Artikel

27-01-2022 - 16:12
20211111STO17184

Europaparlamentet

Så vill Europaparlamentet stärka cybersäkerheten (intervju)

Intervju med föredragande ledamot Bart Groothuis

Parlamentsledamöter vill bättre skydda européer och företag mot det växande hotet från cyberbrott. Lär dig hur i vår intervju med ledamoten Bart Groothuis.

Intervjun genomfördes innan direktivet om säkerhet för nätverks- och informationssystem (NIS2) godkändes av parlamentet i november 2022.

Allteftersom nätverk och informationssystem blir allt mer en centrala i våra dagliga liv, har också cyberhoten ökat. Cyberattacker kan åstadkomma ekonomisk skada och till och med störa vatten och elförsörjningen eller sjukhusverksamhet. En stark cybersäkerhet är nödvändigt för att

skydda medborgare och för att på bästa sätt dra nytta av digitaliseringens sociala och ekonomiska fördelar.

Lär dig mer om hur cybersäkerhet påverkar dig

Parlamentet godkände den 11 november, sin förhandlingsståndpunkt om översynen av direktivet för nätverk och informationssäkerhet (NIS-direktivet). Ledamot Bart Groothuis som ansvarar för akten förklarar parlamentets ståndpunkt.

Vad är de mest största hoten mot cybersäkerheten?

– Utpressningsmjukvara, "ransomware", är med stor marginal det största hotet. Förekomsten tredubblades över världen år 2020 och vi förutser att ett nytt rekord kommer nås i år. För tio år sedan, riktade de skadliga programmen in sig på individer, där offret tvingades betala 100 till 200 euro till hackaren. Nuförtiden ligger utpressningsbeloppen på i snitt 140 000 euro. Inte bara stora utan också små företag blir utsatta och måste betala för att kunna fortsätta driva sin verksamhet. Det är också ett stort hot därför att det har blivit ett utrikespolitiskt verktyg för skrupelfria stater.

Lär dig mer om de vanligaste formerna av cyberbrott.

Vad är "ransomware"? (källa: Enisa)

- En typ av skadlig kod som infekterar datorsystem och hindrar offren från att använda systemet och dess data. Offret får oftast ett meddelande via pop-up som kräver betalning för att återfå tillgång till systemen.

Påverkar utpressningsprogrammen livet hos medborgare och företag?

– Vi ser att de skadliga programmen inriktar sig på nästan allt som erbjuder tjänster till medborgare. Det kan vara ett lokalt kommunkontor, ett sjukhus eller ett lokalt företag.

Parlamentet och rådet arbetar på cybersäkerhetslagstiftning. Målet är att bättre skydda måltavlor från hackers. EU-företag som tillhandahåller livsnödvändiga eller viktiga tjänster måste ta cybersäkerhetsåtgärder och regeringar behöver ha förmågan att hjälpa och dela information med företag och andra regeringar.

Vad vill parlamentet?

– Parlamentet vill att lagstiftning ska bli mer ambitiös. Målsättningen ska vara så bred som möjligt, vi måste skydda och hjälpa sektorer som är vitala för vår levnad. Europa bör vara en säker plats att leva och arbeta. Vi kan inte vänta, vi behöver mer lagstiftning och det snabbt.

Varför är det bråttom?

– Inom cybersäkerheten måste du göra det tydligt att du inte är den svagaste. EU-företag investerar redan 41 procent mindre i cybersäkerhet än vad företag i USA gör. Och USA agerar snabbt. President Biden inför krislagstiftning och vi vill inte ha en situation där Europa blir ett attraktivt mål för utpressningssystem. Därför måste investeringar i cybersäkerhet göras nu. Den andra anledningen är att det finns problem i cybersäkerhetsvärlden som behöver lösas så snabbt som möjligt. GDPR-lagen skapar problem för cybersäkerhetsexperter. Kan de eller kan de inte dela information om cybersäkerhet? Det borde finnas en juridisk grund för att dela information avsedd för att hindra cyberattacker.

Vilka utmaningar finns för parlamentet i förhandlingarna?

– Det kommer föras debatt om förslagets bredd, och om vilka sektorer som ska inkluderas. Vi kommer också att behöva diskutera de administrativa följderna för företag. Parlamentet tror att lagstiftning skulle skydda företag men det bör också vara praktiskt och genomförbart. Vad kan vi rimligen fråga efter? En annan fråga är internets kärna**, rotdomännamnstjänster (**root domain name service). Den europeiska kommissionen och rådet vill inbegripa detta i regleverket. Det är jag emot, eftersom Ryssland och Kina vill göra samma sak. Vi borde hålla internets kärna fri och öppen och behålla vår multiaktör-modell.

Varför är det viktigt att ha gemensamma cybersäkerhetsregler över hela Europa?

– Grunden för lagstiftningen är en fungerande inre marknad. Det ska inte vara en fråga om huruvida du bedriver verksamhet i Slovakien, Tyskland eller Nederländerna. Du vill vara säker på att det finns en gemensam cybersäkerhetsnivå och att landet som du arbetar i har den infrastruktur som krävs. Vi borde harmonisera reglerna och göra våra medborgares liv säkra.

Mer information

Pressmeddelande: "Cybersecurity: MEPs strengthen EU-wide requirements against threats", 2021-10-28 (en)
Följ ärendet från förslag till beslut (en)
Interaktiv grafik
Parlamentets utredningstjänst: "A high common level of cybersecurity in the EU", 2021-02-19 (en)
Europeiska kommissionens digitala strategi
Enisa: Ransomware