Crypto en blockchain: juridische toepassingen en ontwikkelingen

5 juli 2022

dr. Niels Vandezande

NCOI M&D Seminars TIMELEX

1

Overzicht

1. Crypto onder de nieuwe Belgische antiwitwaswetgeving
2. Europese ontwikkeling: Digital Finance Package - Markten in Crypto-Activa en proeftuin voor blockchain marktinfrastructuren
3. Meer dan alleen crypto: blockchain en smart contracten
4. NFT's: volgende evolutie of volgende hype?
5. Digital Operational Resilience Act (DORA) voor de financiële sector
6. Network and Information Security Directive II

2

Crypto onder de nieuwe Belgische antiwitwaswetgeving

3

Europese ontwikkeling: AMLD5

- 2012-2014: herziening derde richtlijn, voorstel vierde richtlijn
  - EBA wou sterke antiwitwasregels voor cryptogeld, Frankrijk riep na aanslag op Charlie Hebdo op tot het aanpakken van risico's van cryptogeld, wat werd bevestigd in een gezamenlijke declaratie van de Europese Raad en Commissie
- Mei 2015: Vierde richtlijn: geen vermelding van cryptogeld
- Juli 2016: voorstel tot aanpassing vierde richtlijn
  - Tegen **anonimiteit van cryptogeld**
  - Voegt **Crypto-dienstenaanbieders** toe als **meldingsplichtige entiteiten**
  - Amendementen aangenomen in mei 2018: Richtlijn 2018/843, om te zetten tegen 10 januari 2020

4

Europese ontwikkeling: AMLD5

- Virtuele valuta
  - *"een digitale weergave van waarde die niet door een centrale bank of een overheid wordt uitgegeven of gegarandeerd, die niet noodzakelijk aan een wettelijk vastgestelde valuta is gekoppeld en die niet de juridische status van valuta of geld heeft, maar die door natuurlijke of rechtspersonen als ruilmiddel wordt aanvaard en die elektronisch kan worden overgedragen, opgeslagen en verhandeld"*
  - Beperking in overweging
- Aanbieders van diensten voor het wisselen tussen virtuele valuta en fiduciaire valuta
- Aanbieders van bewaarportemonnees

NCOI M&D Seminars

5

AMLD5 in België: Wet van 20 juli 2020

- Vrijwel letterlijke omzetting
- Geen preciseringen
- Registratie crypto-diensten bij FSMA
- Uitwerking via KB

NCOI M&D Seminars

6

AMLD5 in België: Wet van 1 februari 2022

- Bijkomende definitie: diensten voor het wisselen tussen virtuele valuta en fiduciaire valuta = diensten die bestaan uit aan- of verkoopverrichtingen, met eigen kapitaal, waarbij virtuele valuta gewisseld worden voor fiduciaire valuta of fiduciaire valuta voor virtuele valuta
- 3 types
  - Gevestigd in BE, bijkantoor in BE, of elektronische infrastructuren (vb. ATM) in BE = BE-wet van toepassing
  - Gevestigd elders in EU = recht van dat land van toepassing
  - Gevestigd buiten EU = verboden diensten in BE aan te bieden **(!)**

7

AMLD5 in België: Wet van 1 februari 2022

- KB regelt inschrijving, “voorwaarden voor uitoefening van activiteiten”
  - Registratie versus vergunning? Zie Bitonic in NL
- Effectieve leiding: noodzakelijke professionele betrouwbaarheid en de passende deskundigheid ➔ geen inschrijving indien wie >5% deelneming heeft of controle uitoefent niet aan voorwaarden voldoet
- FSMA houdt publiek register bij met identificatiegegevens van ingeschrevenen
- Straf: gevangenisstraf van een maand tot een jaar en met een geldboete van 50 tot 10 000 euro, of met één van die straffen alleen

