EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA'S TRUSSELSBILLEDE 2021

April 2020 til medio juli 2021

OKTOBER 2021

OM ENISA

ENISA, Den Europæiske Unions Agentur for Cybersikkerhed, bidrager til at opnå et højt fælles niveau af cybersikkerhed i Europa. Den Europæiske Unions Agentur for Cybersikkerhed blev oprettet i 2004 og blev styrket ved forordningen om cybersikkerhed. Agenturet bidrager til EU's politik for cybersikkerhed, styrker troværdigheden af IKT-produkter, -tjenester og -processer gennem ordninger for cybersikkerhedscertificering, samarbejder med medlemsstater og EU-organer, og hjælper Europa med at forberede sig til fremtidens cybersikkerhedsudfordringer. Gennem videndeling, kapacitetsopbygning og oplysningskampagner samarbejder agenturet med sine centrale interessenter om at styrke tilliden til den integrerede økonomi, om at øge modstandskraften af Unionens infrastruktur og om i sidste instans at garantere EU's og EU-borgernes digitale sikkerhed. Yderligere oplysninger om ENISA og agenturets arbejde findes her: www.enisa.europa.eu.

KONTAKT

Forfatterne kan kontaktes på etl@enisa.europa.eu.

Mediehenvendelser vedrørende dette dokument bedes rettet til press@enisa.europa.eu.

REDAKTØRER

Ifigeneia Lella, Marianthi Theocharidou, Eleni Tsekmezoglou, Apostolos Malatras — Den Europæiske Unions Agentur for Cybersikkerhed

BIDRAGYDERE

Claudio Ardagna, Stephen Corbiaux, Andreas Sfakianakis, Christos Douligeris

TAK

Vi vil gerne takke medlemmerne og observatørerne fra ENISA's ad hoc-arbejdsgruppe om cybertrusselsbilleder for deres værdifulde feedback og kommentarer i forbindelse ved valideringen af denne rapport. Vi vil også gerne takke ENISA's rådgivningsgruppe og netværket af nationale forbindelsesofficerer for deres værdifulde feedback. Vi vil desuden gerne takke ENISA's teams vedrørende situationsbevidsthed og indberetning af hændelser for deres aktive bidrag og støtte til at underbygge forskellige oplysninger i trusselsbilledet.

JURIDISK MEDDELELSE

MEDDELELSE OM OPHAVSRET

ISBN: 978-92-9204-536-4 – DOI: 10.2824/324797 – ISSN: 2363-3050

INDHOLDSFORTEGNELSE

KORT SAMMENFATNING

Dette er den niende udgave af rapporten om ENISA's trusselsbillede. Denne årlige rapport om status for cybersikkerhedstrusselsbilledet identificerer de vigtigste trusler, hovedtendenser i truslerne, trusselsaktører og angrebsteknikker, og beskriver også passende afbødende foranstaltninger. Arbejdet med vedholdende forbedring af vores metode til at opstille trusselsbilleder er i år blevet støttet af en nyoprettet ad hoc-ENISA-arbejdsgruppe om trusselsbilleder.

Tidsintervallet for rapporten om ENISA's trusselsbillede 2021 er april 2020 til juli 2021 og kaldes "rapporteringsperioden" i hele rapporten. I rapporteringsperioden omfatter de vigtigste identificerede trusler:

- **Ransomware**
- **Malware**
- **Cryptojacking**
- **E-mail-relaterede trusler**
- **Trusler mod data**
- **Trusler mod tilgængelighed og integritet**
- **Desinformation — misinformation**
- **Ikke-ondsindede trusler**
- **Angreb mod leverandørkæder**

I denne rapport analyserer vi de første 8 kategorier af trusler mod cybersikkerheden. Trusler mod forsyningskæder — den niende kategori — er på grund af deres særlige betydning blevet analyseret mere i detaljer i en speciel ENISA-rapport, "ENISA Threat landscape for Supply Chain Attacks" [1].

For hver af de identificerede trusler analyseres angrebsteknikker, markante hændelser og udviklingstendenser sammen med foreslåede afbødende foranstaltninger. Med hensyn til tendenser i rapporteringsperioden vil vi fremhæve følgende:

- **Ransomware** er blevet vurderet som **den største trussel i 2020-2021**.
- **Statslige organisationer styrket deres modstandsdygtighed** både nationalt og internationalt.
- **Cyberkriminelle motiveres i stigende grad af pengeafkastet** fra deres aktiviteter, f.eks. ransomware. **Kryptovaluta** er fortsat den almindeligste betalingsmetode for trusselsaktører.
- **Det fald i malware**, der blev konstateret i 2020, fortsætter i 2021. I 2021 så vi en stigning i antallet af trusselsaktører, der benytter relativt nye eller ualmindelige programmeringssprog til at portere deres kode.
- Mængden af **cryptojacking-infektioner** nåede et **rekordhøjt** niveau i første kvartal af 2021 i forhold til de foregående år. Den **økonomiske gevinst** ved kryptojacking har været et incitament for trusselsaktørerne til at foretage disse angreb.
- **Covid-19 er stadig det dominerende lokkemiddel i kampagner** for e-mailangreb.
- **I sundhedssektoren** var der en **kraftig stigning i brud på datasikkerheden**.
- **De traditionelle kampagner med distribueret servicenægtelse (Distributed Denial of Service, DDoS)**) er i 2021 mere målrettede, mere hårdnakkede og har flere og flere indgangsvektorer. **Tingenes internet** (**IoT**) i kombination med **mobilnet** fører til en ny bølge af DDoS-angreb.
- I 2020 og 2021 observerede vi et **maksimum af ikke-ondsindede hændelser**, da covid-19-pandemien i den grad blev en multiplikator for **menneskelige fejl** og **systemfejlkonfigurationer**, at de fleste overtrædelser i 2020 skyldtes fejl.

