Članek

23-11-2022 - 14:33
20211008STO14521

Evropski parlament

Zakaj je kibernetska varnost v EU pomembna? Kakšno škodo povzročajo kibernetski napadi?

Z vse širšo uporabo digitalnih rešitev raste tudi število kibernetskih napadov.

Od ukradenih osebnih podatkov do blokiranih bolnišnic: kibernetski napadi imajo lahko hude posledice. Preberite več o kibernetski varnosti in njenem pomenu.

Digitalna preobrazba gospodarstva in družbe se je v zadnjih letih pospešila, kar prinaša priložnosti in izzive. Med njimi je tudi kibernetska varnost. Ker smo vse bolj vezani na digitalne tehnologije, je škoda zaradi kibernetskih napadov vse večja. Kibernetska varnost je postala zelo pomembna in ključna prednostna naloga EU.

Zanašanje na digitalne tehnologije

Med področji, ki se v veliki meri zanašajo na omrežja in informacijske sisteme ter jih zato kibernetski napadi najbolj ogrožajo, so promet, energetika, zdravstvo, telekomunikacije in digitalna infrastruktura, banke in finančni trgi, varnost, demokratični procesi, vesolski programi in obramba. KIbernetska varnost vključuje tudi osebne naprave, operacijske sisteme in naprave, povezane z internetom, od alarmnih sistemov in do avtomobilov in celo nekaterih hladilnikov.

Že dolgo vse pogosteje uporabljamo digitalne rešitve, delo na daljavo, nakupovanje na spletu in ohranjanje stikov prek spleta pa so med pandemijo strmo narasli. Te rešitve lahko koristijo uporabnikom, gospodarstvu in obnovi EU po covidu. Vendar pa jih je pospremilo tudi naraščajoče število zlonamernih kibernetskih dejavnosti.

Preberite več o ključnih in rastočih grožnjah kibernetski varnosti.

22,3 milijarde

Ocena števila naprav, ki naj bi bile povezane v internet stvari do leta 2024

*Kibernetski napadi, varnost in obramba - definicije**

- Kibernetski napadi so poskusi zlorabe informacij, ki jih napadalci kradejo, uničujejo ali razkrivajo. Njihovi cilji so lahko motnje ali uničenje računalniških sistemov in mrež.
- Kibernetska varnost obsega informacijsko in komunikacijsko varnost, operativno tehnologijo in informacijske plaforme, potrebne za zagotavljanje varnosti digitalnih sistemov.
- Kibernetska obramba vključuje kibernetsko varnost in analize groženj ter strategije za zaščito pred grožnjami za državljane, institucije in države.

Kibernetske grožnje v EU: škoda za posameznika in družbo

Gospodarska škoda zaradi kibernetskega kriminala

Napadalci lahko uporabljajo tehnike, kot je phishing, in s pomočjo zlonamernih elektronskih sporočil in spletnih strani **kradejo bančne informacije** ali pa izsiljujejo organizacije po tem, ko jim **blokirajo informacijske sisteme in podatke**.

Varen kibernetski prostor je eden od temeljev digitalnega enotnega trga EU, saj omogoča ne le digitalne rešitve, temveč tudi doseganje njihovega polnega potenciala - ljudje, ki se ob uporabi spleta počutijo varno, ga bodo raje uporabljali. Rezultati ankete, objavljene v EU maja 2022, kažejo, da se je v letu 28 odstotkov evropskih malih in srednjih podjetij v letu 2021 soočilo s kibernetskim kriminalom.

Več o tem,kako se zaščititi pred kibernetskim kriminalom

5500 milijard evrov

Kibernetski napadi so globalno med najhitreje rastočimi oblikami kriminala. Ocena Komisije pravi, da je leta 2020 kibernetski kriminal stal svetovno gospodarstvo 5500 milijard evrov, kar je dvakrat toliko kot leta 2015.

Posledice za demokracijo

Kibernetski napadi povzročajo škodo, ki ni le gospodarska in finančna, temveč vpliva na same **demokratične temelje Evropske unije** in so grožnja **delovanju družbe**. Kampanje dezinformacij in napačnih informacij so denimo med orodji kibernetskega vojskovanja. Poročilo evropske agencije za kibernetsko varnost (ENISA) o grožnjah v letu 2022 omenja, da roboti, ki se pretvarjajo, da so ljudje, preplavljajo spletne strani vladnih agencij z lažnimi komentarji. Širjenje globokih ponaredkov (deepfakes) in dezinformacij, ki jih pomaga širiti umetna inteligenca, šibi kredibilnost in zaupanje v informacije, medije in novinarstvo.