8

AMLD5 in België: KB van 8 februari 2022

- Dossier indienen bij FSMA, beslissing binnen 3 maanden
- Kost: EUR 8.000 per inschrijving + jaarlijkse kost EUR 8.000/inschrijving
- Vereiste vennootschapsvorm: CV, NV of EU-versie, hoofdbestuur in BE
- Startkapitaal van EUR 50.000
- Effectieve leiding: natuurlijke personen, controle op geschiktheid
- Identificatie van leidinggevenden, controle, deelneming >5%
- Reclame maken met inschrijving verboden!
- Wijziging in leiding of deelneming moeten worden gemeld
- Sancties: FSMA kan uitoefening verbieden of inschrijving schrappen
- Tijdelijke inschrijving als overgang voor bestaande aanbieders

DAC8

- Directive on Administrative Cooperation (v8)
  - Doel: samenwerking tussen autoriteiten om fiscale transparantie te verbeteren
  - Uitgevers van crypto-activa en dienstenleveranciers moeten informatie vrijgeven om correcte en eerlijke belasting mogelijk te maken
- DAC8 en crypto
  - Veel gebruikers houden winsten op exchanges of zetten deze om in stablecoins
  - Aangifte voor meerwaardebelasting gebeurt doorgaans pas bij re-introductie in traditioneel system (overschrijving naar bankrekening)
  - DAC8 wil dit tegengaan: medewerkingsplicht dienstenleveranciers om de fiscus te laten nagaan waar meerwaarden werden gerealiseerd
- In voorbereiding

Europese ontwikkeling: Digital Finance Package – Markten in Crypto-Activa en proeftuin voor blockchain marktinfrastructuren

11

NCOI M&D Seminars

11

Digital Finance Package

- Nieuw initiatief van de Europese Commissie
- Ondersteuning van de digitale markt
  - Waaronder blockchain (of DLT) en AI
- Regulering markten in crypto-activa
  - Central bank digital currencies uitgesloten
- Proefproject voor DLT-markinfrastructuren

12

NCOI M&D Seminars

12

Regulering markten in crypto-activa

- Bescherming van belegger en de markt
- Zowel betaal-coins als investerings-coins

- Personeel toepassingsgebied: personen die zich bezighouden met de uitgifte van crypto-assets of die diensten verlenen in verband met crypto-assets in de Unie
- -> tenzij ze reeds onder ander kader vallen (MiFID, EMD, …)

Regulering markten in crypto-activa

- **Crypto-activa**: "*digitale weergave van waarde of rechten die elektronisch kan worden overgedragen en opgeslagen, met gebruikmaking van Distributed Ledger Technology of vergelijkbare technologie*".
  - Inclusief utility tokens
- **Asset-referenced tokens**: "*een type cryptoactiva dat een stabiele waarde tracht te behouden door te verwijzen naar de waarde van diverse fiduciaire valuta die een wettig betaalmiddel zijn, één of meer grondstoffen, of één of meer cryptoactiva, of een combinatie van dergelijke activa*".
  - Stablecoins
- **Elektronisch geld-token**: speciale soort crypto-asset "*met als hoofddoel het gebruik als ruilmiddel en dat een stabiele waarde tracht te behouden door te verwijzen naar de waarde van een fiduciaire valuta die een wettig betaalmiddel is*".

Regulering markten in crypto-activa

- "*een aanbod aan derden om een crypto-asset te verwerven in ruil voor fiatvaluta of andere crypto-assets*"
- Diensten:
  - bewaring en het beheer ervan voor rekening van derden,
  - exploitatie van een handelsplatform voor crypto-assets,
  - omwisselen van crypto-assets voor fiatvaluta die wettig betaalmiddel zijn,
  - omwisselen van crypto-assets voor andere crypto-assets,
  - uitvoering van orders voor crypto-assets voor rekening van derden,
  - plaatsen van crypto-assets,
  - ontvangen en doorgeven van orders voor crypto-assets namens derden,
  - verstrekken van advies over crypto-assets