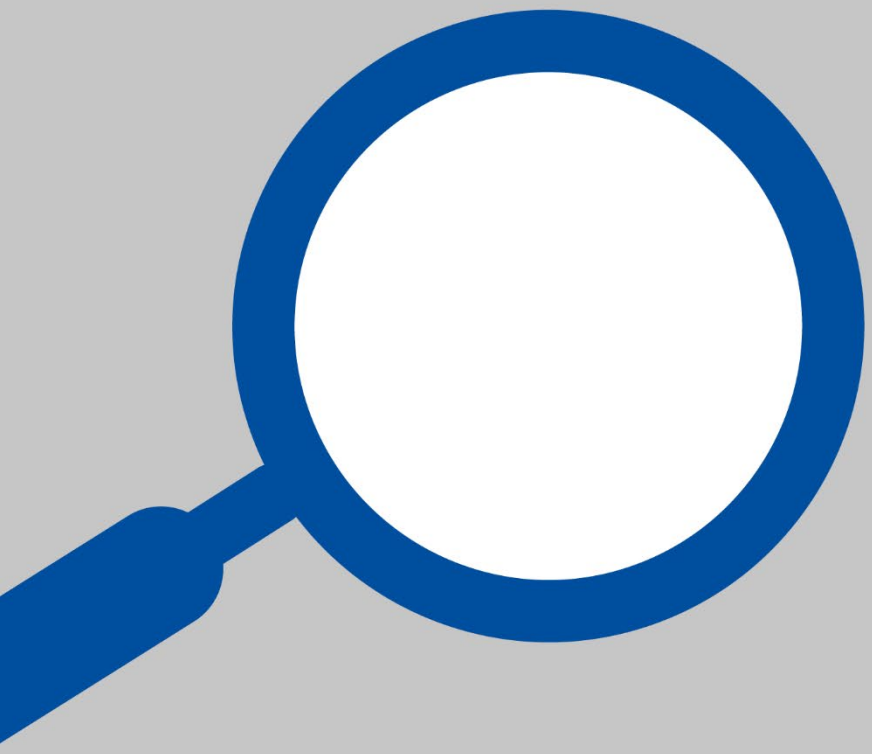
Hvis man har indsigt i udviklingstendenserne vedrørende trusselsaktørerne og deres motiver og mål, bliver det væsentligt lettere at planlægge forsvars- og afbødningsstrategier for cybersikkerhed. Dette indgår i vores overordnede trusselsvurdering, da det gør det muligt at prioritere sikkerhedskontrollerne og udforme en målrettet strategi med udgangspunkt i de mulige konsekvenser af, at truslerne bliver til virkelighed, og sandsynligheden for

[1] ENISA Threat Landscape for Supply Chain Attacks, juli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

det. Med dette for øje omhandler ENISA's trusselsbillede 2021 følgende fire kategorier af trusselsaktører inden for cybersikkerhed:

- **Statsstøttede aktører**
- **Aktører inden for cyberkriminalitet**
- **Hacker-for-hire-aktører (hackere til leje)**
- **Hacktivister**

Gennem løbende analyse har ENISA udledt udviklingstendenser og interessante punkter for hver af de største trusler, der redegøres for i ENISA's trusselsbillede 2021. Hovedresultaterne og vurderingerne i denne bedømmelse bygger på en række offentligt tilgængelige ressourcer, som er anført i de referencer, der er anvendt ved udarbejdelsen af dette dokument. Rapporten retter sig hovedsagelig mod strategiske og politiske beslutningstagere, men vil også være af interesse for det tekniske cybersikkerhedssamfund.



OVERSIGT OVER TRUSSELSBILLEDET

ENISA's trusselsbillede giver i sin niende udgave et generelt overblik over trusselsbilledet for cybersikkerhed. Rapporten ENISA's trusselsbillede er dels strategisk, dels teknisk, og indeholder oplysninger med relevans for både tekniske og ikke-tekniske læsere. Dette års arbejde er blevet støttet af en nyoprettet ad hoc-ENISA-arbejdsgruppe om trusselsbilleder inden for cybersikkerhed[2].

Cybersikkerhedsangrebene er fortsat steget i 2020 og 2021, ikke kun hvad angår vektorer og antal, men også i angrebenes konsekvenser. Også covid-19-pandemien har som forventet påvirket trusselsbilledet for cybersikkerhed. En af de mere vedvarende følger af covid-19-pandemien er varig overgang til en hybrid kontormodel. Cybersikkerhedstrusler, der udnytter af de "nye normale" tilstande i forbindelse med pandemien, er derfor ved at blive mainstream. Denne udvikling har øget angrebsfladen, og konsekvensen har været en stigning i antallet af cyberangreb mod organisationer og virksomheder gennem hjemmekontorerne[3].

