BULETINI I LAJMEVE TË SIGURISË KIBERNETIKE

Tetor 2023

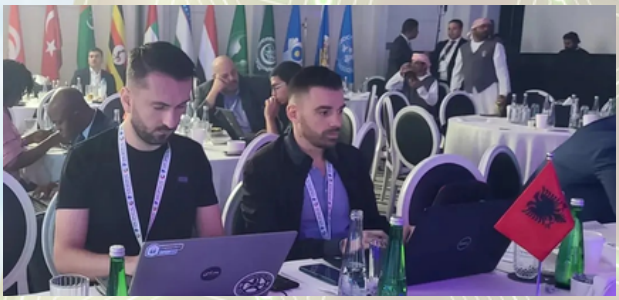
Përmbajtja:

- **Politikat e Sigurisë dhe Menaxhimi i Krizës për Sektorin e Shëndetësisë.**
- **AKCESK pjesmarrës në trajnimin Cyber Week Regional**
- **Finalizohet projekti "Sinjalizues të besuar për një ekosistem kibernetik të sigurtë ndaj ekstremizmit të dhunshëm"**

Politikat e Sigurisë dhe Menaxhimi i Krizës për Sektorin e Shëndetësisë.

Në kuadër të trajnimeve që do të organizohen nga AKCESK për periudhën Tetor-Dhjetor 2023, në datat 11-12 Tetor, u zhvillua trajnimi me temë "Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës " për Sektorët e Shëndetësisë.

Gjatë këtij trajnimi dy ditor u bënë prezantime lidhur me Legjislacionin, Strategjinë, Politikat dhe nevojat mbi Qeverisjen Kibernetike, si dhe u zhvilluan 3 Table Top Exercises për menaxhimin e incidenteve dhe krizës Kibernetike, Simulimi i sulmit "Phishing" si dhe një rast skenari infektimi nga Malware (programe keqdashëse), gjithashtu u organizua një Cyber Drill ku kishte ushtrime konkrete mbi menaxhimin e incidenteve. Gjatë diskutimeve u theksua rëndësia e përmirësimit të koordinimit, bashkëpunimit dhe shkëmbimit të informacionit mbi kapacitetet analizuese dhe reaguese të subjekteve të sektorit shëndetësor lidhur me incidentet e sigurisë kibernetike.



AKCESK pjesmarrës në trajnimin Cyber Week Regional

AKCESK mori pjesë në Cyber Week Regional me ftesë nga Këshilli I Sigurisë Kibernetike të Emirateve të Bashkuara Arabe. Në dy ditët e para u organizua Cyber Drill (Stërvitje Kibernetike) ku kishte përfaqësues nga 70 kombe.

Përfaqësuesit e AKCESK përfaqësuan denjësisht Shqipërinë dhe u klasifikuan si vijon:

Skenari 1 – Log Analysis Web Apps hacked and Crypto mining : Vendi i parë nga 70 vende pjesmarrëse

Skenari 2 – Taktikat e Mbrojtjes për Sigurinë Kibernetike (Vendi I 12);
Skenari 3 – DFIR (Vendi I 9) ;
Skenari 4 – Cyber threat Intelligence (nuk kishte klasifikime) ;
Skenari 5 – CPX Ransomware Technical (Vendi I 11) ;
Skenari 6 - CPX Ransomware MAnagement (nuk kishte klasifikime);
Skenari 7 - Threat Emulation Lead (Vendi I 8);
Skenari 8 – OSINT (Vendi 5);

Finalizohet projekti "Sinjalizues të besuar për një ekosistem kibernetik të sigurtë ndaj ekstremizmit të dhunshëm"

U finalizua me sukses projekti "Sinjalizues të besuar për një ekosistem kibernetik të sigurtë ndaj ekstremizmit të dhunshëm", e organizuar nga Akademia e Studimeve Politike (ASP) në bashkëpunim me Autoritetin Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) me mbështetjen e Ambasadës së Shteteve të Bashkuara të Amerikës në Tiranë.

Rreth 20 pjesëmarrës përfituan njohuri në ciklin e Akademisë së Sinjalizuesve të Besuar, nga ekspertët më të mirë vendas dhe të huaj. AKCESK dhe institucione të tjera shtetërore ofruan praktika dhe trajnime të dedikuara në fushën e sigurisë kibernetike.

Sinjalizuesit e besuar u bënë gjithashtu pjesë e konkursit të monitorimit të përmbajtjeve të paligjshme në internet për një periudhe 4 mujore (prill – korrik 2023), në rrjetet sociale dhe Youtube, ku sinjalizuesi me më shumë raportime iu ofrua një bursë e plotë certifikimi në Data Science, në profilin e kodimit ose sigurisë kibernetike të Academy Coding Dojo inc.

AKCESK, garantoi vijimin e mëtejshëm të formimit dhe bashkëpunimit profesional me rrjetin e Sinjalizuesve të Besuar, për të garantuar një internet më të mirë dhe më të sigurt për fëmijët dhe të rinjtë 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

Tetor 2023

Përmbajtja:

Autoriteti Kombëtar për Cesk organizon trajnime përgatitore së bashku me stafin e Monitorimit të Incidenteve

Sulmet e ransomware, leak data, privilege escalation dhe incidentet e tjera të ndryshimit të informacionit janë përgjegjësi e një sfide të mëtejshme për organizatat dhe jo vetem.

AKCESK ,në kuadër të mbrojtjes së të gjithë Infrastrukturave Kritike dhe të Rëndësishme të Informacionit, kryen rregullisht ushtrime përgatitore dhe simulime të sulmeve së bashku me stafin e Monitorimit të Incidenteve (Albanian National SOC), kjo për të rritur reagimin në rast incidentesh, si dhe monitorimin e sigurisë kibernetike nëpërmjet platformave efikase SIEM apo Threat Intel.

Stafi njihet vazhdimisht me teknikat më të fundit që hakerat përdorin për të thyer sisteme sigurie apo duke anashkaluar mbrojtjet e sistemeve të ndryshme monitoruese, nëpërmjet prezantimeve Table Top Excercise rreth Social Engineering, Ransomware dhe Leak Data si dhe nëpërmjet Cyber Drill.

Mbi 17,000 faqe interneti të WordPress të kompromentuara nga Balada Injector

Më shumë se 17,000 faqe interneti të WordPress janë kompromentuar së fundmi me një malware të njohur si **Balada Injector.**

Nga këto faqe interneti, 9,000 prej tyre mendohet se janë infiltruar duke përdorur një vulnerabilitet të zbuluar së fundmi të identifikuar si: CVE 2023-3169 i cili mund të shfrytëzohet nga përdorues të paautentikuar për të kryer sulme XSS (cross-site scripting).

Link:Lexo më shumë

Google Chrome - patching alert

Google ka publikuar së fundmi Chrome 118 me përditësime për 20 vulnerabilitete, duke përfshirë një vulnerabilitet kritik .

Gjigandi i internetit nuk përmend asnjë nga këto vulnerabilitete të shfrytëzohen në sulme keqdashëse. Versioni i përditësuar i Chrome është 118.0.5993.70 për macOS dhe Linux, dhe si versioni 118.0.5993.70/.71 për Windows.

AKCESK këshillon të gjithë përdoruesit e Google të kryejnë përditësimet e nevojshme.

Link: Lexo më shumë

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