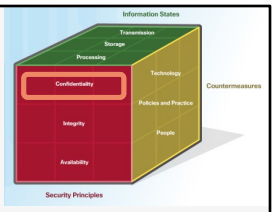
Vertrouwelijkheid



HO GENT

2.2 De CIA-driehoek

Vertrouwelijkheid



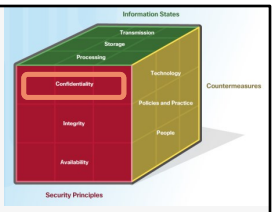
Toegangscontrole omvat een aantal beschermingsmaatregelen die onbevoegde toegang tot computers, netwerken, databanken of andere databronnen verhindert. Deze maatregelen kunnen onderverdeeld worden in de 3 categorieën (AAA):

- Authenticatie (Authentication)
  - Wie mag iets doen?
- Autorisatie (Authorisation)
  - Wat mag iemand wel/niet doen?
- Boekhouding (Accounting)
  - Wie heeft wat gedaan?

HO GENT

Accounting wordt soms ook aangeduid met de term "non-repudiation" (onweerlegbaarheid). M. a. w. iets kan achteraf niet in twijfel getrokken worden.

Vertrouwelijkheid

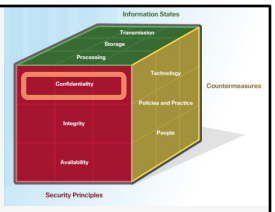


Voorbeeld 1: Bankautomaat

- Authenticatie (Authentication)
  - Enkel iemand met de juiste bankkaart en pincode heeft toegang tot de bankrekening
- Autorisatie (Authorisation)
  - Iemand kan niet meer geld afhalen dan hij heeft
  - Er is een maximum bedrag dat afgehaald kan worden per dag
- Boekhouding (Accounting)
  - Op de rekeninguitreksels staat er welk bedrag er wanneer is gestort op of afgehaald van de rekening

HO GENT

Vertrouwelijkheid

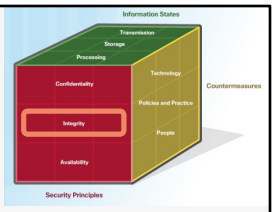


Voorbeeld 2: Forum

- Authenticatie (Authentication)
  - Je moet je aanmelden met een username en paswoord
- Autorisatie (Authorisation)
  - Een gewone gebruiker kan berichten lezen en zelf berichten aanmaken
  - Administratoren kunnen ook topics beheren of afsluiten, berichten van andere gebruikers bewerken en verwijderen en hebben toegang tot administrator topics die niet voor gewone gebruikers zichtbaar zijn.
- Boekhouding (Accounting)
  - Er zijn logs die bij houden wanneer wie welke actie op het forum heeft uitegvoerd (bv. op 25/09/2020 heeft administrator Alice het bericht met id 68132 van Bob verwijderd)

HO GENT

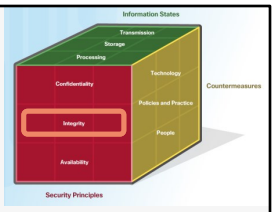
Integriteit



- Integriteit is de nauwkeurigheid, consistentie en betrouwbaarheid van data zolang die data bestaat. Een andere term is de kwaliteit
- Methodes om integriteit te garanderen omvatten hashing, data validatie checks, data consistentie checks en toegangscontroles
- De nood aan integriteit hangt af van de aard van de data. Bijvoorbeeld:
  - Facebook verifieert de data in een gebruikerspost niet
  - Transactie en bedragen bij een bank moeten steeds 100% correct zijn

HO GENT

Integriteit

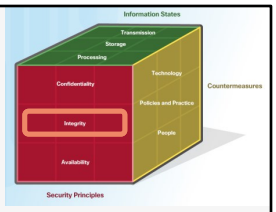


- Verlies van integriteit kan enorme schade brengen aan personen en organisaties, en kan databronnen onbruikbaar of onbetrouwbaar maken
- Een integriteitscontrole is een manier om te bekijken een verzameling van data (bestanden, foto's, transacties, ...) nog steeds correct zijn (niet corrupt of beschadigd). Hiervoor wordt vaak een hash functie gebruikt

HO GENT

2.2 De CIA-driehoek

Integriteit



Onderzoekers kunnen Nederlandse verkeerslichten van afstand op groen zetten

Twee beveiligingsonderzoekers hebben een manier gevonden om Nederlandse verkeerslichten te manipuleren. In zeker tien Nederlandse steden worden 'slimme verkeerslichten' gebruikt, maar door fietsers te spoofen kunnen de lichten op groen worden gezet.