Generelt er cybersikkerhedstruslerne voksende. Cybertrusselsbilledet er vokset i angrebenes raffinement, kompleksitet og konsekvenser, forstærket af den stadigt stigende online tilstedeværelse, omlægningen af traditionelle infrastrukturer til online- og cloudløsninger, avanceret interkonnektivitet og udnyttelse af nye egenskaber ved fremspirende teknologier som kunstig intelligens (AI)[4][5]. Navnlig er truslen mod forsyningskæderne og betydningen heraf kommet øverst på listen over større trusler på grund af deres potentielt katastrofale kaskadevirkninger, og ENISA har derfor opstillet et særligt trusselsbillede for denne trusselskategori[6].

Det er værd at bemærke, at i denne version af ENISA's trusselsbillede er der lagt særlig vægt på konsekvenserne af cybertrusler i forskellige sektorer, herunder dem, der er anført i direktivet om net- og informationssikkerhed (NISD). Hver sektors særlige forhold kan give interessant indsigt, når det kommer til trusselsbillede, potentielle indbyrdes afhængigheder og områder af betydning. Derfor bør der ses nærmere på sektorspecifikke trusselsbilleder.

Der er i år også taget nogle markante skridt af forsvarere i cybersamfundet og af de politiske beslutningstagere. Det globale samfund er begyndt at indse vigtigheden af kommunikation og samarbejde om at undersøge og spore cyberkriminelle på baggrund af, at ransomware er den mest fremtrædende trussel i rapporteringsperioden for ENISA's trusselsbillede 2021, og især at den er ved at blive et hovedpunkt på dagsordenerne for strategimøder mellem globale ledere.

Læsere af tidligere udgaver af ENISA's trusselsbillede 2021 vil bemærke en forskel i kortlægningen af de største trusler. I år gik ENISA et skridt tilbage og konsoliderede trusselskategorierne for at få ensartede trusler integreret og bedre repræsenteret. Dette indgår i den igangværende indsats til at forny trusselsklassificeringen og vil bidrage til metoderne til at fastlægge udviklingstendenserne de næste par år.

ENISA's trusselsbillede 2021 bygger på en række open source-kilder og efterretninger om cybertrusler. Det peger på større trusler, udviklinger og resultater og indeholder relevante strategier for afbødning på højt niveau. ENISA arbejder i øjeblikket på at styrke metoden til at rapportere om trusselsbilledet for at fremme gennemsigtighed og konsekvens i arbejdet.

[2] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[3] IBM – Cost of a Data Breach Report 2020 - https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
[4] ENISA'S trusselsbillede for AI: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
[5] https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/
[6] ENISA' trusselsbillede for angreb mod leverandørkæder, juli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

1.1. STØRSTE TRUSLER

Vi så en række nye cybertrusler i løbet af 2020 og 2021. Ud fra analysen i denne rapport identificerer og fokuserer ENISA's trusselsbillede 2021 på følgende 8 grupper af hovedtrusler (se Figur 1). Disse 8 trusselsgrupper fremhæves på grund af deres fremstående placering i rapporteringsperioden, deres popularitet og de konsekvenser, truslerne har haft.

- **Ransomware**
  Ransomware er en form for ondsindede angreb, hvor angriberne krypterer en organisations data og kræver betaling for at genoprette adgangen. Ransomware har været den største trussel i rapporteringsperioden, hvor den har forårsaget adskillige højtprofilerede, meget omtalte hændelser. Betydningen og konsekvenserne af ransomware-truslen fremgår også af en række relaterede politiske initiativer i EU og verden over.

- **Malware**
  Malware er software eller firmware, der er beregnet til at udføre en uautoriseret proces, som får negativ indvirkning på systemers fortrolighed, integritet eller tilgængelighed. Truslen fra malware har vedholdende rangeret højt i mange år, dog i aftagende grad i rapporteringsperioden for ENISA's trusselsbillede 2021. Brugen af nye vedhæftningsteknikker og visse større fremskridt for retshåndhævelsessamfundet har påvirket de pågældende trusselsaktørers operationer.

- **Cryptojacking**
  Cryptojacking eller skjult kryptominering er en form for cyberkriminalitet, hvor en kriminel bruger i hemmelighed udnytter offerets computerkraft til at generere kryptovaluta. Med den stigende udbredelse af kryptovalutaer i den brede offentlighed er der iagttaget en stigning i tilsvarende cybersikkerhedshændelser.

- **E-mail-relaterede trusler**
  E-mail-relaterede angreb er en række trusler, der udnytter svagheder i folks psyke og daglige vaner fremfor tekniske sårbarheder i informationssystemer. Interessant nok består truslen stadig i mærkbart omfang trods de mange oplysnings- og uddannelseskampagner mod disse typer angreb. Navnlig kompromitteringen af forretnings-e-mails og avancerede teknikker til at opnå pengegevinst er stigende.

- **Trusler mod data**
  Denne kategori omfatter brud/lækager i datasikkerheden. Et datasikkerhedsbrud eller en datalækage er frigivelse af følsomme, fortrolige eller beskyttede data til et usikkert miljø. Brud på datasikkerheden kan opstå som følge af et cyberangreb, et insiderjob eller utilsigtet tab eller eksponering af data. Truslen er fortsat høj, da adgang til data er et vigtigt mål for angribere af mange grunde, f.eks. afpresning, løsepenge, æreskrænkelse, misinformation mv.