Regulering markten in crypto-activa

- Crypto-activa
  - Publicatie witboek
    - Inhoud: omschrijving crypto, emittent, aanbod, risico's, …
    - geen voorafgaande goedkeuring regulator, wel notificatie
      - Wel mogelijkheid regulator om extra informatie te bevelen
    - Uitzonderingen:
      - Indien crypto gratis aangeboden (en ook niet tegen alternatieve voorwaarden)
      - Indien automatische creatie als beloning voor miners
      - Indien non-fungible
      - Aanbod aan minder dan 150 personen, of tegenwaarde <1M, of gekwalificeerde beleggers
  - Uitgever moet rechtspersoon zijn, is aansprakelijk
  - Eerlijke en niet-misleidende reclame
  - Consument heeft herroepingsrecht van 14 dagen

Regulering markten in crypto-activa

- Asset-referenced tokens
  - Vergunningsplicht
    - Statutaire zetel in EU
    - Uitzondering: gekwalificeerde beleggers of tegenwaarde <5M, kredietinstellingen
    - Vergunning geeft EU-paspoort
    - Vereisten vergelijkbaar met bestaande vergunningen onder EMD2, PSD2, MiFID2
    - Vergunning kan worden ingetrokken
  - Publicatie witboek
    - Moet *wel* goedgekeurd worden door regulator, onderdeel van vergunningsaanvraag
    - Ook omschrijving activa-reserves
  - Moet voorzien in klachtenprocedure

NCOI M&D Seminars

17

Regulering markten in crypto-activa

- Asset-referenced tokens
  - Operationele vereisten
    - Voorkomen van belangenconflicten
    - Governanceregels
    - Leidinggevenden zijn fit & proper
    - Verplichting tot houden activareserve per token, beperkte mogelijkheid tot beleggen, regels voor rechten tokenhouders, renteverbod
    - Beleid inzake stabilisatie
    - Eigen vermogen minstens het hoogste van 350.000 EUR of 2% van gemiddelde reserveactiva
  - Regels inzake overname/gekwalificeerde deelneming
  - Significante tokens:
    - Grootte van marktkapitalisatie (>1 miljard), gebruikers, transacties
    - Onder toezicht van de EBA, strengere regels

NCOI M&D Seminars

18

Regulering markten in crypto-activa

- E-geld tokens
  - Vallen onder EMD2 -> licentie als EMI vereist
    - Uitzondering: gekwalificeerde beleggers, <5M tegenwaarde
  - Publicatie witboek (kennisgeving regulator)
  - Houders hebben claim op uitgever
    - Uitgifte tegen nominale waarde en in ruil voor ontvangen middelen
    - Terugbetaalbaarheid
    - Renteverbod
  - Significante e-geld tokens: onder toezicht EBA, strengere voorwaarden

Regulering markten in crypto-activa

- Crypto-activa dienstverleners
  - Vergunningsplicht (met paspoort)
    - statutaire zetel in EU
    - Vereisten vergelijkbaar met MiFID2
    - Fit & proper
    - Scheiding van crypto en gelden van cliënten
  - Eerlijk handelen (inclusief informatie en reclame)
  - Kapitaal: ten minste het hogere van het in bijlage IV vermelde bedrag (tussen 50k en 150k) of een kwart van de vaste kosten van het voorgaande jaar, jaarlijks te herzien
    - Via eigen vermogen of verzekeringspolis
  - Beveiliging van bewaarde crypto en gelden
  - Klachtenprocedure
  - Regels voor uitbesteding

Regulering markten in crypto-activa

- Specifieke regels naargelang soort dienst
  - Bewaring: minimumvereisten overeenkomst met cliënt, intern toegangsbeleid, positieregister, scheiding van middelen, aansprakelijkheid
  - Handelsplatform: exploitatieregels, due diligence, niet zelf op eigen platform handelen, operationele veerkracht, koersinformatie, back-up plan
  - Omwisseling: niet-discriminerend beleid, koerspublicatie
  - Orders: best result, orderuitvoeringsbeleid
  - Plaatsing: informatieplicht, regeling belangenconflicten
  - Doorgifte van orders: correcte doorgifte, geen affiliate-benefits, geen misbruik van informatie
  - Advies: afgestemd op cliënt, kennis, cliëntbeoordeling, risicowaarschuwing, verslag
- Overnameregels