In verschillende Nederlandse steden worden pilots gehouden met slimme verkeerslichten en apps. Als fietsers een bepaalde app installeren kan het verkeerslicht herkennen dat ze eraan komen, om zo precies op het juiste moment groen te worden. In het onderzoek konden Wesley Neelen en Rik van Duijn van beveiligingsbedrijf Zolder zich voordoen als fietsers en dus van een afstand een verkeerslicht op groen zetten.

New hacking risks threaten US election as online voting considered

Ballots 'could be manipulated at scale', investigators find

David E. Sanger, Nicole Perlroth, Matthew Rosenberg | Monday 08 June 2020 10:34

With the US election less than 150 days away, there are rising concerns that the push for remote voting prompted by the pandemic could open new opportunities to hack the vote — for Vladimir Putin, but also others hoping to disrupt, influence or profit from the election.

Most popular

The Wind In The Willows, Royal Opera House, Londo
<3-- none onestar

Thai Hospitals and Companies Hit by Ransomware Attacks

By Reuters, Wire Service Content Sept. 10, 2020, at 7:31 a.m.

BANGKOK (REUTERS) - Hospitals and companies in Thailand were hit by hackers who held their computer systems and data ransom, demanding payment to restore information, police said on Thursday.

Chilean bank shuts down all branches following ransomware attack

All BancoEstado branches will remain closed on Monday, September 7, and possibly more days.

By Catalin Cimpanu for Zero Day | September 7, 2020 -- 16:31 GMT (17:31 BST) | Topic: Security

HO GENT

https://en.wikipedia.org/wiki/Stuxnet is een mooi voorbeeld! (vermoedelijke US/Israelische staatshackers pasten machine waarden aan om nucleaire machines in Iraanse faciliteiten te vernielen)
https://tweakers.net/nieuws/170598/onderzoekers-kunnen-nederlandse-verkeerslichten-van-afstand-op-groen-zetten.html
https://www.independent.co.uk/us-election-2020/2020-election-trump-online-voting-hack-russia-mail-a9553811.html
https://www.usnews.com/news/world/articles/2020-09-10/thai-hospitals-and-companies-hit-by-ransomware-attacks
https://www.zdnet.com/article/chilean-bank-shuts-down-all-branches-following-ransomware-attack/
https://www.infosecurity-magazine.com/magazine-features/financial-markets-a-playground-for/
https://www.defenseone.com/threats/2015/09/next-wave-cyberattacks-wont-steal-data-theyll-change-it/120701/

2.2 De CIA-driehoek

Integriteit

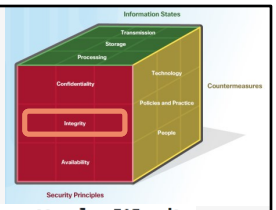


Photo credit: lev radin/Shutterstock.com

It's the kind of thing you might imagine happening in a cyberwar. Last year, a hacking attack wiped out 1% of the US stock market's value – around $136bn – in a little over a second. It didn't take months of careful orchestration, the theft of trading exchange source code, or the theft of insider information. All it took was the hacking of a Twitter account.

The Associated Press owns the account in question, and the attacker – still unidentified – gained access, using it to post a report saying the White House had been bombed, and the President injured. The market went wild. As stock prices slumped, US treasury bonds – a traditionally stable asset that people retreat to in times of extreme uncertainty – spiked. Futures contracts on the CBOE volatility index (known as the VIX, an index that tracks market volatility) also spiked in price. And it all happened in the space of about five minutes, at which point the AP corrected the bogus tweet, and the markets returned to normal.

The Next Wave of Cyberattacks Won't Steal Data — They'll Change It

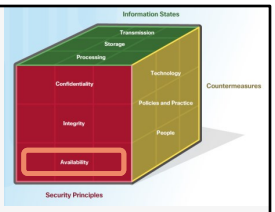
America's intelligence chiefs say data that goes missing may become the least of our cyber worries.

Stuxnet, a computer worm, discovered in June 2010, that was specifically written to take over certain programmable industrial control systems and cause the equipment run by those systems to malfunction, all the while feeding false data to the systems monitors indicating the equipment to be running as intended.

HO GENT

2.2 De CIA-driehoek

Beschikbaarheid



- Informatiesystemen moeten op elk moment beschikbaar zijn
- Aanvallen en fouten kunnen toegang tot systemen in gevaar brengen
- Maatregelen voor beschikbaarheid: redundantie, backups, verhoogde weerstand, onderhoud, up-to-date software en OS, noodplannen om terug online te komen na een onvoorziene omstandigheid, gebruik van nieuwe technologieën, detecteer ongebruikelijke activiteit en beschikbaarheidstesten

HO GENT

2.2 De CIA-driehoek

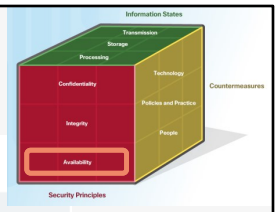
Beschikbaarheid

Kaspersky: leeromgevingen zijn vaker doelwit van ddos-aanvallen

Het aantal ddos-aanvallen op leeromgevingen is dit voorjaar met meer dan 350 procent toegenomen. Dat zegt Kaspersky op basis van eigen onderzoek. De stijging was in januari het sterkst, met 550 procent meer ddos-aanvallen dan in januari 2019 het geval was.