- **Trusler mod tilgængelighed og integritet**
  Tilgængelighed og integritet er mål for en lang række trusler og angreb, hvor kategorierne servicenægtelse (Denial of Service (DoS)) og angreb på websteder er fremtrædende. Distribueret servicenægtelse (DDoS) er tæt knyttet til webbaserede angreb og er en af de mest kritiske trusler mod IT-systemerne, da de er rettet mod deres tilgængelighed ved at udtømme ressourcer. Dette medfører fald i ydeevne, tab af data og tjenesteudfald. DDoS rangerer konsekvent højt i ENISA's trusselsbillede, både på grund af dets tilstedeværelse i faktiske hændelser og dets potentiale for store konsekvenser.

- **Desinformation — misinformation**
  Desinformations- og misinformationskampagner er i stigning som følge af den øgede brug af sociale medieplatforme og onlinemedier og af folks øgede onlinetilstedeværelse i forbindelse med covid-19-pandemien. Det er første gang, at denne gruppe trusler dukker op i ENISA's trusselsbillede, men de har stor betydning i cyberverdenen. Desinformations- og misinformationskampagner anvendes ofte i hybride angreb for at svække den almindelige tillid, der er et vigtigt argument for cybersikkerhed.

- **Ikke-ondsindede trusler**
  Trusler anses sædvanligvis for tilsigtede ondsindede aktiviteter, der iværksættes af modstandere, som har visse incitamenter til at angribe et givet mål. Med denne kategori dækker vi trusler, hvor der ikke er synlige ondsindede

hensigter. De skyldes hovedsagelig menneskelige fejl og systemfejlkonfigurationer, men kan også være fysiske katastrofer, der rammer IT-infrastrukturer. Disse trusler grundet deres natur altid til stede i det årlige trusselsbillede og volder stor bekymring ved risikovurderinger.

Figur 1: ENISA's trusselsbillede 2021 — De største trusler

Det skal her bemærkes, at de ovennævnte trusler omfatter kategorier og indsamlede trusler, og er konsolideret i de otte ovennævnte områder. Hver trusselskategori analyseres yderligere i et særligt kapitel i denne rapport, som uddyber dens særlige karakteristika og giver mere specifik information, resultater, udviklingstendenser, angrebsteknikker og afbødende vektorer.

1.2. HOVEDTENDENSER

Nedenstående liste opsummerer de vigtigste udviklingstendenser, der er iagttaget i cybertrusselsbilledet i rapporteringsperioden. Disse tendenser gennemgås også detaljeret i de forskellige kapitler, der udgør ENISA's trusselsbillede 2021.

- **Meget sofistikerede og slagkraftige kompromitteringer af forsyningskæder** blev mere udbredte, som belyst i ENISA's særlige rapport "Threat Landscape on Supply Chain". **Leverandører af forvaltede tjenester** er højt prioriterede mål for cyberkriminelle.
- **Covid-19 var drivkraft for cyberspionage** og skabte **muligheder for cyberkriminelle**.
- **Statslige organisationer har styrket deres modstandsdygtighed** både nationalt og internationalt. Myndighederne har øget deres indsats for at standse statsstøttede trusselsaktører og tage retlige skridt over for dem.
- **Cyberkriminelle motiveres i stigende grad af pengeafkastet** fra deres aktiviteter, f.eks. ransomware. **Kryptovaluta** er fortsat det almindeligste betalingsmiddel for trusselsaktører.
- Cyberkriminelle angreb **er i stigende grad rettet mod og rammer kritisk infrastruktur**.
- **Kompromittering gennem phishing e-mails og brute force-angreb mod fjernkontroltjenester (Remote Desktop Services (RDP))** er fortsat de to almindeligste **smitteveje for ransomware**.

