BULETINI I LAJMEVE TË SIGURISË KIBERNETIKE

Nëntor 2023

Përmbajtja:

Trajnimi "Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës" për Sektorët e Transportit dhe Energjetikës.

Në kuadër të trajnimeve që do të organizohen nga AKCESK për periudhën tetor-dhjetor 2023, në lidhje me ngritjen e kapaciteteve të infrastrukturave kritike dhe të rëndësishme të informacionit, në datat 6 dhe 7 nëntor, në bashkëpunim me Risi Albania u zhvillua trajnimi me temë *"Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës" për Sektorët e Transportit dhe Energjetikës.*

Gjatë këtij trajnimi dy ditor u bënë prezantime lidhur me kuadrin ligjor, strategjinë, politikat, masat e nevojshme të sigurisë që duhet të ndërmerren nga infrastrukturat e informacionit dhe nevojat për qeverisje kibernetike. Pjesë e rëndësishme e këtij trajnimi ishte gjithashtu zhvillimi i 2 Table Top Exercises për menaxhimin e incidenteve dhe krizës Kibernetike, kërcënime kibernetike industriale që përfshijnë sulme mbi sistemet IT, OT dhe IoT, si dhe simulimi i sulmit "Phishing", ku në skenarët e zhvilluar u analizuan raste nga infeksionet Malware (programe keqdashëse). Gjithashtu u organizua Cyber Drill nëpërmjet platformës FISA.al, ku u zhvilluan ushtrime konkrete mbi identifikimin dhe menaxhimin e incidenteve kibernetike. Gjatë diskutimeve u theksua rëndësia e përmirësimit të koordinimit, bashkëpunimit dhe shkëmbimit të informacionit mbi kapacitetet analizuese dhe reaguese të subjekteve në sektorët e Transportit dhe Energjetikës lidhur me incidentet e mundshme në sigurinë kibernetike.

Rritja e kapaciteteve, esenciale për mbrojtjen e infrastrukturave kritike dhe të rëndësishme të informacionit

AKCESK, i fokusuar në rritjen e nivelit të sigurisë kibernetike në infrastrukturat e informacionit në nivel kombëtar, mbështet Operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit, për rritjen e kapaciteteve profesionale dhe teknike.

Duke e konsideruar rritjen e kapaciteteve si një ndër shtyllat esenciale për mbrojtjen e infrastrukturave të informacionit, AKCESK ofron në mënyrë të vazhdueshme ndihmë dhe mbështetje për të gjithë operatorët e këtyre infrastrukturave. Në këtë linjë, u zhvillua me mbështetjen e partnerit tonë Risi Albania/Helvetas dhe kontributin e çmuar të ekspertëve të Autoritetit, aktiviteti i datës 23-24 nëntor me sektorin financiar/bankar.

Aktiviteti dy ditor u përqendrua në zhvillimin e skenarëve të ndryshëm TTX, të dedikuar për këtë sektor dhe pjesëmarrësit u përfshinë në stërvitjen Cyber Drill, duke treguar aftësitë e tyre në zgjidhjen e incidenteve kibernetike mbështetur në procedurat përkatëse.

AKCESK, është gjithmonë i vëmendshëm ndaj përdorimit të teknologjive dhe teknikave të reja, duke ndjekur standardet ndërkombëtare për fushën e sigurisë kibernetike dhe i gatshëm për të mbështetur të gjitha grupet e shoqërisë, për ndërtimin e një ekosistemi kibernetik të qendrueshëm në Shqipëri.

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

BULETINI I LAJMEVE TË SIGURISË KIBERNETIKE

Nëntor 2023

Përmbajtja:

GitHub shton masat e sigurisë me ndihmën e Inteligjencës Artificiale

Platforma GitHub, ka publikuar paraprakisht tre veçori të reja të fuqizuara nga Inteligjenca Artificiale në GitHub Advanced Security.

I disponueshëm për klientët e GitHub Enterprise Cloud dhe Enterprise Server, Advanced Security ofron një sërë veçorish për të ndihmuar në ruajtjen dhe përmirësimin e cilësisë së kodit.

Link:Lexo më shumë

Smasung-data breach

Samsung Electronics njoftoi së fundmi disa nga klientët e saj për një shkelje të të dhënave që ekspozoi informacionin e tyre personal ndaj një individi të paautorizuar.

Kompania thotë se sulmi kibernetik ka ndikuar vetëm tek klientët që kanë bërë blerje online në Mbretërinë e Bashkuar .
Të dhënat e ekspozuara mund të përfshijnë emra, numra telefoni dhe adresë email. Megjithatë kompania thekson se kredencialet dhe informacionet financiare mbeten të paprekura nga incidenti.

Link: Lexo më shumë

Vulnerabiliteti i identifikuar në Sophos Web Appliance është shfrytëzuar aktivisht

CISA ka shtuar tre vulnerabilitete në katalogun e saj të vulnerabiliteteve të shfrytëzuara aktivisht, mes tyre një vulnerabilitet kritik (CVE-2023-1671) në Sophos Web Appliance.

Një shfrytëzim publik PoC për CVE-2023-1671 ka qenë i disponueshëm që nga fundi i prillit, dhe po ashtu një skript që mund të përdoret nga mbrojtësit për të skanuar për pajisje të cënueshme në rrjetin e tyre.

Link: Lexo më shumë

Cisco - patching alert

Cisco ka publikuar së fundmi përditësime lidhur me 27 vulnerabilitete.
Si pjesë e publikimit të saj gjashtëmujor , kompania e teknologjisë publikoi gjithsej 22 këshilla sigurie që përshkruajnë vulnerabilitete të vlerësuara si kritike dhe të mesme .

Gjigandi i teknologjisë njoftoi se deri tani nuk kanë dijeni të ndonjë sulmi që synon ndonjë nga vulnerabilitetet e adresuara.

Link: Lexo më shumë

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