In de maanden maart en mei was de stijging het kleinst, blijkt uit het Digital Education-onderzoek van Kaspersky. In maart was de stijging 350 procent, in mei 357 procent. In januari, februari, april en juni lag de stijging op 450 procent of hoger. Volgens Kaspersky lag het aantal ddos-aanvallen op leeromgevingen dit jaar hoger, omdat deze online leeromgevingen dit jaar vaker worden gebruikt. Vanwege het coronavirus kregen veel studenten wereldwijd sinds dit jaar meer les op afstand, waarbij dergelijke omgevingen worden gebruikt.

Januari	Februari	Maart	April	Mei	Juni
550 procent	500 procent	350 procent	480 procent	357 procent	450 procent



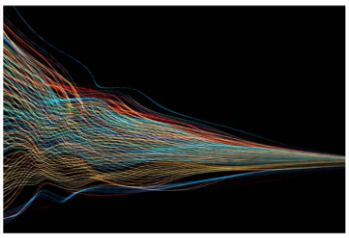
DDoS-aanval treft edpnet

31/08/20 om 16:14 Bijgewerkt om 16:14 Bron: DataNews

Pieterjan Van Leemputten
is redacteur bij Data News

De alternatieve provider edpnet ondervindt al enkele dagen problemen door een grootschalige DDoS-aanval. Ook Nederlandse providers lagen recent onder vuur.

8
Keer gedeeld



. © Getty Images

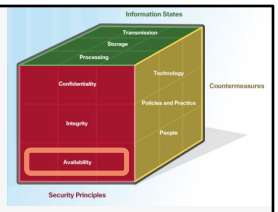
Klanten van edpnet kunnen momenteel problemen ondervinden met hun internet. Vooral dan met het verbinden met sommige websites. De operator krijgt sinds vrijdag aanvalsgolven te verwerken, maar de aanval van vandaag lijkt langer aan te houden.

HO GENT

https://tweakers.net/nieuws/171896/kaspersky-leeromgevingen-zijn-vaker-doelwit-van-ddos-aanvallen.html
https://datanews.knack.be/ict/nieuws/ddos-aanval-treft-edpnet/article-news-1635675.html?cookie_check=1600001131
https://tweakers.net/nieuws/171594/belgische-provider-edpnet-heeft-al-vier-dagen-te-maken-met-ddos-aanvallen.html
https://issues.edpnet.be/?p=3099

2.2 De CIA-driehoek

Beschikbaarheid

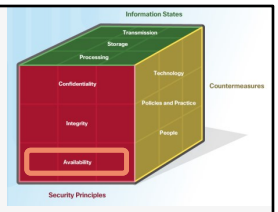


HO GENT

https://www.techradar.com/news/aws-stops-largest-ddos-attack-ever
https://www.bbc.com/news/technology-35204915
https://github.blog/2018-03-01-ddos-incident-report/

2.2 De CIA-driehoek

Beschikbaarheid



Patient Dies After Ransomware Attack on Düsseldorf Hospital

According to reports, the network failure announced by Düsseldorf University Hospital (UKD) last week – which turned out to be a ransomware infection – has resulted in a patient dying.

"In the morning hours of Thursday (September 10th), larger parts of the IT systems of the Düsseldorf University Hospital were gradually no longer usable," the institution said in a notice last week. "This has far-reaching consequences for hospital operations, as activities in the computer system are necessary for many processes. For this reason, the UKD has canceled the emergency care," reads a machine-translated version of the notice.

On September 11, a day after the network failure, UKD was already investigating a "possible hacker attack." The Associated Press now reports:

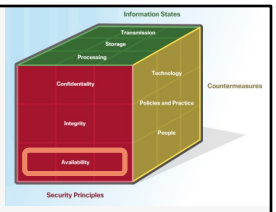
"German authorities say a hacker attack caused the failure of IT systems at a major hospital in Duesseldorf, and a woman who needed urgent admission died after she had to be taken to another city for treatment."