- Fokus på **forretningsmodeller med ransomware as a service (RaaS)** er steget i løbet af 2021 og gør det vanskeligt at placere de enkelte trusselsaktører korrekt.
- Forekomsten af **ransomware med tredobbelt afpresning** steg kraftigt i løbet af 2021.
- Det **fald i malware**, der blev konstateret i 2020, fortsætter i 2021. I 2021 så vi en stigning i det antal trusselsaktører, der benytter relativt nye eller usædvanlige programmeringssprog til at portere deres kode.
- **Malware rettet mod containermiljøer** er blevet meget mere udbredt, med nye udviklinger som filløs malware, der eksekveres fra arbejdslageret.
- Udviklere af malware finder stadig metoder til at **vanskeliggøre reverse engineering og dynamisk analyse**.
- Mængden af **cryptojacking-infektioner** nåede et **rekordhøjt** niveau i første kvartal af 2021 i forhold til de seneste år. Den **økonomiske gevinst** ved kryptojacking har givet trusselsaktørerne incitament til sådanne angreb.
- **Omfanget af kryptominering i 2021 og cryptojacking-aktiviteter er rekordhøjt.**
- Vi ser, at der sker et **skift fra browser- til filbaseret kryptojacking**.
- **Covid-19 er stadig det dominerende lokkemiddel i kampagner** for e-mailangreb.
- **Kompromittering gennem forretnings-e-mails** er steget og er blevet mere **sofistikeret** og **målrettet**.
- **Phishing-as-a-Service (PhaaS)** som forretningsmodel vinder udbredelse.
- Trusselsaktørerne rettede deres opmærksomhed mod **information om vacciner** i forbindelse med trusler mod data og information.
- **I sundhedssektoren** var der en **kraftig stigning i brud på datasikkerheden**.
- Traditionelle angreb med distribueret servicenægtelse (DDoS, Distributed Denial of Service) bevæger sig over mod **mobilnet og tingenes internet (IoT)**.
- **Servicenægtelse med løsesum (RDoS, Ransom Denial of Service)** er den nye grænse for angreb med servicenægtelse.
- **Deling af ressourcer i virtuelle miljøer** virker forstærkende på DDoS-angreb.
- **DDoS-kampagnerne** er i 2021 blevet mere målrettede, langt mere hårdnakkede og benytter flere og flere indgangsvektorer.
- **Desinformation baseret på kunstig intelligens (AI)** hjælper angribere med at foretage deres angreb.
- **Phishing er kernen i desinformationsangreb** og udnytter i høj grad folks overbevisninger.
- **Misinformation og desinformation** er kernen i cyberkriminelle aktiviteter og vokser i et hidtil uset tempo.
- **Forretningsmodellen Disinformation as a-Service (DaaS)** er vokset betydeligt, ansporet af den stigende indvirkning af covid-19-pandemien og behovet for at få mere information.
- I 2020 og 2021 så vi et **højdepunkt af ikke-ondsindede hændelser**, da covid-19-pandemien blev en multiplikator for **menneskelige fejl** og **systemfejlkonfigurationer** i en sådan grad, at de fleste overtrædelser i 2020 skyldtes fejl.
- Der har været en **skarp stigning i ikke-ondsindede hændelser inden for cloudsikkerhed**.

1.3. DE STØRSTE TRUSLERS NÆRHED TIL EU

Cybertruslers nærhed til EU er et vigtigt aspekt af ENISA's trusselsbillede. Det er især vigtigt for at hjælpe analytikere med at vurdere betydningen af cybertrusler og kæde dem sammen med potentielle trusselsaktører og -vektorer, og desuden for at guide valget af passende målrettede afbødende vektorer. I overensstemmelse med den foreslåede klassificering for EU's fælles sikkerheds- og forsvarspolitik (FSFP)[7] inddeler vi cybertrusler i fire kategorier som illustreret i **Tabel 1**.

Tabel 1: Klassificering af cybertruslers nærhed

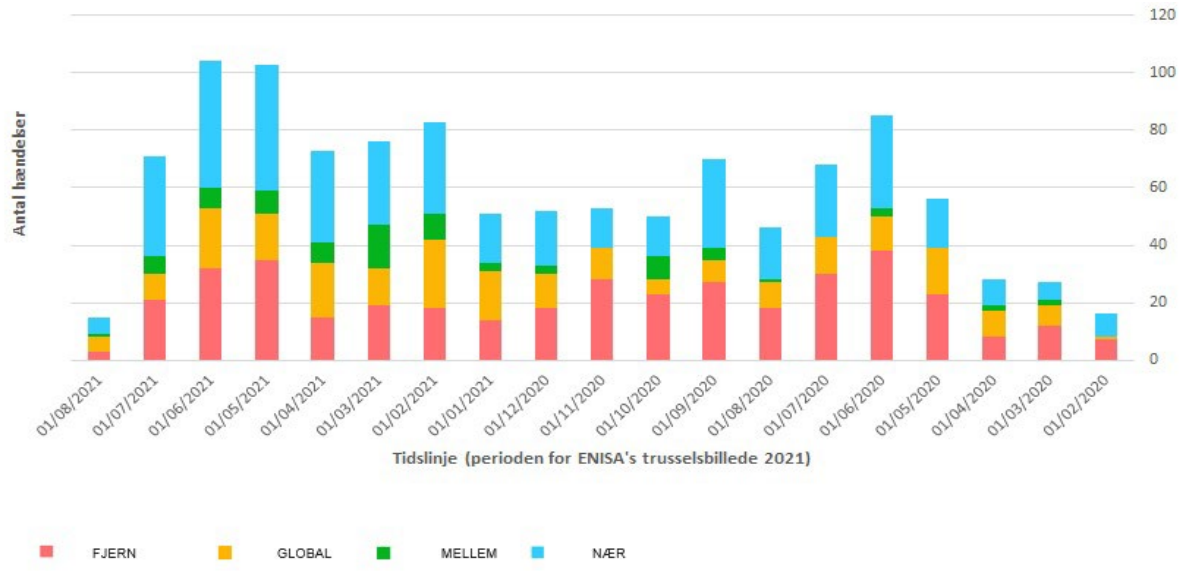
Nærhed	Bekymring
NÆR	Berørte net og systemer, som styres og er sikret inden for EU's grænser. Berørt befolkning inden for EU's grænser.

