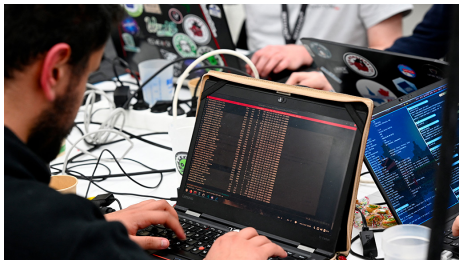
Artikel

03-04-2024 - 11:37
20221103STO48002

Europa-Parlamentet

Bekæmpelse af cyberkriminalitet: Nye EU-cybersikkerhedslov forklaret

Parlamentet har vedtaget nye regler til at styrke EU's cybersikkerhed i nøglesetorer. Find ud af hvordan de nye regler vil beskytte dig.



Cybersikkerhed
https://multimedia.europarl.europa.eu/x_N01_AFPS_221109_CYBS_ev?p_p_state=pop_up&lang=da&autoplay=off

Med den hurtigtvoksende digitalisering af vores daglige liv, der er gået endnu hurtigere som følge af Covid-19-pandemien, er beskyttelsen mod cybertrusler blevet essentielt for, at samfundet kan fungere på en ordentlig måde.

Cyberangreb er dyrbare. Ifølge Europa-Kommissionen, kostede cyberkriminalitet årligt den globale økonomi €5,5 billioner ved udgangen af 2020.

I november 2022 opdaterede Europa-Parlamentet EU's lov til at fostre investeringer i stærkere cybersikkerhed for vigtige tjenester og kritisk infrastruktur og styrke reglerne på tværs af EU. Parlamentet godkendte endeligt reglerne til at forbedre beskyttelsen af EU's essentielle infrastruktur, herunder den digitale infrastruktur den 22. november. Lovgivningn strammer risikoevalueringen og rapporteringskravene for kritiske aktører for 11 essentielle sektorer.

Læs mere om hvordan EU skaber den digitale omstilling

Strammere cybersikkerhedsforpligtelser - NIS2-direktivet

Netværks- og informationssikkerhedsdirektivet (NIS2) introducerer nye regler til at gøre

fremskridt for et højt fælles cybersikkerhedsniveau på tværs af EU – både for virksomheder og lande. Det styrker også cybersikkerhedskravene for medium og større virksomheder, der har forretninger og udbyder tjenester inden for vigtige sektorer.

Som en opdatering af NIS-direktivet i 2016 skal det forbedre klarheden og implementeringen, såvel som adressere hurtig udvikling på området. Det dækker flere sektorer og aktiviteter end tidligere, effektiviserer rapporteringsforpligtelser og adresserer leveringskædesikkerheden.

Efter godkendelse af Parlamentet og EU-landene i Rådet i november har medlemslandene nu 21 måneder til at implementere det.

Find ud af hvad de vigtigste og nye cybertrusler er

Flere sektorer inkluderet

Den nye lov udvider spændet for sektorer og aktiviteter, der er kritiske for økonomien og samfundet herunder energi, transport, bankforretning, sundhed, digital infrastruktur, offentlig administration og rumsektoren. Men den dækker ikke national og offentlig sikkerhed, lovhåndhævelse eller retsvæsenet. Loven gælder for offentlig administration på centralt og regionalt niveau, men ikke for alle parlamentet og nationalbanker.

Det kræver flere selskaber og sektorer for at kunne foretage cybersikkerhedsrisicihåndtering herunder udbydere af offentlige, elektroniske kommunikationstjenester, sociale medieoperatører, fabrikanter af vigtige produkter (f.eks. medicinsk udstyr), post og kurertjenester.

Mere strikse forpligtelser for lande

Loven fastsætter strikse cybersikkerhedsforpligtelser for EU-landene, når det gælder tilsyn. Den forbedrer håndhævelsen af disse forpligtelser herunder harmonisering af sanktioner på tværs af medlemslandene. Den forbedrer også samarbejdet mellem EU-landene inklusiv for større hændelser under EU's Agentur for Cybersikkerheds (ENISA) paraply.

Cyber Resilience Act: Øget sikkerhed for digitale produkter

Flere og flere hverdagsprodukter har en digital komponent - f.eks. babyalarmer, opkoblede dørklokker eller wifi-routere - hvilket gør dem sårbare over for cyberangreb. For at sikre, at de er sikre, godkendte Parlamentet Cyber Resilience Act, som giver et ensartet sæt af obligatoriske, EU-dækkende cybersikkerhedskrav til produkter, der er forbundet til en anden enhed eller et netværk.

Under forhandlingerne om den endelige udformning af loven med EU-landene i Rådet sørgede MEP'erne for, at listen over systemer og produkter, der skal opfylde strengere sikkerhedskrav, omfatter private sikkerhedskameraer, babyalarmer, intelligente hjemmeassistenter, intelligente ure og intelligent legetøj. Sikkerhedsopdateringer vil blive installeret automatisk og adskilt fra

funktionelle opdateringer.

Digital Operational Resilience Act: Beskyttelse af EU's finansielle system -

Idet den finansielle sektor bliver mere og mere afhængig af software og digitale processer, har den også brug for en øget beskyttelse. Den **digitale operationelle resiliensakt (DORA)** vil sikre, at EU's finansielle sektor er mere modstandsdygtig over for operationelle forstyrrelser og cyberangreb. Parlamentet gav endelig godkendelse til lovgivningen, der tidligere blev indgået med Rådet, den 10. november. Rådet godkendte formeldt lovgivningen den 28. november 2022.

Loven introducerer og harmoniserer digitale operationelle modstandsdygtighedkrav for EU's finansielle tjenestessektor, der forpligter virksomheder til at sikre, at de kan modstå, modsvare og komme sig efter at informations- og kommunikationsteknologisforstyrrelser og trusler.

De nye regler vil gælde for alle virksomheder, der udbyder finansielle tjenester - såsom banker, betalingsudbydere, elektroniske pengeudbyder, investeringsfirmaer, kryptoaktivitetsudbydere såvel som alle vigtige udbydere inden for informations- og kommunikationsteknologi.

Nationale myndigheder vil føre tilsyn og håndhæve implementeringen.

Læs mere om hvordan EU skaber den digitale omstilling:

- Bekæmpelse af seksuelt misbrug af børn på nettet
- Regler for kunstig intelligens
- Den Europæiske Datastrategi
- EU's digitale markeds- og tjenestesforordninger
- Faren ved kryptovalutaer
- EU's plan til at overvinde leveringskrisen for halvledere

Mere

Briefing
Kommissionen glæder sig over den politiske aftale om nye cybersikkerhedsregler for net- og informationssystemer
Lovgivningstoget
Lovgivningstoget for DORA
Rådet: Tidslinje over digital finansiering