HO GENT

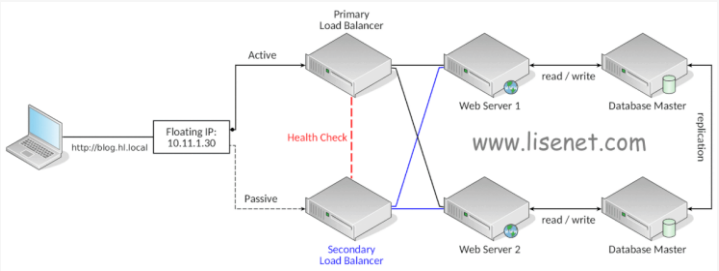
https://hotforsecurity.bitdefender.com/blog/patient-dies-after-ransomware-attack-on-dusseldorf-hospital-24159.html

2.2 De CIA-driehoek

Beschikbaarheid



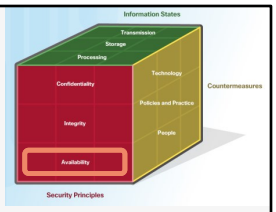
- Altijd-online systemen hebben typisch 3 pijlers:
  - Vermijd zwakke punten (single point of failure)
  - Zorg voor betrouwbare overdrachtsystemen
  - Detecteer storingen zodra ze zich voordoen



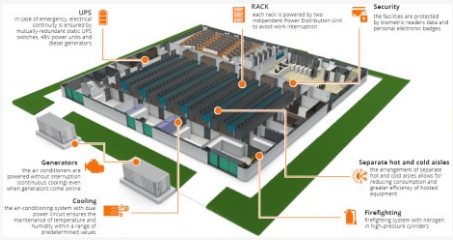
HO GENT

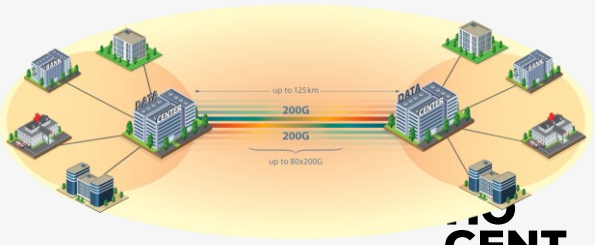
2.2 De CIA-driehoek

Beschikbaarheid



- Altijd-online systemen hebben typisch 3 pijlers:
  - Vermijd zwakke punten (single point of failure)
  - Zorg voor betrouwbare overdrachtsystemen
  - Detecteer storingen zodra ze zich voordoen



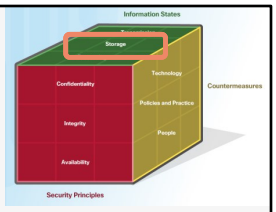


GENT

2.3 De staten van data

HO
GENT

Data in rust

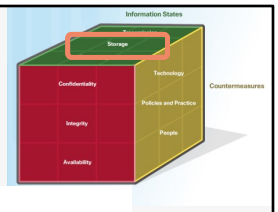


- Data opgeslagen op opslagapparaten (harde schijven, USB-sticks, databanken, …) dat niet wordt gebruikt door personen of processen
- Opslagapparaten kunnen lokaal (harde schijf, USB-stick, …) of gecentraliseerd op afstand aangesloten zijn (Dropbox, Google drive, NAS, …)
- Data kan zo verloren of gestolen worden
  - Harde schijf kapot
  - Laptop vergeten op trein
  - Smartphone gestolen

HO GENT

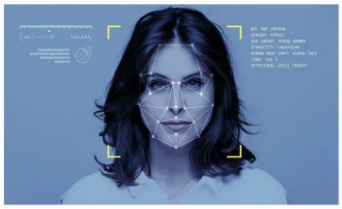
2.3 De staten van data

Data in rust



Major breach found in biometrics system used by banks, UK police and defence firms

Fingerprints, facial recognition and other personal information from Biostar 2 discovered on publicly accessible database



▲ Security company Suprema uses facial recognition, fingerprints and passwords to secure facilities for the likes of the Metropolitan Police, defence contractors and banks. Photograph: iZusek/Getty Images/iStockphoto

The fingerprints of over 1 million people, as well as facial recognition information, unencrypted usernames and passwords, and personal information of employees, was discovered on a publicly accessible database for a company used by the likes of the UK Metropolitan police, defence contractors and banks.

Major Recent Example of an Unencrypted USB breach

Case in point, Heathrow Airport in London (October 30, 2017) uses Unencrypted USB Drives for its non-cloud storage. Unfortunately, they were not standardized on Encrypted USB drives. Their lack of implementing proper standards in data security / data loss protection with encrypted USB storage has now cost the EU a major breach of confidential and restricted information.