Regulering markten in crypto-activa

- Regels tegen marktmisbruik
  - Regels inzake voorwetenschap
  - Verbod op marktmanipulatie
- Toezicht: nationale autoriteiten, EBA, ESMA
  - Uitgebreide actiemogelijkheden, onderzoeksbevoegdheden, etc.
  - Samenwerkingsplicht, onderling en met EBA/ESMA
  - Significante spelers: college van toezicht onder leiding van EBA
  - Bestuurlijke sancties
    - Boetes van minstens 5M of 3% jaaromzet, kan oplopen tot 15M of 15% jaaromzet
    - Bescherming van klokkenluiders
    - Significante spelers: EBA kan ook dwangsommen en boetes opleggen

Proefproject voor DLT-marktinfrastructuren

- Doel: DLT-MTF of effectenafwikkeling via DLT mogelijk maken
  - DLT-MTF: mag enkel in DLT-effecten handelen
  - DLT-CSD: centrale effectenbewaarinstelling die afwikkeling via DLT doet
- In principe algemene regels MiFID van toepassing
  - Vergunning als MTF of CSD nodig + bijkomende vergunning DLT-versie
- Bijkomende regels
  - Beperking effecten <200M kapitalisatie, <500M obligaties
  - Maximale marktwaarde DLT-effecten: 2,5 miljard
  - Aantonen nodige IT-kennis en infrastructuur te hebben, maatregelen cyberrisico's
- Proefproject: vergunning in principe voor 6 jaar, evaluatie door Commissie achteraf

NCOI M&D Seminars

Meer dan alleen crypto: blockchain en smart contracten

NCOI M&D Seminars

Smart contracten?

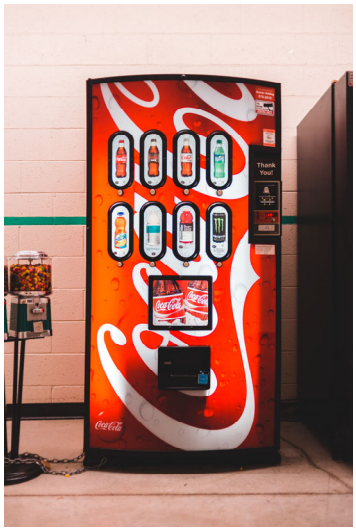

Photo by Erik Mclean on Unsplash

25

Smart contracten

- Blockchain laat toe applicaties te ontwikkelen (vb. Dapps op Ethereum)
- In eigen scripting taal
- Kunnen zelf-uitvoerend zijn (geen nood aan tussenpersonen)
- Kunnen ook gebruikt worden om contracten af te sluiten
  - vb. Koopovereenkomst, stemsysteem, veiling

26

26

Dapps

		CATEGORY	BALANCE	USERS	VOLUME	ACTIVITY
1	**Alien Worlds** WAX · BNB Chain	Games	$1.26k	213.81k -0.01%	$3.28k	
2	**PancakeSwap** BNB Chain	DeFi	$80M	198.52k -9.16%	$71.78M	
3	**Farmers World** WAX	Games	$6.89k	140.26k -1.20%	$23.96	
4	**Splinterlands** Hive · WAX	Games	$132.95k	128.26k -24.90%	$2.9k	
5	**Orca** Solana	DeFi	$123.18k	63.32k -28.42%	$21.56k	
6	**AtomicAssets** WAX · EOS	Other	$74.66k	54.08k +10.51%	$12.97k	
7	**GoodDollar** ETH · Fuse	DeFi	$77.86k	44.22k -1.63%	$68.15	
8	**Upland** EOS	Games	$22.4k	41.09k -4.97%	$0	
9	**Magic Eden** Solana	Marketplaces	$30.32k	36.17k +8.20%	$9.62M	
10	**Axie Infinity** Ronin · ETH	Games	$556.7M	35.01k -19.70%	$1.79M	

