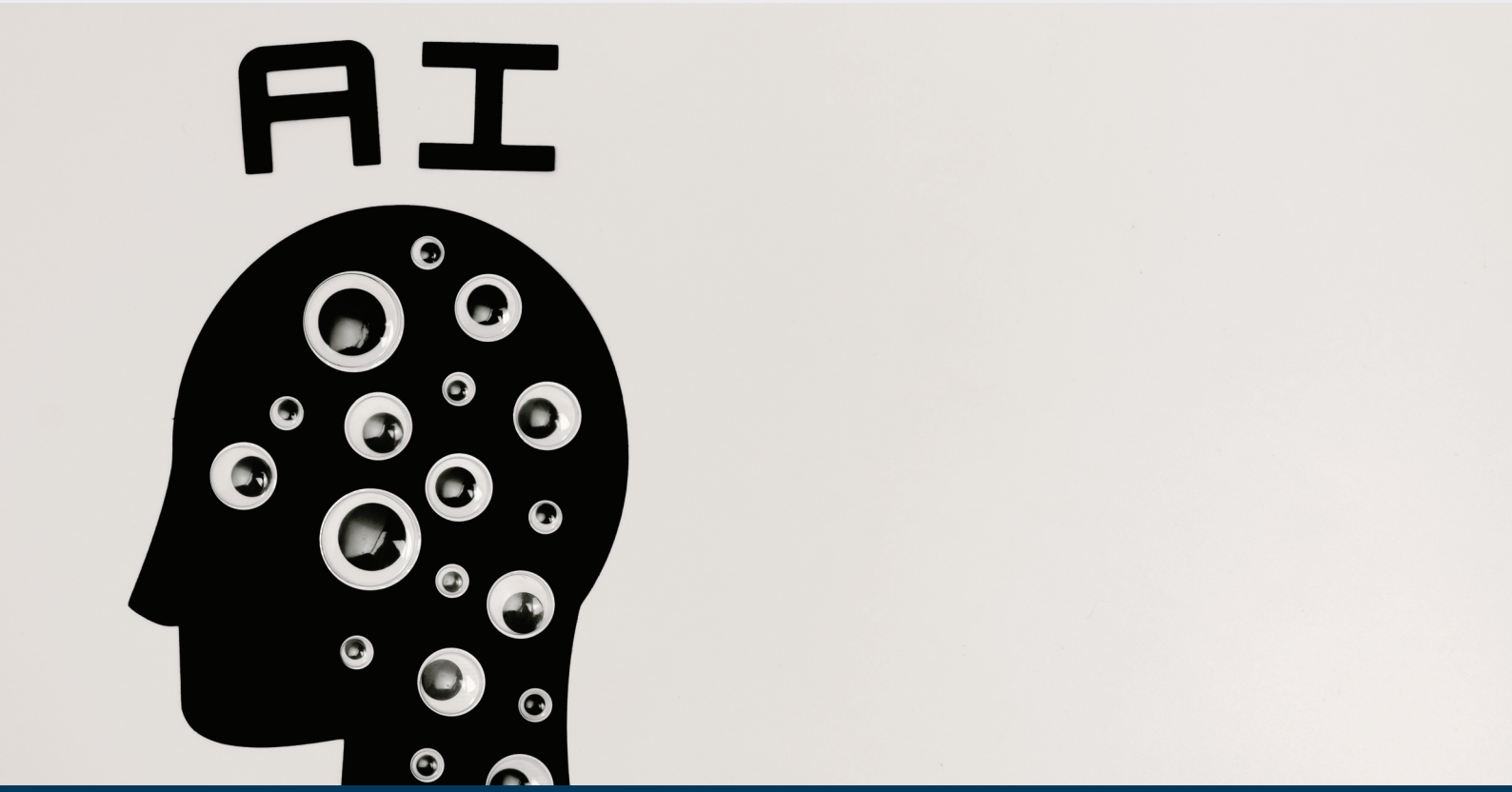
In deze rubriek geven enkele iB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.



Artificial Intelligence een nieuwe bedreiging?

Kunstmatige intelligentie, algoritmen en andere manieren om van ruwe data nuttige informatie te maken, winnen steeds meer terrein. Menig organisatie werkt met Business Intelligence afdelingen en/of werkt steeds meer data gedreven. Dat geldt niet alleen voor organisaties, maar ook voor (digitale) criminelen. Moeten wij als informatiebeveiligers ons zorgen maken? Een reflectie van een deel van de redactie.

In oktober 2021 was in het nieuws dat bij een bankroof in de Verenigde Arabische Emiraten gebruik gemaakt is van AI om de stem van de bankdirecteur na te maken (1). In de basis is dit voorbeeld natuurlijk een vorm van CEO-fraude, maar er zijn natuurlijk andere dreigingen die voortkomen uit meer en meer AI. Zo kunnen algoritmes kritisch worden voor de bedrijfsvoering (beschikbaarheid) of is de gewenste werking van algoritmen of termijn niet meer te achterhalen (integriteit).