London – An Unencrypted USB just gave away "confidential" / "restricted" files:

- The drive had 76 folders / 174 documents
- Details of measures used to protect the Queen
- Files disclosed the types of ID needed to access restricted areas
- A timetable of security patrols
- Maps pinpointing CCTV cameras
- One document highlighted recent terror attacks and talked about the type of threat the airport could face

USB losses like this happens more frequently than expected or thought and are prime examples why implementing an encrypted USB standard / policy should be a top priority; within your personal habits and most urgently, your organization. Learn more

HO GENT

https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms
https://www.kingston.com/belgium/us/community/articledetail/articleid/49705

2.3 De staten van data

Data in rust

Lost USB drive leads to breach of 6,000 patient records

by healthcarebus | January 24, 2013 | Comments (1)

Many healthcare providers have policies about clinicians and staff members carrying sensitive patient data around on laptops, tablets and smartphones. But here's another mobile gadget to address in those rules:

USB thumb drives.

Though they're certainly convenient for transferring data from location to location, those tiny, portable and easily misplaced storage devices have also been responsible for plenty of data breaches.

Most recently, it was a breach of healthcare data caused by a lost drive.

The Utah Department of Health (UDOH) recently notified affected Medicaid recipients that their data may have been compromised after it was misplaced by a third-party contractor.

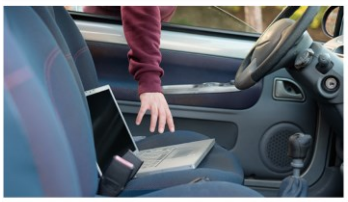
According to UDOH, an employee of the contractor, Good Health Systems (GHS), loaded personal health information about 6,000 individuals onto an unencrypted USB thumb drive while traveling between Salt Lake City, Denver and Washington, DC.

The drive didn't contain any Social Security numbers or financial information, but was loaded with patients' names, Medicaid identification numbers, ages and prescription drug history.

Data of 43,000 patients breached after theft of unencrypted laptop

A laptop of a Coplin Health Systems employee was stolen from a car in November and serves as a reminder to healthcare organizations to encrypt all data that physically leave the building.

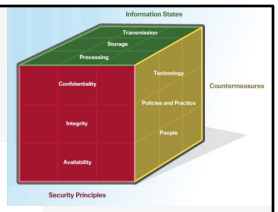
By Jessica Davis | January 12, 2018 | 11:50 AM



West Virginia-based Coplin Health Systems is notifying 43,000 patients of a potential data breach due to the theft of a laptop from an employee's car.

Officials discovered the theft on Nov. 2. And while the organization equipped the laptop with security tools and was password-protected, it failed to encrypt data stored on the hard drive.

Data on the laptop included patient names, Social Security numbers, financial information, addresses, dates of birth and medical data.



HO GENT

http://www.healthcarebusinesstech.com/data-breach-lost-usb-drive/
https://www.healthcareitnews.com/news/data-43000-patients-breached-after-theft-unencrypted-laptop

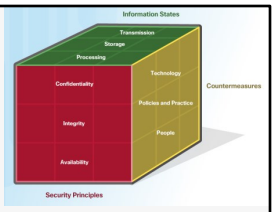
2.3 De staten van data

Data in rust

Hacker achterhaalt plaintext-wachtwoorden uit tweedehandscomputers van Tesla's

Tesla-bezitters lopen het risico dat gegevens over hun auto- en entertainmentgebruik in verkeerde handen vallen. Informatie uit de Media Control Unit, waaronder wachtwoorden, worden in plaintext opgeslagen. Die MCU's zijn inmiddels voor weinig geld op internet te koop.

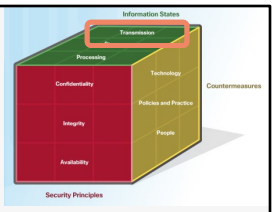
Dat zegt hacker Green The Only. Hij kocht verschillende oude infotainment-units van Tesla-computers op en wist daar informatie uit te achterhalen. Bij een upgrade van een auto worden zulke units vaak verwisseld, waardoor er inmiddels steeds meer voor steeds minder geld op tweedehandsmarktplaatsen zoals eBay worden aangeboden. De hacker ontdekte niet alleen informatie over de gebruiker, maar ook wachtwoorden en toegangstokens voor externe apps.



HO GENT

https://tweakers.net/nieuws/166742/hacker-achterhaalt-plaintext-wachtwoorden-uit-tweedehandscomputers-van-teslas.html

Data tijdens het verzenden

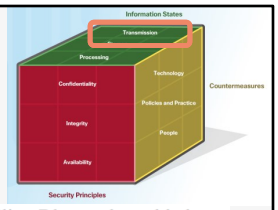


- Verschillende manieren:
  - Sneaker net: gebruikt opslagapparaten om data tussen computers over te zetten (USB-stick, draagbare harde schijf, ...)
  - Bedraad netwerk: gebruikt koperkabels
  - Draadloos netwerk: gebruikt elektromagnetische straling (kan door iedereen in de buurt "gehoord" worden)
- Een van de grootste uitdagingen voor cybersecurity personeel om te beveiligen. Enkele uitdagingen:
  - Cybercriminelen kunnen data tijdens het verzenden afluisteren, kopiëren of stelen (vertrouwelijkheid)
  - Cybercriminelen kunnen data tijdens het verzenden aanpassen (integriteit)
  - Cybercriminelen kunnen data tijdens het verzenden verhinderen of verstoren(beschikbaarheid)