[7] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

Nærhed	Bekymring
MELLEM	Net og systemer, der anses for at være af afgørende betydning for operationelle målsætninger, er inden for EU's digitale indre marked og sektorerne i NIS-direktivet, men deres kontrol og sikkerhed afhænger af institutionelle, offentlige eller private instanser, der er uden for EU eller hører under medlemsstaterne. Berørt befolkning i geografiske områder tæt på EU's grænser.
FJERN	Netværk og systemer, der, hvis de påvirkes, vil få kritisk indvirkning på de operationelle målsætninger inden for EU's digitale indre marked og sektorerne under NIS-direktivet. Kontrollen og sikkerheden af disse net og systemer ligger uden for EU's institutionelle instanser og medlemsstaternes offentlige og private instanser. Den berørte befolkning befinder sig i geografiske områder langt fra EU.
GLOBAL	Alle ovennævnte områder

Figur 2 illustrerer en tidslinje for hændelser for de vigtigste trusselskategorier, der er rapporteret i ENISA's trusselsbillede 2021. Bemærk, at oplysningerne i diagrammet er baseret på efterretninger indhentet fra åbne kilder (OSINT) og er et resultat af ENISA's arbejde inden for situationsbevidsthed[8].

Figur 2: Tidslinje for observerede hændelser i forbindelse med større trusler i ENISA's trusselsbillede (OSINT-baseret situationsbevidsthed) baseret på nærhed.



I 2021 var der flere hændelser end i 2020, som ovenstående tal viser. Navnlig er der i kategorien NÆR et stadigt stigende antal observerede hændelser i forbindelse med de største trusler, hvad der viser deres betydning i sammenhæng med EU. Den månedlige udvikling (som for kortheds skyld ikke er vist i figuren) er ret ens for de forskellige klassificeringer. Dette er ikke overraskende, da cybersikkerhed ikke har grænser, og trusler i de fleste tilfælde bliver virkeliggjort på alle niveauer af nærhed. Det er værd at bemærke, at der i de sidste måneder af ENISA's trusselsbillede 2021 konstateres en øget nærhed af EU, en tendens som ENISA fortsat vil overvåge for at se, hvordan den udvikler sig og hvordan den hænger sammen med trusselsaktørernes aktiviteter og de fortsatte trusselsvektorer.

[8] I overensstemmelse med forordningen om cybersikkerhed, artikel 7, stk. 6, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

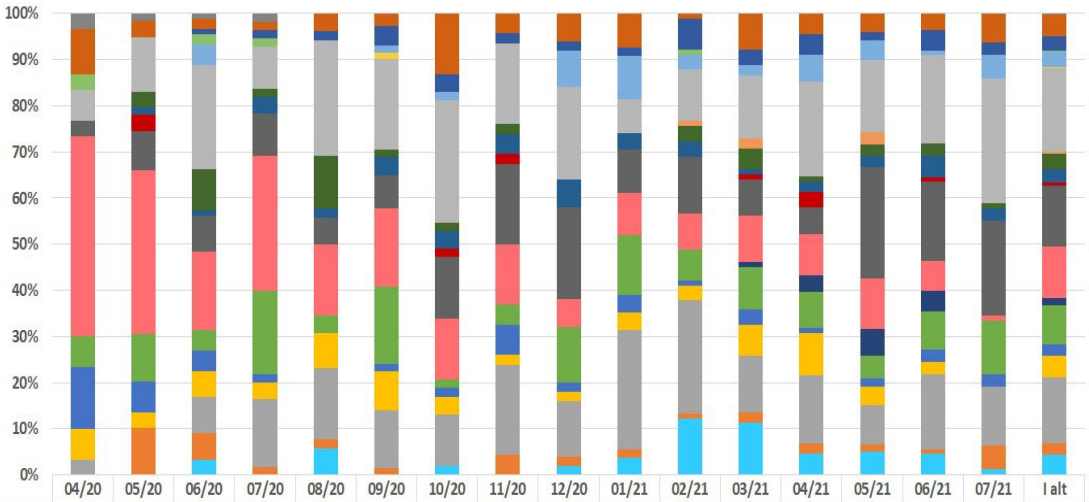
1.4. DE VIGTIGSTE TRUSLER FORDELT PÅ SEKTOR

Cybertrusler er normalt ikke begrænset til én bestemt sektor og berører i de fleste tilfælde mere end én af dem. Dette hænger givetvis sammen med, at truslerne i mange tilfælde udnytter sårbarheder i underliggende IKT-systemer, der anvendes i flere forskellige sektorer. Hvad der imidlertid må tages i betragtning, er målrettede angreb og angreb, der udnytter forskellene i modenhed af cybersikkerheden i de forskellige sektorer, og visse sektorers popularitet/fremtrædende placering. Disse faktorer bidrager til trusler, der manifesterer sig som hændelser i bestemte sektorer, og derfor er det vigtigt at se nærmere på sektorspecifikke aspekter af iagttagne hændelser og trusler. En sådan analyse kan belyse udviklingen i hver sektor og sektorers indbyrdes afhængighed.

Figur 3 og figur 4 fremhæver sektorer, der er berørt af iagttagne hændelser i henhold til oplysninger fra åbne kilder (OSINT) som resultat af ENISA's arbejde inden for situationsbevidsthed[9]. Figurerne afspejler hændelser, som er knyttet til de største trusler i ENISA's trusselsbillede 2021. Dette er ENISA's første forsøg på at kortlægge truslers indvirkning på specifikke sektorer. I de kommende år og i fremtidige versioner af trusselsbilledet vil der blive sat ind på bringe sektorerne i overensstemmelse med dem, der er opført i NIS-direktivet (NISD) og forslaget til revision heraf (NISD 2.0).