NCOI M&D Seminars

27

Smart contracten: voorbeeld

```
pragma solidity ^0.4.21;

contract Purchase {
    uint public value;
    address public seller;
    address public buyer;
    enum State { Created, Locked, Inactive }
    State public state;

    // Ensure that `msg.value` is an even number.
    // Division will truncate if it is an odd number.
    // Check via multiplication that it wasn't an odd number.
    function Purchase() public payable {
        seller = msg.sender;
        value = msg.value / 2;
        require((2 * value) == msg.value);
    }

    modifier condition(bool _condition) {
        require(_condition);
        _;
    }

    modifier onlyBuyer() {
        require(msg.sender == buyer);
        _;
    }

    modifier onlySeller() {
        require(msg.sender == seller);
        _;
    }

    modifier inState(State _state) {
        require(state == _state);
        _;
    }

    event Aborted();
    event PurchaseConfirmed();
    event ItemReceived();

    /// Abort the purchase and reclaim the ether.
    /// Can only be called by the seller before
    /// the contract is locked.
    function abort()
        public
        onlySeller
        inState(State.Created)
    {
        emit Aborted();
        state = State.Inactive;
        seller.transfer(this.balance);
    }

    /// Confirm the purchase as buyer.
    /// Transaction has to include `2 * value` eth...
    /// The ether will be locked until confirmReceived
    /// is called.
    function confirmPurchase()
        public
        inState(State.Created)
        condition(msg.value == (2 * value))
        payable
    {
        emit PurchaseConfirmed();
        buyer = msg.sender;
        state = State.Locked;
    }

    /// Confirm that you (the buyer) received the item.
    /// This will release the locked ether.
    function confirmReceived()
        public
        onlyBuyer
        inState(State.Locked)
    {
        emit ItemReceived();
        // It is important to change the state first because
        // otherwise, the contracts called using `send` below
        // can call in again here.
        state = State.Inactive;

        // NOTE: This actually allows both the buyer and the seller to
        // block the refund - the withdraw pattern should be used.

        buyer.transfer(value);
        seller.transfer(this.balance);
    }
```


NCOI M&D Seminars

28

Bestaande toepassingen/proefprojecten

- Axa Fizzy: verzekering bij vertraagde/geannuleerde vlucht
- Siemens-Hutten DDO: corporate social responsibility
- T-Mining: logistiek en maritieme supply chain
- Energy-coins: energycoin, solarcoin
- IP: Inmusik
- Kunst: NFT art sale -> recente veiling voor $69M
- Diamantindustrie: DeBeers' Tracr

Privaatrechtelijke aspecten van smart contracten

- Consensualisme: in principe geen formele vereisten voor contracten
- Maar: er moet wel een tegenpartij zijn
  - Probleem bij vb. DAO waar tegenpartij (DAO) geen juridische persoon is
- Identificatie van partijen?
- Wilsovereenstemming?
- Elektronisch contract: op zich geen probleem
- Informatieverplichtingen mogelijks van toepassing (vb. consumentenrecht)
  - Ook voor precontractuele fase!

Interpretatie van contracten

- Uitleg: gebruik van code vereist uitleg volgens vierhoekenbeding
  - Dus in principe geen aandacht voor intenties van partijen
  - Wil ook zeggen dat het contract alles zelf moet regelen -> hogere complexiteit
  - Hoewel de praktijk (vb. DAO 'hack') aantoont dat zij dat niet altijd zo willen…
  - -> Vaak dus wel vraag naar menselijke correctiemogelijkheden
- Maar ook dergelijke bedingen zijn niet absoluut
  - Afwegen van bedoeling en redelijke verwachtingen is dus onvermijdelijk
  - Maar beoordeling tekst blijft uitgangspunt
- Tekst = computertaal
  - *Quid* begrijpbaarheid? Te aanvaarden indien partij bijgestaan door deskundige
  - Maar wel ervaring vereist voor dergelijke deskundige

NFT's: volgende evolutie of volgende hype?

