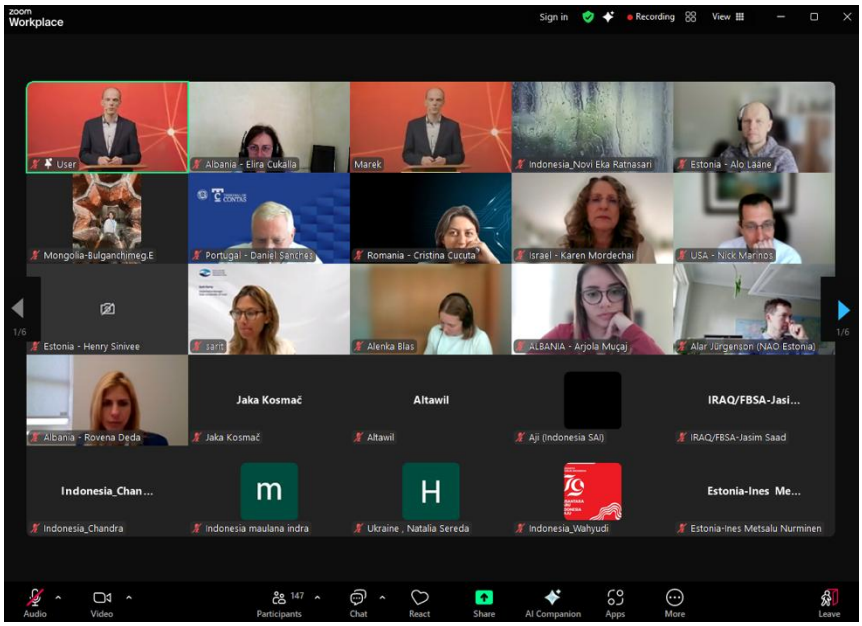
KLSH ndjek e-seminarin e organizuar nga ITWG mbi "Auditimin e Infrastrukturës kritike të Informacionit"

24 prill 2025

Grupi i punës i EUROSAI-t për IT (ITWG) në të cilin KLSH anëtarëson, organizoi në datë 24 prill 2025, e-seminarin me titull "Auditimi i Infrastrukturës kritike të Informacionit". Qëllimi i këtij seminari ishte eksplorimi mbi sigurinë kibernetike dhe auditimi i infrastrukturës kritike të informacionit në një mjedis gjithnjë e më të ndërlikuar dixhital, duke shkëmbyer përvoja ndërkombëtare dhe praktika të mira mes anëtarëve të EUROSAI-t dhe partnerëve ndërkombëtarë.

Seminari online u organizua si kombinim i ndarjes së përvojave nga SAI të ndryshëm, diskutime me panel ekspertësh, si dhe pyetje dhe sondazhe ndërvepruese me pjesëmarrësit.

Në fjalën e hapjes Kryetari i EUROSAI ITWG, njëkohësisht drejtues i SAI-t të Estonisë, cilësoi se sistemet e ngritura mbi infrastruktura kritike janë shumë të rëndësishme për funksionimin e një shteti dhe ofrimin e shërbimeve cilësore për qytetarët. Në këtë kontekst po aq i rëndësishëm është dhe zhvillimi i auditimit IT në këto infrastruktura.



Qëndrueshmëria e Infrastrukturave Kritike në Evropë - Ku ndodhemi?

Agjencia e Bashkimit Evropian për Sigurinë Kibernetike (ENISA) - Misioni i Agjencisë së Bashkimit Evropian për Sigurinë Kibernetike (ENISA) është të arrijë një nivel të lartë dhe të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, në bashkëpunim me komunitetin më të gjerë. ENISA e realizon këtë mision duke vepruar si një qendër ekspertize për sigurinë kibernetike, duke mbledhur dhe ofruar këshilla teknike të pavarura dhe me cilësi të lartë, si dhe ndihmë në çështjet e sigurisë kibernetike për shtetet anëtare dhe institucionet, organet dhe agjencitë e BE-së. Ajo kontribuon në zhvillimin dhe zbatimin e politikave të sigurisë kibernetike.

Sfidat e Sigurisë Kibernetike për Infrastrukturat Kritike të Informacionit - Perspektiva Estoneze

Autoriteti i Sistemit të Informacionit të Estonisë, ofroi shembujt e praktikave të veta, si institucioni model në drejtim të zhvillimeve teknologjike, në të cilin standardet për sigurinë kibernetike *(cybersecurity)* rinovohen çdo vit. Kjo, duke pasur parasysh ndryshimet teknologjike të shpejta dhe përvojat e së shkuarës, me fokus riskun e sulmeve kibernetike, siç e theksoi në fjalën e tij dhe përfaqësuesi i Autoritetit të Sistemit të Informacionit të Estonisë *(Estonian Information System Authority).*

Në panelin e diskutimit për sigurinë kibernetike të infrastrukturës kritike në të ardhmen, u ndanë mendime mbi sfida të vazhdueshme mbi standardet dhe reagimet ndaj incidenteve, qasjen ndaj riskut të sulmeve kibernetike, ndërgjegjësimin për monitorim të vazhdueshëm, etj. Pjesëmarrësit u shprehën se maturimi me qëllim menaxhimin dhe reagimin ndaj incidenteve kibernetike, nuk është i njëjtë në shtete të ndryshme, për këtë arsye entet publike dhe private duhet të kenë prioritet simulimin e incidenteve kibernetike, me fokus marrjen e informacionit për situatën aktuale të infrastrukturave të tyre dhe ku duhet të ndërhyjnë me qëllim rritjen e sigurisë.

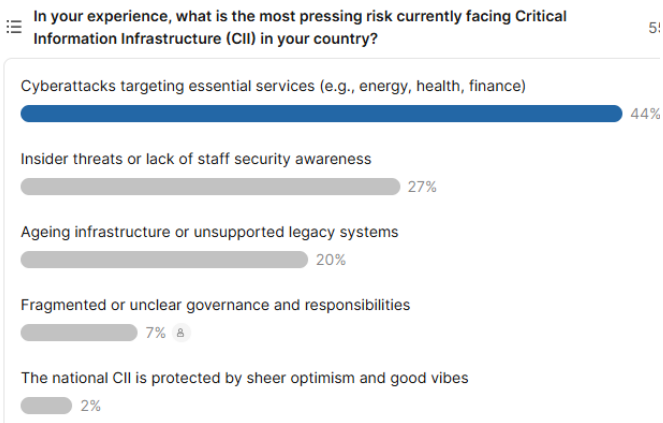
Në vijim të seminarit u prezantuan auditime konkrete nga SAI të zhvilluara si Zyra Federale Gjermane mbi Sigurinë e Informacionit në Infrastruktura Kritike. Përvojë në këtë drejtim ndau dhe Sllovenia, mbi menaxhimin e vazhdimësisë së shërbimit *(business continuity)* në fushën e furnizimit me ujë të pijshëm, si një shërbim esencial për qytetarët.

Në pjesën e dytë të seminarit u ndanë eksperienca nga:

- SAI i Finlandës, për auditimin në sistemet e informacionit të Policisë dhe Administratës Gjyqësore, si infrastruktura kritike me rëndësi të madhe publike;
- SAI i Izraelit, për forcimin e qëndrueshmërisë dixhitale të Izraelit;
- SAI i Hollandës, për ripërdorimin e kornizës (*framework)* aktuale për auditimin e kontratave në *cloud;*
- SAI i Zvicrës, mbi faktorët kritikë të suksesit për Qëndrueshmërinë Kibernetike të Infrastrukturës Kritike;

Në vijim, përfaqësuesi nga Zyra e Përgjithshme e Auditimit të SHBA (U.S GAO) zhvilloi prezantimin me temë: *"Përdorimi i auditimeve për të përmirësuar mbrojtjen e infrastrukturës kritike nga kërcënimet kibernetike"*, duke bërë një pasqyrim të situatës aktuale dhe çfarë mund të përmirësohet për të zvogëluar riskun e sulmeve *ransomware*. Në këtë kuadër, GAO ka krijuar dhe udhëzuesin për Auditimin e Programeve të Sigurisë Kibernetike *(Cybersecurity Program Audit Guide)*, me qëllim për t'iu siguruar audituesve metodologjinë, si dhe teknikat e procedurat për të bërë vlerësimet e duhura gjatë auditimeve të infrastrukturave kritike.

Gjithashtu, përfaqësuesit e ARABOSAI-t, ndanë përvojat e tyre me raste konkrete mbi qasjen dhe sfidat e tyre në këtë fushë, që nga identifikimi i infrastrukturave kritike, deri te auditimi i tyre.



Me qëllim rritjen e ndërveprimit midis të pranishmëve, u përdor platforma "*Slido"* për të drejtuar pyetje direkte për prezantuesit, si dhe instrumenti i sondazheve *(polls)*, ku të pranishmit në seminar shprehen mendimet e tyre bazuar në përvojat personale gjatë auditimit të infrastrukturave kritike.

Në fjalën përmbyllëse, sekretariati i ITWG falenderoi të pranishmit për pjesëmarrjen dhe ndarjen e përvojave të tyre mbi auditimin e infrastrukturave kritike dhe njoftoi mbi planifikimin

e takimit vjetor hibrid të ITWG me fokus qeverisjen dhe shërbimet elektronike (e-government, e-service).

Ky seminar u ndoq nga audituesit e Departamentit të Auditimit IT, si dhe Drejtoria e Teknologjisë së Informacionit në KLSH.