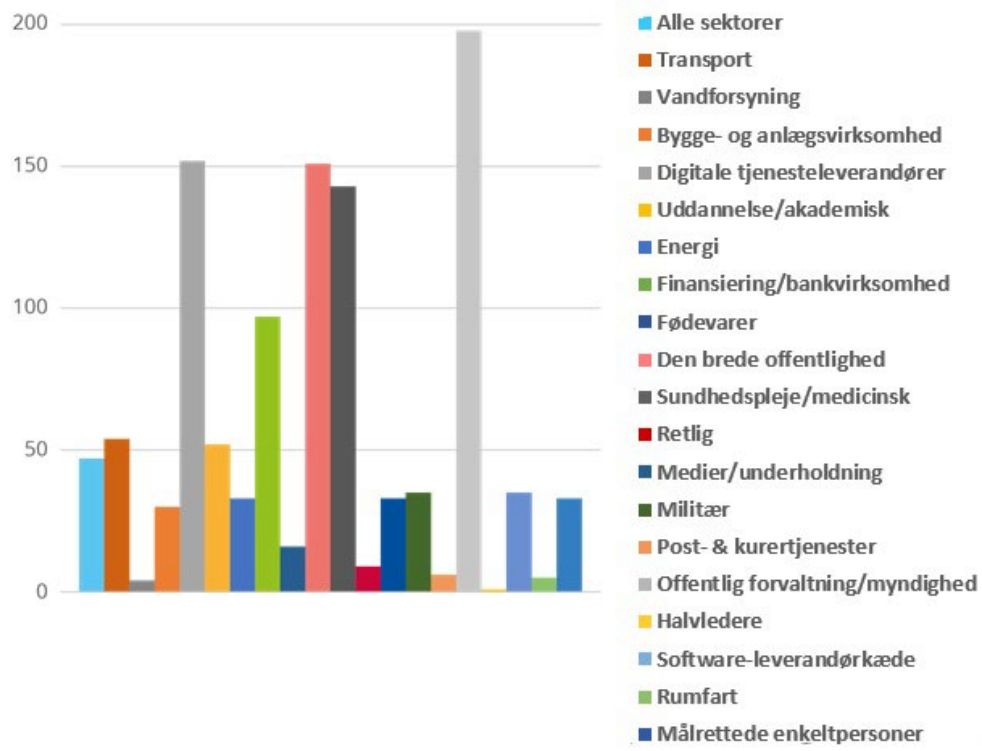
[9] I overensstemmelse med forordningen om cybersikkerhed, artikel 7, stk. 6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)

Figur 3: Tidslinje for observerede hændelser relateret til de vigtigste trusler i ENISA's trusselsbillede for den berørte sektor.



	04/20	05/20	06/20	07/20	08/20	09/20	10/20	11/20	12/20	01/21	02/21	03/21	04/21	05/21	06/21	07/21	I alt
Vandforsyning	1	1	1	1													2
Transport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	49
Målrettede enkeltpersoner			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Rumfart	1		2	1							1						4
Software-leverandørkæde			4			1	1		4	5	3	2	5	5	1	4	35
Halvledere						1											1
Offentlig forvaltning/myndighed	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	189
Post- & kurertjenester											1	2		3			6
Militær		2	8	1	6	1	1	1			3	4	1	3	3	1	33
Medier/underholdning		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	32
Retlig		2					1	1				1	3		1		7
Sundhedspleje/medicinsk	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	137
Den brede offentlighed	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	117
Fødevarer												1	3	7	5		16
Finansiering/bankvirksomhed	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	89
Energi	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	25
Uddannelse/akademisk	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		48
Digitale tjenesteleverandører	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	151
Bygge- og anlægsvirksomhed		6	5	1	1	1		2	1	1	1	2	2	2	1	4	24
Alle sektorer			3		3		1		1	2	11	10	4	6	5	1	47

Figur 4: Målsektorer fordelt på antal hændelser (april 2020-juli 2021)



I denne rapporteringsperiode var der en lang række hændelser, som var rettet mod den offentlige administration og forvaltning og leverandører af digitale tjenester. Sidstnævnte er ikke overraskende i betragtning af den horisontale levering af tjenester til denne sektor og dermed dens indvirkning på mange andre sektorer. Vi konstaterede også et betydeligt antal hændelser, der var rettet mod slutbrugerne og ikke nødvendigvis en bestemt sektor. Sundhedssektoren var også et vigtigt mål, og denne aktivitet viser tegn på at stige i de sidste måneder af rapporteringsperioden (maj-juli 2021). Interessant nok ser finanssektoren et konstant antal hændelser hele året rundt. Også i leverandørkæden for software ses der et stigende antal hændelser i løbet af 2021, en iagttagelse, der går igen i ENISA's rapport om trusselsbilledet i leverandørkæden[10].