NFT's

- Non-fungible tokens
  - Elk token is uniek
  - Creëert zeldzaamheid en verzamelbaarheid
    - Elk NFT-token is uniek, zelfs al zijn er meer tokens met dezelfde achterliggende asset
  - Alles kan worden gekoppeld aan een NFT, waardoor een digitaal eigendomscertificaat ontstaat

Bloomberg

NFT Market Surpassed $40 Billion in 2021, New Estimate Shows

NCOI M&D Seminars

33

NFT's

- Veiligheid en transparantie
  - Blockchain maakt namaak moeilijk
  - Eigendom kan worden getraceerd
  - Garantie voor authenticiteit
  - -> positief voor de bestrijding van namaak
  - Maar:
    - platforms en accounts kunnen nog steeds worden gehackt!
    - Onderliggende asset kan wel worden gekopieerd

NCOI M&D Seminars

34

NFT's

- Traceren van IP-rechten
  - Smart contract kan bepaling bevatten dat maker automatisch een percentage krijgt op elke (door)verkoop
    - Dus: vergoeding voor maker op zowel primaire als secondaire markt
  - Echter: ook behoefte aan duidelijke overeenstemming over wie welke IP bezit
    - NFT = token dat verwijst naar een digitaal mediabestand. Bestand zelf maakt over het algemeen geen deel uit van de NFT zelf
    - Vaak blijft IP bij de maker *(bonusvraag: is er IP-bescherming?)*
      - Morele rechten versus vermogensrechten
      - Quid reproductierecht, distributierecht, mededelingsrecht, volgrecht, etc.? Of licentie?
      - Nood aan duidelijke afspraken!
    - Veel mensen maken NFT's met IP die ze niet bezitten
      - Minstens een reproductie, mededeling en distributie
      - Vb. Miramax v Tarantino, Hermitage v Lindemann, Hermès v MetaBirkins

NFT's

- Effectenwetgeving?
  - In se mogelijk om fractionele NFT's te creëren => deelnamerechten
  - NFT kan ook deelnamerechten inhouden, vb. stemrecht, winstdeling
  - MiFID kan dus van toepassing zijn, maar geval-per-geval te bekijken
    - In US: belang van verwachting van winst
  - Ook van belang voor platformen die handelen in NFT's!
- The taxman cometh
  - In de meeste landen onderworpen aan vermogenswinstbelasting!
- AML?
  - Exchange of wallet provider? "ruilmiddel"?
  - Ook van toepassing op transacties in kunsthandel >10.000 EUR
    - Kunstgalerijen, veilinghuizen, freeports?

Digital Operational Resilience Act (DORA) voor de financiële sector

37

37

DORA

- Voorstel voor een VERORDENING VAN HET EUROPEES PARLEMENT EN DE RAAD betreffende digitale operationele veerkracht voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014 en (EU) nr. 909/2014 (Digital Finance Package)
- Nood aan regels rond IT-risico's en operationele veerkracht
- Financiële sector blijft onder NIS (DORA = *lex specialis*)
- Kernprincipes:
  - IT-risicobeheer, testen van digitale operationele veerkracht
  - Incidentrapportage en informatie-uitwisseling
  - Goed beheer
  - Contractvereisten voor derden
  - Toezicht en samenwerking

38

38

DORA

- Entiteiten:
  - (a)kredietinstellingen,
  - (b)betalingsinstellingen,
  - (c)instellingen voor elektronisch geld,
  - (d)beleggingsondernemingen,
  - (e)aanbieders van cryptoactivadiensten, emittenten van cryptoactivadiensten, emittenten van asset-referenced tokens en emittenten van significante asset-referenced tokens,
  - (f)centrale effectenbewaarinstellingen,
  - (g)centrale tegenpartijen,
  - (h)handelsplatformen,
  - (i)transactieregisters,
  - (j)beheerders van alternatieve beleggingsinstellingen,
  - (k)beheermaatschappijen,
  - (l)aanbieders van datarapporteringsdiensten,
  - (m)verzekerings- en herverzekeringsondernemingen,
  - (n)verzekeringstussenpersonen, herverzekeringstussenpersonen en nevenverzekeringstussenpersonen,
  - (o)instellingen voor bedrijfspensioenvoorziening,
  - (p)ratingbureaus,
  - (q)wettelijke auditors en auditkantoren,
  - (r)beheerders van cruciale benchmarks,
  - (s)aanbieders van crowdfundingdiensten,
  - (t)securitisatieregisters;
  - (u)derde aanbieders van ICT-diensten,