HO GENT

2.3 De staten van data

Data tijdens het verzenden



WORLD NEWS JANUARY 23, 2020 / 10:46 PM / UPDATED 8 MONTHS AGO

U.N. says officials barred from using WhatsApp since June 2019 over security

By Reuters Staff 3 MIN READ

UNITED NATIONS (Reuters) - United Nations officials do not use WhatsApp to communicate because "it's not supported as a secure mechanism," a U.N. spokesman said on Thursday, after U.N. experts accused Saudi Arabia of using the online communications platform to hack the phone of Amazon chief executive and Washington Post owner Jeff Bezos.

KNOB attack threatens over a billion Bluetooth-enabled devices

August 15, 2019 By Pierluigi Paganini

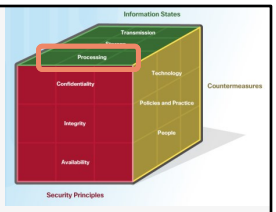
A vulnerability tracked as CVE-2019-9506 and referred as Key Negotiation of Bluetooth (**KNOB**) attack could allow attackers to spy on encrypted connections.

Researchers at the Center for IT-Security, Privacy and Accountability (CISPA) found a new Bluetooth vulnerability, referred as Key Negotiation of Bluetooth (KNOB) attack, that could allow attackers to spy on encrypted connections.

HO GENT

https://www.reuters.com/article/us-un-whatsapp/u-n-says-officials-barred-from-using-whatsapp-since-june-2019-over-security-idUSKBN1ZM32P
https://securityaffairs.co/wordpress/89890/hacking/bluetooth-knob-attack.html

Data tijdens het verwerken

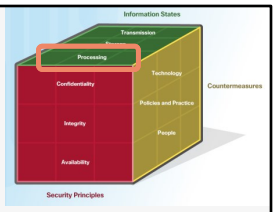


- Dit omvat data tijdens de invoer, aanpassing, berekening of uitvoer
- Organisaties gebruiken verschillende methodes om data te verzamelen: manuele invoer, het uploaden van bestanden, dataverzameling van sensoren, … . Elk van deze input-methoden is een mogelijke bedreiging voor integriteit
- Data kan aangepast worden door manuele verandering door gebruikers, programma's die de data wijzigen, defecte apparaten, … . Bijvoorbeeld encoderen/decoderen, compressie/decompressie, encryptie/decryptie zijn voorbeelden van data aanpassingen.
- Data dat zodanig wordt aangepast dat het fouten bevat of onbruikbaar wordt, noemt men corrupte data

HO GENT

2.3 De staten van data

Data tijdens het verwerken



Comment | Open Access | Published: 23 August 2016

Gene name errors are widespread in the scientific literature

Mark Ziemann, Yotam Eren & Assam El-Osta

Genome Biology **17**, Article number: 177 (2016) | Cite this article

123k Accesses | **41** Citations | **2491** Altmetric | Metrics

Abstract

The spreadsheet software Microsoft Excel, when used with default settings, is known to convert gene names to dates and floating-point numbers. A programmatic scan of leading genomics journals reveals that approximately one-fifth of papers with supplementary Excel gene lists contain erroneous gene name conversions.

The problem of Excel software (Microsoft Corp., Redmond, WA, USA) inadvertently converting gene symbols to dates and floating-point numbers was originally described in 2004 [1]. For example, gene symbols such as *SEPT2* (Septin 2) and *MARCH1* [Membrane-Associated Ring Finger (C3HC4) 1, E3 Ubiquitin Protein Ligase] are converted by default to '2-Sep' and '1-Mar', respectively. Furthermore, RIKEN identifiers were described to be

SQL Injection Still Causing Trouble

Posted on April 25, 2018

An on-going and important aspect of managing database security is designing your applications to avoid SQL injection attacks. SQL injection is a form of web hacking whereby SQL statements are specified in the fields of a web form to cause a poorly designed web application to dump database content to the attacker.

This type of attack has been known for years now, but still there are new stories where SQL injection was used for nefarious purposes. SQL injection played a role in a hacking incident during the 2016 US presidential election, TalkTalk — a UK-based telecoms company — suffered a data breach in 2015 due to SQL injection, and the hardware manufacturer Archos suffered a SQL injection attack late in 2014.

And remember the Heartland Payment Systems breach from 2009? That SQL injection attack cost $300 million and the hackers that pulled it off were recently sent to federal prison (February 2018).

