BULETIN JAVOR
4-8 MARS 2024

Shprehja e javës

"Dikur ishte e shtrenjtë për t'i bërë gjërat publike dhe e lirë për t'i bërë ato private. Tani është e shtrenjtë për t'i bërë gjërat private dhe e lirë për t'i bërë ato publike."

Clay Shirky

Përmbajtja:

Shqipëria - rol aktiv në diskutimet e Kombeve të Bashkuara për Sigurinë Kibernetike

Në datat 4-8 Mars, Departamenti i Shtetit të SHBA-së zhvilloi Seksionin e 7-të Substancial të OEWG, në New York.

Në këtë angazhim të rëndësishëm kombëtar, delegacioni i Shqipërisë ka luajtur një rol aktiv dhe ka dhënë kontribut të qenësishëm. AKCESK është pjesë e këtij delegacioni përmes zëvendës drejtoreshës së përgjithshme, znj. Floreta Faber. Pjesëmarrja e saj në seksionin e radhës u mbështet nga Departamenti Amerikan i Shtetit, Byroja e Hapësirës Kibernetike dhe Politikave Digjitale (CDP), në kuadër të fuqizimit të grave në çështjet e sigurisë kibernetike në OEWG.

Bashkëpunimi ndërkombëtar mbetet një gur themeli i qasjes së Shqipërisë në forcimin e kapaciteteve të sigurisë kibernetike. Përfshirja aktive e vendit tonë në forume ndërkombëtare pasqyrojnë një përpjekje shumëdimensionale, për të përmirësuar qëndrueshmërinë kibernetike kombëtare dhe rajonale.

Duke qenë gjithmonë në linjë të plotë me praktikat më të mira ndërkombëtare dhe duke forcuar bashkëpunimin, Shqipëria po pozicionohet si një lojtar kyç në përpjekjet globale për të ofruar një ekosistem digjital të sigurt dhe të qëndrueshëm për të gjithë.

AKCESK mbështet bashkëpunimin rajonal në reagim të sulmeve kibernetike

AKCESK mori pjesë në Konferencën Rajonale të Sigurisë Kibernetike, "Cyber Zero", e cila u mbajt në Prishtinë, në datat 4 dhe 5 Mars. Kjo konferencë solli në vëmendje thelbin e bashkëpunimit rajonal në mbrojtjen e infrastrukturave kritike kundër kërcënimeve në rritje kibernetike në rajonin e Ballkanit Perëndimor.

Gjatë panelit "Ndërtimi i një mburoje mbrojtëse për infrastrukturat kritike në Ballkanin Perëndimor përmes bashkëpunimit", Z. Saimir Kapllani, Drejtor i Analizës së Përputhshmërisë, Riskut dhe Kontrollit në AKCESK, hodhi dritë mbi sfidat me të cilat përballet rajoni ynë në fushën e sigurisë kibernetike. Ai theksoi rëndësinë vitale të zgjerimit të bashkëpunimit për ndarjen e të dhënave mbi kërcënimet kibernetike, rritjen e kapaciteteve të ekspertëve rajonalë përmes iniciativave të përbashkëta të trajnimit, dhe domosdoshmërinë e fuqizimit të partneriteteve publike dhe private në sektorët e kërkimit dhe akademik. Z. Kapllani gjithashtu nënvizoi nevojën për investime strategjike në teknologji të avancuara që do të ndihmojnë në monitorimin efikas dhe menaxhimin e incidenteve kibernetike.

Ky takim ishte një platformë për të ndërtuar marrëdhënie më të forta rajonale dhe për të përcaktuar rrugët e ardhshme të veprimit për një Ballkan Perëndimor më të sigurt në hapësirën kibernetike. AKCESK vazhdon të jetë i angazhuar për të ndërmarrë hapa konkretë drejt një bashkëpunimi më të ngushtë rajonal dhe ndërkombëtar, duke ndarë përgjegjësitë dhe duke përbashkuar forcat për të përballuar sfidat e sigurisë kibernetike.

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039

BULETIN JAVOR
4-8 MARS 2024

Sprehja e javës

"Dikur ishte e shtrenjtë për t'i bërë gjërat publike dhe e lirë për t'i bërë ato private. Tani është e shtrenjtë për t'i bërë gjërat private dhe e lirë për t'i bërë ato publike."

Clay Shirky

Përmbajtja:

Përdorimi i WordPress për të hakuar faqe të tjera

Kriminelët kibernetikë po përdorin faqet e internetit të kompromentuara të WordPress për të formuar një ushtri masive për sulme kredenciale. Studiuesit kanë zbuluar një fushatë ku sulmuesit instalojnë një skrip në shabllonet HTML, duke i detyruar vizitorët të vizitojnë një faqe web-i të ndryshme nga WordPress dhe të përpiqen të identifikohen duke përdorur kombinime të ndryshme të emrave të përdoruesit dhe fjalëkalimeve. Pasi viktima thyen kodin e hyrjes, ata i transmetojnë informacionin sulmuesve, të cilët më pas dërgojnë udhëzime të mëtejshme. Mbi 1,700 faqe interneti e mbajnë këtë skript, duke ofruar një grup të madh përdoruesish që do të rekrutohen pa dashje në këtë ushtri të shpërndarë *bruteforce*.

Link: Lexo më shumë

Mediat sociale Instagram dhe Facebook u përballën me ndërpreje globale

Përdoruesit e Facebook dhe Instagram në mbarë botën janë loguar dhe kanë probleme me hyrjen, me përdoruesit që marrin fjalëkalime të pasakta. Ndërprerja e këtyre aplikacioneve preku përdoruesit në SHBA, Evropë dhe Azi. Meta, një faqe interneti që ndjek ndërprerjet e shërbimit në internet, ka marrë raporte që sugjerojnë se çështja nuk është e izoluar në një rajon apo vend të caktuar. Meta konfirmoi ndërprerjen dhe po punon për ta zgjidhur atë. Shërbimet Meta u rikthyen në internet, por shkaku i ndërprerjes mbetet i panjohur.

Link: Lexo më shumë

American Express - Data Breach

American Express po paralajmëron klientët se kartat e kreditit u ekspozuan në një shkelje të të dhënave të palëve të treta pasi një përpunues tregtar u hakerua. Shkelja preku të dhënat e anëtarëve të American Express Card, duke përfshirë numrat e llogarisë, emrat dhe të dhënat e skadimit. American Express këshillon klientët që të rishikojnë deklaratat e llogarisë së tyre dhe të raportojnë aktivitetet e dyshimta, të aktivizojnë njoftimet e menjëhershme përmes aplikacionit në celular dhe të marrin në konsideratë të kërkojnë një numër të ri karte nëse informacioni i kartës së tyre është vjedhur.

Link: Lexo më shumë

PATCHING ALERT

JetBrains - Patching alert

Agjencia e SHBA-së për Sigurinë Kibernetike dhe Sigurinë e Infrastrukturës (CISA) ka shtuar një vulnerabilitet kritik për JetBrains TeamCity, një server për menaxhim ndërtimi dhe integrim të vazhdueshëm. Vulnerabiliteti, me një rezultat të ashpërsisë 9.8 nga 10, i lejon sulmuesit të anashkalojnë identifikimin dhe të kryejnë veprime të administratorit. Vulnerabiliteti është një vektor i shpeshtë sulmi për aktorët keqdashës kibernetikë dhe paraqet rreziqe të konsiderueshme për ndërmarrjet federale. JetBrains ka nxjerrë një përditësim të TeamCity duke u kërkuar përdoruesve ta instalojnë atë. Përditësimi gjithashtu rregullon një vulnerabilitet tjetër me rrezik të lartë, duke lejuar aktorët me qëllime keqdashëse të kryejnë veprime të kufizuara të administratorit duke anashkaluar kontrollet e vërtetimit në server.

Link:Lexo më shumë

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039