NCOI M&D Seminars

DORA

- 'Digitale operationele veerkracht'
  - het vermogen van een financiële entiteit om haar operationele integriteit vanuit technologisch oogpunt op te bouwen, te verzekeren en te herzien door direct of indirect, door gebruik te maken van diensten van derden-ICT-aanbieders, te zorgen voor het volledige scala aan ICT-gerelateerde capaciteiten die nodig zijn om de beveiliging van de netwerk- en informatiesystemen aan te pakken waarvan een financiële entiteit gebruik maakt; en die de voortdurende verlening van financiële diensten en de kwaliteit ervan ondersteunen
- Governance- en controlekader
  - Het management draagt de eindverantwoordelijkheid voor het beheer van IT-risico's
  - Definieer het juiste risicotolerantieniveau
  - Bedrijfscontinuïteit en noodherstelplan
  - IT-audits en follow-up
  - Overeenkomsten met derden beheren en beoordelen

NCOI M&D Seminars

DORA

- Kader voor IT-risicobeheer
  - Alle beleidsregels, protocollen, etc. die u nodig hebt om uw IT te beveiligen
  - Informatiebeveiligingsbeheersysteem dat voldoet aan internationale normen
  - Functiescheiding (drie verdedigingslinies)
  - Regelmatige evaluatie en audit
- IT-systemen moeten worden bijgewerkt, geschikt voor het doel, betrouwbaar en veerkrachtig
- IT-systemen en -processen moeten worden geïdentificeerd en geclassificeerd op basis van de impact van potentiële incidenten
- Bescherming en preventie
- Detectie, respons en herstel
  - -> met rapportagevereisten aan toezichthouders en potentiële gebruikers

DORA

- Back-upbeleid en herstelmethoden
  - Inclusief transactieherstel om afwikkeling mogelijk te maken
  - Tweede site voor CSD's
- Leren en evolueren + communicatie
- Technische reguleringsnormen door EBA/ESMA/EIOPA + ENISA
  - Ook voor incidentclassificatie en rapportage
  - EU-hub voor het melden van grote incidenten
- IT incident management - > early warning systeem

DORA

- Veerkracht testen
  - Implementeer testprogramma, jaarlijks onafhankelijk testen
  - Belangrijke entiteiten: geavanceerde tests om de 3 jaar door middel van door bedreigingen geleide penetratietests door gecertificeerde testers - > resultaten delen
- Risicobeheer door derden
  - Adequate contractuele afspraken met audits en exitstrategie
    - Lijst van belangrijke bepalingen!
  - Multi-vendor strategie, vermijd concentratierisico
  - Jaarlijkse rapportage
  - Strategie voor kritische outsourcing (criteria te ontwikkelen door ESA's)

DORA

- Toezichtforum
- Informatie delen
- Hoofdtoezichthouder
  - Toezicht, onderzoeksbevoegdheden en inspecties ter plaatse
  - Vergoedingen die worden geheven op kritieke externe dienstverleners
  - Dwangsommen 1% dagelijkse wereldwijde omzet
- Administratieve sancties + mogelijke strafrechtelijke sancties

Network and Information Security Directive II

45

NIS2

- Toegenomen digitalisering van de samenleving (ook in licht van COVID-19)
- NIS1 is er niet in geslaagd om volledige potentieel te bereiken
- -> nieuwe richtlijn, uitgebreid toepassingsgebied, intrekking van NIS1
- Kern:
  - De lidstaten moeten nationale cyberbeveiligingsstrategieën vaststellen, bevoegde nationale autoriteiten, centrale contactpunten en responsteams voor computerbeveiligingsincidenten (CSIRT's) aanwijzen
  - Vereisten voor risicobeheer en rapportageverplichtingen voor cyberbeveiliging voor entiteiten van een type dat in bijlage I essentiële entiteiten wordt genoemd en belangrijke entiteiten in bijlage II
  - Verplichtingen vaststellen voor het delen van informatie over cyberbeveiliging