Posledice kibernetskih napadov za mir in varnost

Kibernetski napadi, kombinirani z dezinformacijami, gospodarskimi pritiski ter konvencionalnimi oboroženimi napadi, preizkušajo odpornost demokratičnih držav in institucij ter neposredno ogrožajo mir in varnost v EU. Po podatkih agencije ENISA tekom ruske vojne v Ukrajini kibernetski napadi hodijo z roko v roki s konvencionalnimi vojaškimi taktikami. Namen hekerjev je uničevati in motiti delovanje vladnih agencij in organizacij, ki upravljajo s kritično infrastrukturo, prav tako pa tudi spodkopavati zaupanje v vodstvo države.

Posledice kibernetskih napadov za osnovne storitve in kritične sektorje

Osnovne storitve in kritični sektorji, kot so promet, zdravje in finance, so vse bolj odvisni od digitalnih tehnologij. Skupaj z rastočim številom predmetov, povezanih v internet stvari, ima lahko neposredne posledice, kibernetska varnost je lahko celo vprašanje življenja in smrti.

Od kibernetskih napadov na bolnišnice, zaradi česar morajo preložiti nujne medicinske storitve,

do napadov na električna omrežja in vodovodne sisteme - napadalci ogrožajo izvajanje osnovnih storitev. En kibernetski napad ima lahko posledice za milijone ljudi. Maja 2021 je denimo hekerski napad z izsiljevalsko programsko opremo za več ur onemogočil zdravstvene storitve po vsem Irskem, posledice je bilo čutiti še več tednov.

Celo denimo avtomobile in domove, ki so vse bolj povezani s spletom, bi lahko napadi ogrozili na načine, ki si jih sploh še ne moremo predstavljati.

Velika grožnja

Svetovni gospodarski forum opredeljuje kibernetske napade kot eno od desetih najpomembnejših globalnih groženj.

Ukrepi EU za kibernetsko varnost

Evropska podjetja in organizacije za kibernetsko varnost porabijo bistveno manj kot ameriška. Da zagotovi varnost bolnišnic, bank in ponudnikov energije ter dobro delovanje institucij, mora EU investirati v močno kibernetsko varnost ključnih storitev in kritične infrastrukture ter nadgraditi evropsko zakonodajo.

Novembra 2022 je Parlament sprejel **direktivo za visoko skupno raven kibernetske varnosti v Uniji (NIS2)**, ki orisuje predpise za krepitev odpornosti EU. V istem mesecu so evropski poslanci sprejeli akt o digitalni operativni odpornosti (DORA) , ki veča odpornost finančnega sektorja EU proti kibernetskim napadom.

Parlament je 22. novembra 2022 podal svojo dokončno odobritev predpisov, ki izboljšujejo zaščito ključne infrastrukture EU, vključno z digitalno infrastrukturo. Zakonodaja uvaja strožja merila za ocene tveganja in poročanja za ključne akterje v 11 ključnih sektorjih.

Več o tem, kako EU oblikuje digitalni svet:

- Akt o digitalnih storitvah in akt o digitalnih trgih: razlaga
- Evropska strategija za podatke
- Zakonodaja na področju umetne inteligence: kako izkoristiti potencial te tehnologije
- Kakšna so tveganja kriptovalut in kako lahko zakonodaja EU pomaga

Trdna strategija EU za kibernetsko varnost
https://multimedia.europarl.europa.eu/en/a-robust-eu-cybersecurity-strategy_N01-AFPS-211012-CYBE_ev

Več o kibernetski varnosti v EU

Evropska komisija: Nova strategija EU za kibernetsko varnost in nova pravila za bolj odporne fizične in digitalne kritične subjekte
Služba Evropskega parlamenta za raziskave: Zmogljivosti EU na področju kibernetske obrambe
Visoka raven kibernetske varnosti v EU (Direktiva NIS2) (Služba Evropskega parlamenta za raziskave)
Akt o digitalni operativni odpornosti (DORA)
Indeks digitalnega gospodarstva in družbe (DESI)