HO GENT

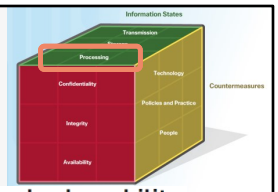
https://genomebiology.biomedcentral.com/articles/10.1186/s13059-016-1044-7
https://datatechnologytoday.wordpress.com/2018/04/25/sql-injection-still-causing-trouble/

Extra:

- https://tweakers.net/nieuws/163166/onderzoekers-lezen-data-van-computers-door-schermhelderheid-te-manipuleren.html
- https://tweakers.net/nieuws/166806/wetenschappers-luisteren-pc-af-door-frequentie-van-voedingen-te-manipuleren.html

2.3 De staten van data

Data tijdens het verwerken



Zoom liet e-mailadressen uitlekken

De veelgebruikte videobelapplicatie Zoom ligt onder vuur vanwege diverse beveiligingsproblemen. Zo liet de app persoonlijke e-mailadressen van gebruikers naar anderen uitlekken en zou het Windows-wachtwoord van gebruikers te onderscheppen zijn.

Zoom liet de e-mailadressen van 'zeker duizenden gebruikers' naar andere gebruikers uitlekken, schrijft Motherboard. Ook de bijbehorende profielfoto zou daarbij zitten. Zoom heeft een ingebouwde functie waarmee gebruikers met dezelfde domeinnaam elkaar gemakkelijk kunnen vinden. Die Company Directory-functie is vooral interessant voor bedrijven waarvan medewerkers de app gebruiken. Motherboard sprak met verschillende Zoom-gebruikers die met hun persoonlijke e-mailadres inlogden. Die werden in een lijst gezet met duizenden andere gebruikers, waarbij het leek alsof ze allemaal voor hetzelfde bedrijf werkten. De gebruikers konden op die manier elkaars accountinformatie zien. Dat gebeurde bij gebruikers die bij Nederlandse e-mailproviders waren aangesloten. Als die bijvoorbeeld een @xs4all.nl-, @dds.nl- of @quicknet.nl-e-mailadres hadden, konden ze alle andere gebruikers met zulke adressen zien. Xs4all zegt op Twitter dat het probleem bij Zoom ligt. Dat bedrijf heeft daar nog niet op gereageerd.

Five years later, Heartbleed vulnerability still unpatched

Posted: September 12, 2019 by Gilad Maayan
Last updated: July 31, 2020

The Heartbleed vulnerability was introduced into the OpenSSL crypto library in 2012. It was discovered and fixed in 2014, yet today—five years later—there are still unpatched systems.

This article will provide IT teams with the necessary information to decide whether or not to apply the Heartbleed vulnerability fix. However, we caution: The latter could leave your users' data exposed to future attacks.

What is the Heartbleed vulnerability?

Heartbleed is a code flaw in the OpenSSL cryptography library. This is what it looks like:

```
memcpy(bp, pl, payload);
```

In 2014, a vulnerability was found in OpenSSL, which is a popular cryptography library. OpenSSL provides developers with tools and resources for the implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

HO GENT

https://tweakers.net/nieuws/165340/zoom-liet-e-mailadressen-uitlekken.html
(Zoom heeft een slechte reputatie qua beveiliging)
https://heartbleed.com/
https://blog.malwarebytes.com/exploits-and-vulnerabilities/2019/09/everything-you-need-to-know-about-the-heartbleed-vulnerability/

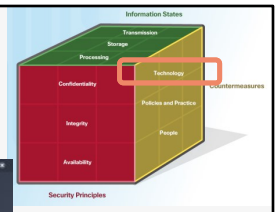
2.4 Beschermings-maatregelen

HO GENT

2.4 Beschermingsmaatregelen

Technologieën

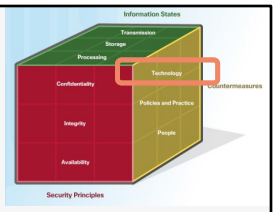
- Software-gebaseerd
  - Bv. Virusscanner of firewall op eigen laptop
- Hardware-gebaseerd
  - Bv. Firewall apparaat op het netwerk
- Netwerk-gebaseerd
  - Bv. Je moet je aanmelden om met een WiFi netwerk te verbinden



https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_900D.pdf

2.4 Beschermingsmaatregelen

Technologieën



- Cloud-gebaseerd
  - De beveiliging ligt nu bij de cloud-provider
  - Bv. MEGA, Dropbox, Google Drive, Onedrive, …
    - Is jouw data daar veilig?
      - Wat als zij gehacked worden?
    - Is jouw data dan nog van jou?
      - Wie kan er meelezen?

Users told to ditch OneDrive and Office 365 to avoid 'covert' data harvesting

Microsoft now faces sanctions as investigators claim the policy breaches GDPR

by: **Keumars Afifi-Sabet** 15 Nov 2018

Google admits it sent private videos in Google Photos to strangers

The privacy breach affected a small number of Google Photos users

2018 Google data breach

From Wikipedia, the free encyclopedia

The **2018 Google data breach** was a major scandal in late 2018 when Google engineers discovered a software leakage

Attackers can access Dropbox, Google Drive, OneDrive files without a user's password

The so-called "man-in-the-cloud" attack is said to be a common flaw in most cloud-based file synchronization servic

Google's student privacy policies called into question

Company policies for student data collection remain opaque despite lawsuits

by Kevin Forestieri / Mountain View Voice

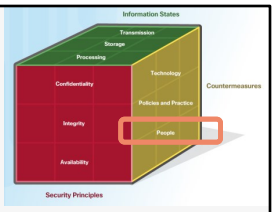
Uploaded: Fri, Feb 19, 2016, 12:42 pm
Time to read: about 10 minutes

Dropbox hack leads to leaking of 68m user passwords on the internet

Data stolen in 2012 breach, containing encrypted passwords and details of around two-thirds of cloud firm's customers, has been leaked

https://www.theverge.com/2020/2/4/21122044/google-photos-privacy-breach-takeout-data-video-strangers
https://www.zdnet.com/article/dropbox-google-drive-onedrive-files-man-cloud-attack/
https://en.wikipedia.org/wiki/2018_Google_data_breach
https://mv-voice.com/news/2016/02/19/googles-student-privacy-policies-called-into-question
https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach
https://www.itpro.co.uk/general-data-protection-regulation-gdpr/32372/users-told-to-ditch-onedrive-and-office-365-to-avoid

Opleidingen en training

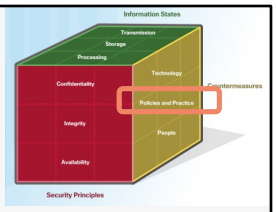


- Gebruikers hebben niet altijd slechte bedoelingen, maar weten soms niet beter
- Gebruikers kunnen op verschillende manieren bewust gemaakt worden van cybersecurity binnen een organisatie
  - Maak cybersecurity training een deel van het opleidingsproces voor nieuwe werknemers
  - Maak cybersecurity een onderdeel van de werkvereisten of evaluaties
  - Geef opleidingen aan werknemers
  - Biedt online cursussen aan
- Bewustmaking van cybersecurity is een steeds aanwezig proces, want er ontstaan continu nieuwe bedreigingen en technologieën

HO GENT

2.4 Beschermingsmaatregelen

Beleid en procedures



- Er bestaan verschillende standaarden, richtlijnen en procedures om een cybersecurity beleid uit te stippelen voor een organisatie
- Een cybersecurity beleid is een reeks van doelstellingen voor een organisatie dat gedragsregels, systeemvereisten voor soft- en hardware, … bepaalt voor gebruikers en administratoren
  - Bijvoorbeeld:
    - Iedereen moet om de 6 maand zijn paswoord veranderen
    - Netwerken worden beveiligd met een firewall apparaat
    - Elke account moet beveiligd worden met 2FA
    - Enkel administratoren hebben toegang tot de server ruimte
    - …

HO GENT

Extra:

- https://tweakers.net/nieuws/154330/medewerker-canadees-financieel-bedrijf-laat-data-2-komma-7-miljoen-mensen-uitlekken.html

2.5 Het ISO cybersecurity model

HO
GENT

Het ISO model

- Het beveiligen van data is een enorme taak. Het is onmogelijk voor een persoon om alles van begin tot einde te weten
- Het International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) hebben een volledig framework opgesteld om te helpen dit in goede banen te leiden. Dit framework noemt het ISO model
- Het ISO model is een hulpmiddel om complexe problemen te begrijpen en aan te pakken

HO GENT

Het ISO model

- Het ISO/IEC 27000 is een standaard opgesteld in 2005 (en geupdated in 2013). Het is gepubliceerd door ISO
- Alhoewel de standaard niet verplicht is, wordt het door veel landen en organisaties gebruikt als het model voor cybersecurity

HO GENT

Het ISO model gebruiken

- Het ISO 27000 model is bruikbaar voor elk type organisatie en bevat controle doelstellingen in de vorm van een checklist.
- De organisatie moet bepalen welk van deze controle doelstellingen op de organisatie van toepassing zijn

ISO/IEC 27002 Section	Primary Objective		
	Confidentiality	Integrity	Availability
5			
5.1			
5.1.1	√	√	√
5.1.2	√	√	√
6			
6.1			
6.1.1	√	√	√
6.1.2		√	√
6.1.3			√
6.1.4	√		√
6.1.5	√		
6.1.6	√	√	√
6.1.7	√	√	√
6.1.8	√	√	√

HO GENT


HO
GENT