Samen slimmer - Lilian Knippenberg

Digitalisering gaat harder dan ooit en onze organisaties werken meer en meer op data of zelfs alleen maar op data. In de basis

Chris de Vries | Fook Hwa Tan | Lilian Knippenberg

denk ik dat alle digitale ontwikkelingen steeds terug te voeren zijn op bekende dreigingen, zoals de genoemde CEO-fraude. Het probleem met de snelle doorontwikkeling van technieken is alleen dat de digitale producten die je onder ogen krijgt voor gemiddelde mensen niet meer van echt te onderscheiden zijn. We moeten dus gezamenlijk toe naar meer bewustzijn en veiligheidsprocedures: MFA in techniek én in procedures. Spreek af dat je die CEO terugbelt op het jouw bekende nummer in plaats van het nummer waar hij je belde. Zorg voor het 'meer ogen'-principe. Daarnaast zijn algoritmen natuurlijk net zo goed 'systemen' die een classificatie moeten krijgen op B, I en V. Qua integriteit hoop ik eigenlijk op een soortgelijke actie als bij de ontwikkeling van aparte ontwikkeling (Dev) en operatie (Ops) van systemen naar één team dat beiden doet (DevOps) en daarna naar een veilige variant daarvan (DevSecOps) waar de ontwikkelaars en beheerders samen invulling geven aan security by design en by default. Ik introduceer dus alvast bij deze de Artificial Secure Intelligence (Asecl). Met het ontzettend wijdverbreide gebruik van AI worden we daar allemaal slimmer van!

Menselijke toets achteraf - Chris de Vries

Artifical Intelligence (AI) oftewel in goed Nederlands 'Kunstmatige Intelligentie' is "de natuurlijk domme poging van slimme wetenschappers om menselijke intelligentie in een computer na te bootsen." (2) Ik voel wel wat voor deze definitie, want er zijn heel wat slimme mensen die ooit eens over Frederick Winslow Taylor's wetenschappelijke bedrijfsvoering hebben gelezen en daarbij de 'time & motion studies' als basis voor efficiëntie hebben leren kennen. De mens is altijd bezig om iets uit te vinden dat efficiënter is en minder werk van hemzelf vergt.

Et voila, de geboorte van de 'black box'. In een set van programmatuur wordt het besluitvormingsproces vormgegeven en vervolgens hoeft de mens zelf niet meer te beslissen. Voorbeelden uit de praktijk: 'De Bazel I t/m 3' besluiten (bankwezen) en de toeslagenaffaire (de belastingdienst c.q. de overheid).

In het eerste geval is voorgeschreven hoe banken hun vermogen op peil moeten houden en hoe risico's onderkend, geanalyseerd en beheerst worden. Op zich een lovenswaardig streven, maar in ons land leidde het er wel toe dat het MKB niet financierbaar is geworden. De toeslagenaffaire: een affreus gebeuren dat met de dag meer schandalige gevolgen laat zien en nog steeds niet goed opgepakt wordt. Laat staan dat de verantwoordelijkheid wordt genomen.
Beide zaken zijn 'black boxes' gebaseerd op efficiëntie, perfect werkende computers en verworpen menselijkheid. Artificial Intelligence heeft de toekomst, maar ik vrees bij blinde toepassing voor de mensheid.Ik onderschrijf dus de stelling van mijn mede-redactielid Lilian dat, Artificial Secure Intelligence een moeten is, maar dan moet Secure ook neerkomen op de altijd noodzakelijke menselijke toets achteraf of in het voorkomende geval het mogelijk maken van aantekening geen bezwaar.

Ingehaald door technologie - Fook Hwa Tan

We zien in ons dagelijks leven steeds meer gebruik van AI, ML en in het algemeen algoritmen, zoals in wasmachines, waterkokers of rijstkokers. Maar het geldt natuurlijk ook voor het laten zien van advertenties of ander personaliseringssoftware. Het begon met regels die werden geautomatiseerd, inmiddels heb je beslisbomen die een computer kunnen volgen om tot beslissingen te komen. En natuurlijk heb je de getrainde neurale netwerken die uit data gedrag kunnen destilleren om deze vervolgens te emuleren. Met de nieuwe generatie AI kunnen steeds complexere acties en besluiten worden genomen.
Computers voeren steeds snellere calculaties uit. Hierdoor kunnen steeds kleinere apparaten steeds meer besluiten van mensen overnemen. Met kwantumtechnologie en meer nieuwe technologieën zijn er nóg meer mogelijkheden beschikbaar voor ons om in te zetten.

We zien dus, dat technologie zorgt voor complexiteit en snelheid in nog meer toepassingen. Het gaat inmiddels zo snel, dat wij als mensen niet meer begrijpen wat onze machines doen. We zien dit al bij algoritmes die door onze overheid gebruikt worden om fraude op te sporen of verdachte gevallen te identificeren. Hoe kunnen we bijblijven met technologie als informatiebeveiligers? Het lijkt soms alsof we worden ingehaald door technologie. We moeten dus zorgen dat we qua kennis bijblijven en op de hoogte zijn van alle ontwikkelingen. Als wij de kennis niet najagen, zullen criminelen het wel doen!

(1) https://tweakers.net/nieuws/188220/criminelen-gebruiken-ai-namaakstem-bij-bankroof-van-ruim-30-miljoen-euro.html
(2) Computable, ICT Woordenboek 2003.