46

Essentiële entiteiten

- **Elektriciteit:** bedrijven, distributie, transmissie, *producenten, benoemde markten, marktdeelnemers*
- ***Stadsverwarming en -koeling***
- **Olie:** pijpleidingbeheerders, productie en raffinage, *voorraadbeheer*
- **Gas:** levering, distributie, transport, opslag, LNG, aardgas, operators
- ***Waterstof:*** *operatoren*
- **Vervoer:** lucht, spoor, water, weg
- **Bankwezen:** kredietinstellingen
- **Financiële marktinfrastructuren:** handelsplatformen en centrale tegenpartijen
- **Gezondheid:** zorgverleners, *basisfarmaceutica, referentielaboratoria, fabrikanten van kritieke hulpmiddelen, R&D*
- **Drinkwater:** leveranciers
- ***Afvalwater:*** *diensten die afvalwater verwerken*
- **Digitale infrastructuur:** IXP's, DNS, TLD, *clouddiensten, datacenters, contentlevering, trustserviceproviders, openbare e-communicatiediensten en -netwerken*
- ***Openbaar bestuur:*** *bestuursentiteiten van centrale overheden en NUTS1 en NUTS2*
- ***Ruimte:*** *grondexploitanten en dienstverleners*

NCOI M&D Seminars

Belangrijke entiteiten

- ***Post en koerierdiensten***
- ***Afvalverwerking***
- ***Chemicaliën***
- ***Voedingsbedrijven***
- ***Productie:***
  - *medische hulpmiddelen en hulpmiddelen voor in-vitrodiagnostiek; computer-, elektronische en optische producten; elektrische apparatuur; machines; motorvoertuigen en aanhangwagens; overige transportmiddelen*
- **Digitale aanbieders:**
  - Online marktplaatsen, online zoekmachines*, sociale netwerkplatforms*

NCOI M&D Seminars

NIS2

- In principe niet van toepassing op KMO's
- "incident": elke gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de daarmee verband houdende diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt
- Nationale cyberbeveiligingsstrategie
- Gecoördineerde openbaarmaking van kwetsbaarheden
- Nationale kaders voor crisisbeheer op het gebied van cyberbeveiliging
- Nationale bevoegde autoriteit en SPOC

NIS2

- CSIRTs en CSIRTs netwerk
- Europees netwerk van verbindingsorganisaties voor cybercrises (EU - CyCLONe)
- Gecoördineerd beheer van grootschalige cyberincidenten
- Vertegenwoordigers van de lidstaten, EC, ENISA
  - Paraatheid vergroten, gedeeld situationeel bewustzijn, gecoördineerd crisisbeheer, nationale plannen bespreken
- Tweejaarlijks Enisa-verslag over cyberbeveiliging
- Beleidsaanbevelingen
- Peer review
- Risicomanagement in essentiële en belangrijke entiteiten

NIS2

- Gecoördineerde EU-risicobeoordeling van kritieke toeleveringsketens
- Rapportering
  - Elk incident met significante impact op de dienstverlening
  - Significant = substantiële operationele verstoring of verliezen, (potentieel) effect op gebruikers
  - Afnemers van diensten moeten mogelijk ook worden geïnformeerd
  - Ook significante bedreigingen met potentiële impact
  - Eerste kennisgeving binnen 24 uur, tussentijds verslag, eindverslag
- EU-cyberbeveiligingscertificering
- TLD domeinnaam en registratiegegevens database
- Belangrijkste vestigingscriterium
  - Voor DNS, TLD, cloud, datacenters, content delivery en digitale providers
  - Geen vestiging = vertegenwoordiger

51

NCOI M&D Seminars

51

52