1.5. METODOLOGI

Rapporten om ENISA's trusselsbillede 2021 bygger på oplysninger fra åbne, hovedsageligt strategiske, kilder og på ENISA's egne kapaciteter til efterretninger om cybertrusler, og dækker mere end én sektor, teknologi og kontekst. Rapporten sigter mod at være industri- og sælgeruafhængig og henviser til eller citerer arbejde af forskellige sikkerhedsforskere, sikkerhedsblogs og nyhedsmedieartikler, som teksten refererer til i mange fodnoter. Tidsintervallet for rapporten om ENISA's trusselsbillede 2021 er april 2020 til juli 2021 og kaldes "rapporteringsperioden" i hele rapporten.

Fremgangsmåden for rapporten om ENISA's trusselsbillede 2021 var følgende: I hele den relevante periode indsamlede ENISA gennem situationsbevidsthed en liste over større hændelser fra åbne kilder. Denne liste dannede grundlaget for opstillingen af listen over de vigtigste trusler og var kildemateriale til flere tendenser og statistikker i rapporten.

Efterfølgende gennemførte ENISA og eksterne eksperter en grundig dokumentationsundersøgelse af foreliggende litteratur fra åbne kilder som nyhedsmedieartikler, ekspertudtalelser, efterretningsrapporter, hændelsesanalyser og rapporter om sikkerhedsforskning. Gennem løbende analyse udledte ENISA tendenser og punkter af interesse for hver af de største trusler, der fremlægges i ENISA's trusselsbillede 2021. Hovedresultaterne og vurderingerne i

[10] ENISA Threat Landscape for Supply Chain Attacks, juli 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

denne bedømmelse bygger på en række offentligt tilgængelige ressourcer, som er anført i de referencer, der er anvendt ved udarbejdelsen af dette dokument

I rapporten søger vi at skelne mellem, hvad der er rapporteret af vores kilder, og hvad der bygger på vores egen vurdering. (Vi anfører udtrykkeligt "efter vores vurdering"). Endelig udtrykker vi ved vurderinger sandsynligheden for hændelsen (med ord som f.eks. sandsynlig, meget sandsynlig, helt sikker)[11].

I denne rapport er endelig anvendt MITRE ATT&CK® -rammen[12] til at fremhæve de angrebstaktikker og -teknikker, der er relevante for en given trussel (se bilag A). For hver ATT&CK®-taktik fremlægges de anvendte teknikker. Dette kan føre til en liste over ATT&CK Mitigations[13], der kan anvendes til afbødning. MITRE ATT&CK® er en videnbase, der er et fælles sprog for imødegåelsestaktik og -teknikker baseret på iagttagelser fra den virkelige verden. Videnbasen MITRE ATT&CK® anvendes som grundlag for at udvikle specifikke trusselsmodeller og -metoder i den private sektor, hos myndighederne og i samfundet omkring cybersikkerhedsprodukter og -tjenester.

Rapporten blev valideret af ENISA's ad hoc-arbejdsgruppe om cybertrusselsbilleder[14], der blev nedsat i april 2021. Gruppen bestod af eksperter fra europæiske og internationale offentlige og private instanser.

Med henblik på den fremtidige udvikling af trusselsbilleder er ENISA i færd med at formalisere en ny metode, der skal fremme gennemsigtighed og skabe grundlag for strukturerede, veltilpassede processer. I denne forbindelse vil metoden til trusselsbilleder fremover blive offentliggjort sammen med en revideret trusselsklassificering.

1.6. RAPPORTENS STRUKTUR

ENISA's trusselsbillede 2021 har bibeholdt den samme struktur som i tilsvarende tidligere ENISA-rapporter om trusselsbilledet til at belyse de største cybertrusler i 2021. Læsere af tidligere versioner vil bemærke, at trusselskategorierne er blevet samlet i forbindelse med overgangen til det nye klassificeringssystem for cybersikkerhedstrusler, der skal anvendes i fremtiden.

Denne rapport er struktureret som følger:

Kapitel 2 ser på udviklingen inden for trusselsaktører (dvs. statsstøttede aktører, cyberkriminelle, hacker-for-hire-aktører og hacktivister).
Kapitel 3 drøfter vigtige resultater, hændelser og tendenser inden for ransomware.
Kapitel 4 fremlægger vigtige resultater, hændelser og tendenser inden for malware.
Kapitel 5 beskriver vigtige resultater, hændelser og tendenser inden for cryptojacking.
Kapitel 6 belyser vigtige resultater, hændelser og tendenser inden for e-mail-relaterede trusler.
Kapitel 7 drøfter vigtige resultater, hændelser og tendenser inden for datatrusler.
Kapitel 8 fremlægger vigtige resultater, hændelser og tendenser inden for trusler mod tilgængelighed og integritet.
Kapitel 9 understreger betydningen af hybride trusler og beskriver vigtige resultater, hændelser og tendenser inden for desinformation og misinformation.
Kapitel 10 fokuserer på vigtige resultater, hændelser og tendenser inden for ikke-ondsindede trusler.
Bilag A beskriver, hvilke teknikker der hyppigt bruges for hver trussel, baseret på MITRE ATT&CK®-rammen.
Bilag B beskriver markante hændelser for hver trussel, der er iagttaget i rapporteringsperioden.

[11] CIA - Words of Estimative Probability https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
[12] MITRE ATT&CK®, https://attack.mitre.org/
[13] https://attack.mitre.org/mitigations/enterprise /
[14] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes