Cheat Sheet / Samenvatting

Cassandra.exe



De samenvatting van het theatercollege Cassandra.exe van Bernold Nieuwesteeg

Laatste informatie:
https://www.bernoldnieuwesteeg.nl/

N.B. Dit is de samenvatting van de volledige voorstelling Cassandra.exe. Het kan zijn dat je een deel van de voorstelling hebt gezien, bijvoorbeeld op een zakelijk event. Details op https://www.bernoldnieuwesteeg.nl/show.

De belofte van het Internet

Nederland werd op 17 november 1988 als eerste land in Europa op het internet aangesloten.[1]



En het begon als een prachtige belofte:

- Veiligheid: we hoefden niet meer met cash geld over straat
- Minder afhankelijk: van post en fax
- En het belangrijkste van alles: ongekende productiviteit

Kortom: een beter leven voor iedereen omdat we allemaal verbonden zijn.

1 https://www.cwi.nl/nl/nieuws/nederland-35-jaar-geleden-als-eerste-in-europa-op-het-publieke-internet/

AI

En toen kwam AI op 30 november 2022 (althans, toen werd ChatGPT gereleased). Iedereen voelde wel het initiële enthousiasme bij het kennismaken met AI (LLMs).

Wel zijn er een paar nadelen verbonden aan AI.

- Als ik zie hoeveel kolencentrales ervoor nodig zijn, denk ik aij energietransitie
- Als ik zie dat we ons afhankelijker maken van Amerika, denk ik aij autonomie
- Als ik zie hoe AI werk van juniors overneemt, denk ik aij management trainee
- Als ik zie hoe mensen ChatGPT vragen op welke politieke partij ze moeten stemmen denk ik aij democratie.
- Als ik zie hoe AI gebruikt wordt om een openingszin te genereren in een datingapp denk ik aij liefdeschemie.
- Als ik zie hoe we ons denken uitbesteden, denk ik, aij, intelligentie
- Als ik zie hoe AI er losgeslagen op loshackt dan denk ik aij, cybersecurity.

Maar, moeten we dat nadeel voor lief nemen omdat AI onze arbeidsproductiviteit een ongekende boost gaat geven?

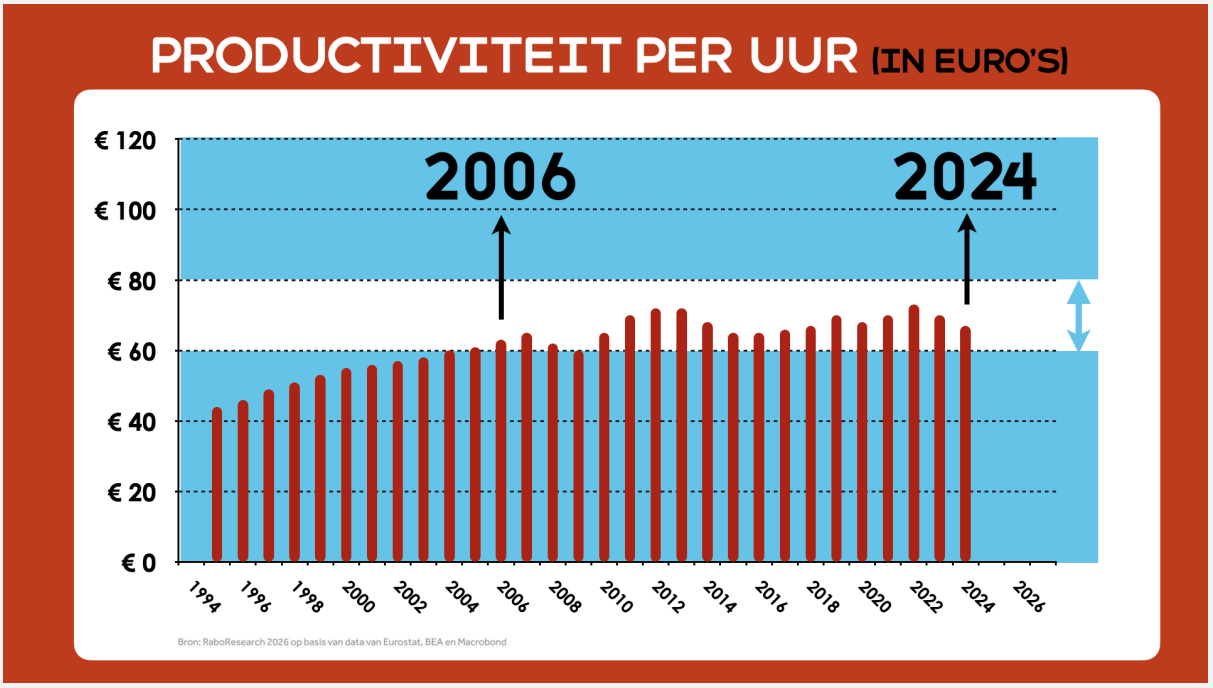
De Gaston Paradox - de productiviteitsparadox.

Als iedereen een extra LinkedIn-post kan schrijven dankzij AI halveert de impact per post. Je moet die extra post wel schrijven om je impact te behouden. En je kan denken, ik doe niet mee, maar dan ga je achteruit.

Dit is de productiviteitsparadox. Ik noem het de Gaston Paradox.



De afgelopen 20 jaar stijgt de arbeidsproductiviteit nauwelijks.[2]



Dus we moeten steeds harder rennen, om op dezelfde plek te blijven.

2 https://www.cbs.nl/nl-nl/nieuws/2024/32/arbeidsproductiviteit-neemt-steeds-minder-toe-in-afgelopen-50-jaar

Cybersecurity in het AI-tijdperk

Het is maar zeer de vraag of AI wel de arbeidsproductiviteit gaat doen stijgen, juist door bijvoorbeeld cyberrisico's van agents die de arbeidsproductiviteit weer tenietdoen. Zoals het McKinsey-voorbeeld laat zien:

Voorbeeld McKinsey:

- Recent wist een ethisch hacker binnen te dringen bij McKinsey. Hij kon de AI Agents van McKinsey hacken. Een AI-agent is een autonoom systeem dat beslissingen kan nemen en acties kan uitvoeren.
- McKinsey kon er niet langer zeker van zijn dat de agents wel de juiste dingen hadden gedaan.
- Als je dat niet meer kan zeggen, dan zijn al die rapporten ook niets meer waard
- Is dat productiviteitswinst?

Statelijke actoren - hybride oorlogsvoering

Maersk Case:

- In 2017 werd Maersk, het grootste containerbedrijf ter wereld, getroffen door een verwoestende cyberaanval.[3]
- De aanval kwam vanuit Rusland. Het was onderdeel van de hybride oorlogsvoering tussen Rusland en Oekraïne.
- De Russische Geheime Dienst had de aanval verstopt in een update van het boekhoudprogramma ME-DOC.
- Dit boekhoudprogramma werd veel gebruikt in Oekraïne, maar ook gebruikt door Maersk.

Lessen:

[3] http://phishingforanswers.com/blog/how-ghana-saved-a-conglomerate-from-cyberattack , https://www.controleng.com/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/ , https://sosintel.co.uk/case-study-maersks-response-to-notpetya-how-cybersecurity-best-practices-mitigated-a-major-cyberattack/



- Cybersecuritymaatregelen, zoals het segmenteren van je digitale omgeving (net als de waterdichte schotten in de Titanic) kosten geld, maar kunnen een veelvoud aan schade voorkomen. Ook in een AI-tijdperk. Als McKinsey schotten had aangebracht tussen de Agents, waren ze niet allemaal tegelijk gehackt.
- De digitale dreiging was bij Maersk geen *chefsache*, en dat is het bij veel bedrijven nu ook nog niet het geval. → hier vertel ik meer over in CyberSecurityBooster #37 en #47[4].
- Cybersecurityprofessional zijn is een ondankbaar beroep, als je het heel erg goed doet, gebeurt er niets. Geef de cybersecurityprofessionals in je organisatie dus een schouderklopje.

Cybercrime als businessmodel

In de training "Hoe word ik een cybercrimineel" leerde ik je hoe je een cybercrimineel wordt en hoe het businessmodel van een cybercrimineel werkt.

[4] Zie de bibliotheek aan boostersessies op https://www.cybersecuritybooster.nl/



Tips als je ransomware gaat plaatsen:

1. Benader je slachtoffers als klant
2. Heel belangrijk: vraag om geld
3. Zorg voor een anonieme manier om het geld over te maken, via een bitcoin wallet.

En dan denk je misschien, heb ik technische kennis nodig? Sommige ransomware kan je gewoon op het dark web kopen.

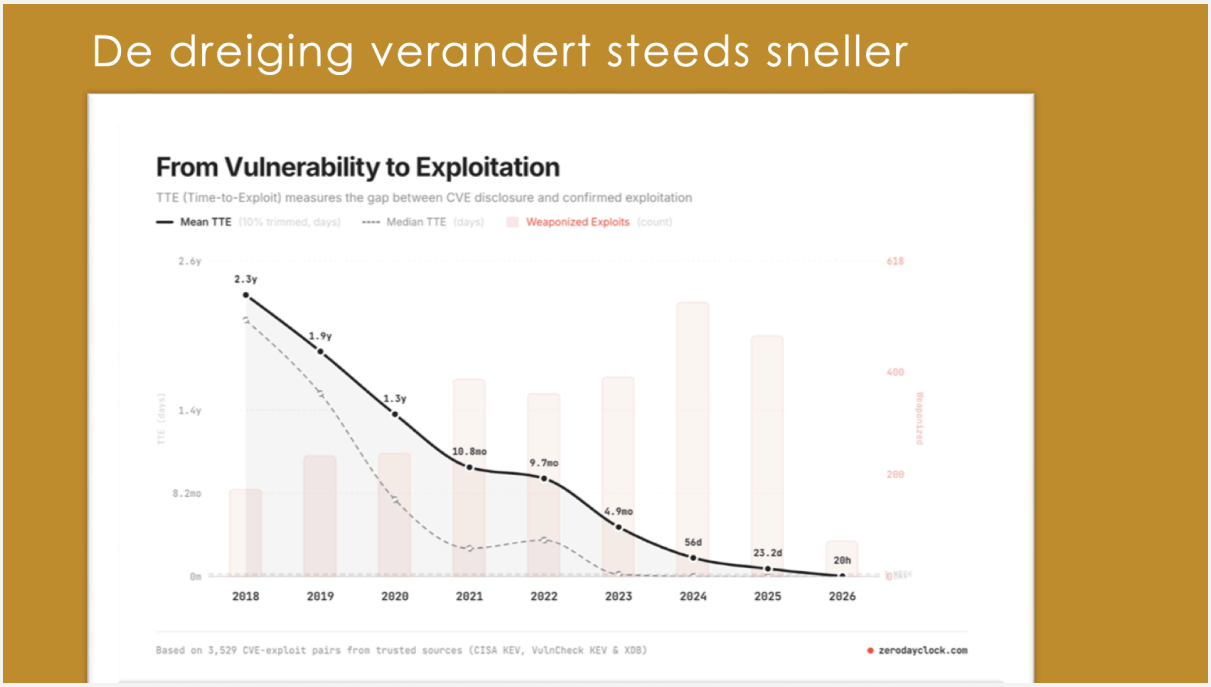


Dit is meteen het lastigste, cyberdreigingen veranderen, in tegenstelling tot veel andere risico's, voortdurend. Door AI gaat dit nu veel sneller.

Samenvattend. We hebben twee dingen geleerd over cybersecurity in relatie tot AI.

1. De basis op orde is nog steeds belangrijk (voorbeeld van netwerksegmentatie, zoals de Titanic, als McKinsey dat had toegepast dan waren niet alle agents in 1 keer gehackt)

2. De dreigingen veranderen steeds sneller door AI



Hierboven zie je een grafiek die feitelijk aangeeft dat er nauwelijks nog tijd zit tussen het ontdekken van een kwetsbaarheid en het misbruiken ervan. Dat betekent voor jou persoonlijk het volgende:

1. Zorg dat je je basis op orde hebt. En daar versta ik in ieder geval onder: een passwordmanager gebruiken (bijv. Proton pass, dat is Europees), je scherm locken, 2-factorauthenticatie aanzetten op je belangrijke accounts en een back-up niet verbonden met het Internet hebben. En maak een cyberplan voor als je er niet meer bent of niet meer toerekeningsvatbaar bent.

2. Blijf op de hoogte van de dreigingen via theatercolleges als deze, onafhankelijke nieuwsbronnen en school je bij. Via de maandelijkse webinar CyberSecurityBooster nodig ik je uit om als je vragen hebt ze te stellen. Elke maand hebben we op een dinsdag een live-sessie.

Digitale autonomie in het AI-tijdperk



Onze digitale afhankelijkheid is te vergelijken met een loverboyrelatie:

- We krijgen eerst allemaal cadeautjes: goedkope softwarelicenties, het eerste jaar gratis. (ook bijvoorbeeld de schijnbaar goedkope diensten, onder de kostprijs, van Amerikaanse AI-aanbieders zoals OpenAI en Anthropic)
- Dan worden we met valse liefde ingepalmd: de liefde voor gemak en efficiëntie.
- En daarna worden we uitgebuit: de prijzen worden verhoogd en onze afhankelijkheid wordt ingezet als geopolitiek drukmiddel.

Trump kan met 1 knop (bij wijze van spreken, die knop is er niet echt hè) Microsoft bevelen om de Nederlandse overheid uit te zetten.

- De Nederlandse overheid zit voor bijna 100% in Microsoft.
- Dat betekent dat bijna alle communicatie en data-opslag van de Nederlandse overheid via Microsoft gaat.
- En nu gebruiken we ook weer AI van diezelfde Amerikanen, en worden er weer cadeautjes uitgedeeld om je verslaafd te maken. Het zakelijke basisabonnement van Anthropic weerspiegelt bijvoorbeeld totaal niet de werkelijke kosten.

Samenvatting: we hebben o.a. door onze focus op cyberveiligheid en onze liefde voor efficiëntie en gemak een nieuwe enorme afhankelijkheid gecreëerd. Het leek veiliger om naar Microsoft-cloud te gaan, dan hoeft er bijvoorbeeld geen datacenter meer in de gemeente Ommen te staan dat in de fik kan gaan. En nu gebeurt het weer met AI.

Hoe komen we hier uit?

- Inkoop. Amerikaanse partijen zijn vaak eerst goedkoper en kunnen daarna hun prijzen verhogen. Geef Europese bedrijven voorrang bij inkoop.
- Investeringen. Europa betaalt jaarlijks meer dan 265 miljard euro aan Amerikaanse Big Tech, dat is het bbp van Portugal.[5] Investeer meer in Europese tech.
- Mythe. Amerikanen zijn goed in marketing. Maar dat kunnen wij ook. Wij kunnen onze eigen mythe creëren.

En wat kan je persoonlijk doen?

- Gebruik eens de Europese ChatGPT: Vibe van Mistral. Dat is ongeveer de ChatGPT van 6 maanden geleden
- Gebruik een Europese back-up voor je foto's, bijvoorbeeld Jottacloud.
- Bij nieuwe tech: gebruik gelijk een Europees alternatief, dan hoef je niet over te stappen. Bekijk https://european-alternatives.eu/bijvoorbeeld.

[5] https://www.ictmagazine.nl/blogs/europa-betaalt-265-miljard-euro-voor-digitale-afhankelijkheid/

Intelligentie in het AI-tijdperk

Als we met AI ons denken uitbesteden, moeten we ons denken actief gaan trainen. Net als dat we in de jaren 50 massaal naar de sportschool gingen omdat we allemaal in de auto konden stappen. Steve Jobs, de oprichter van Apple, de uitvinder van de iPhone, gaf zijn eigen kinderen geen iPhone of iPad. Hij was zich bewust van technologie als geen ander, dus wat voor tips zou hij geven over AI?

Advies van Steve Jobs in het AI-tijdperk

Richt je op activiteiten met een hoge ROI: een hoge Return on Intelligence. [6]

Vier tips van Steve:[7]

1. Lees elke dag
2. Blijf zelf dingen opschrijven
3. Maak een wandeling en concentreer je op 1 gedachte
4. Leer iets moeilijks

Kortom: we lopen met AI het risico dat we onveiliger, afhankelijker en dommer worden. Als we ons bewust zijn, kunnen we dat risico voor onszelf en de samenleving verkleinen.

[6] https://www.nytimes.com/2026/03/27/opinion/technology-mental-fitness-cognitive.html
[7] Tips zijn eigenlijk van Cal Newport

De ontsnappingsroute → toch productiever in een digitale wereld?

De Roosevelt Regel. Minder = meer



Kies sneller voor "goed genoeg". Dat scheelt heel veel tijd. Maar dat is moeilijk, want de drempel om een revisie te doen is door digitalisering en AI enorm verlaagd.

Als er al productiviteitswinst is door AI, dan wordt die volkomen teniet gedaan door te veel revisies, prompts en door AI-gegenereerde opties die leiden tot verlamming (Brain Fry).[8] De gemiddelde Microsoft-gebruiker verwerkt 117 e-mails per dag met een gemiddelde concentratietijd van slechts 2 minuten.[9]

Dus de Roosevelt Regel, minder = meer!

Minder revisies
Minder gefrituurde breinen
Minder mails
Minder afleiding

Daarvoor moet je je wel beheersen.

Dus mijn advies, wil je een productieve arbeider zijn in het AI-tijdperk: “doe elke dag een beetje minder”

[8] https://hbr.org/2026/03/when-using-ai-leads-to-brain-fry
[9] https://www.microsoft.com/en-us/worklab/work-trend-index/breaking-down-infinite-workday