BULETIN JAVOR
5-9 SHKURT 2024

Shprehja e javës

"Si udhëheqës të sigurisë kibernetike, duhet të krijojmë një mesazh influencimi sepse siguria është një kulturë dhe duhet që biznesi të zhvillohet dhe të jetë pjesë e asaj kulture sigurie."

Britney Hommertzheim

Përmbajtja:

- **Konferenca: "Një hapësirë kibernetike më e sigurt për fëmijët"**
- **AKCESK në forcim të kapaciteteve të sigurisë kibernetike**

Konferenca: "Një hapësirë kibernetike më e sigurt për fëmijët"

Në kuadër të "Ditës Ndërkombëtare të Internetit të Sigurt" AKCESK në bashkëpunim me ASHDMF, organizuan Konferencën me temë "Një hapësirë kibernetike më e sigurt për fëmijët". Kjo konferencë u organizua në ambientet e Kryeministrisë, në Qendrën për Hapje dhe Dialog (COD), me datë 6 Shkurt 2024, ku dy drejtuesit e institucioneve z. Igli Tafa dhe znj. Alma Tandili nënshkruan marrëveshjen e bashkëpunimit midis dy institucioneve përgjegjëse në përmbushje të objektivave për mbrojtjen e fëmijëve dhe të rinjve online. Institucionet u angazhuan të zbatojnë një plan të përbashkët veprimi përgjatë vitit 2024, për të realizuar aktivitete dhe fushata të ndryshme ndërgjegjesimi.

Në Konference u zhvillua një diskutimi proaktiv me fëmijët dhe të rinjtë e ftuar nga dy shkolla të Tiranës, shkolla 9 vjeçare Kosova dhe Gjimnazi Sami Frashëri, mbi rreziqet e shumta me të cilat të përballen në hapësirës digjitale, si të mbrohen dhe të raportohen rastet e abuzimit apo shpërndarja e imazheve me përmbajtje të papërshtatshme, si dhe masat që duhet të marrin institucionet përgjegjëse për ndërgjegjësim dhe mbrojtje të fëmijëve.

Në Konferencë mbajtën një fjalë përshëndetëse znj. Bora Muzhaqi Ministër i Shteti për Rininë dhe Fëmijët, znj. Clarisse Pasztory, Kryetarja në detyrë e prezencës së OSBE në Shqipëri, si dhe morën pjesë përfaqësues nga institucione të ndryshme si Ambasada Hollandeze, Ambasada Zvicerane, Policia e Shtetit, Bashkia Tiranë, Alo 116 111, AKEP, AMA, Risi Albania, organizata Save the Children etj, të cilët ndanë eksperiencat e tyre në lidhje me raste ku fëmijë kanë qenë subjekte të abuzimit, bullizimit ose viktima në materiale me përmbajtje të paligjshme të shpërndara online.

AKCESK në forcim të kapaciteteve të sigurisë kibernetike

Në kuadër të krijimit të një ekosistemi kibernetik të sigurt për biznesin në Shqipëri, më datë 31 Janar 2024, u organizua aktiviteti "Cybersecurity Hackathon" me pjesëmarrës nga sektori i biznesit, nën drejtimin e Bashkimit Tregtar Shqiptar me mbështetjen e AKCESK dhe projektit Risi Albania, implementuar nga Helvetas.

Duke konsideruar digjitalizimin e proceseve dhe evoluimin e teknologjive që bizneset përdorin si dhe rritjen e numrit të kërcënimeve të sigurisë kibernetike, zhvillimi i kapaciteteve njerëzore dhe teknike në këtë fushë është thelbësor për të garantuar sigurinë dhe vazhdimësinë e operacioneve të biznesit. Ky aktivitet, i organizuar në formatin e një stërvitje kibernetike, krijoi mundësinë për ekspertët e teknologjisë së informacionit dhe sigurisë kibernetike të bizneseve për të testuar dhe zgjeruar njohuritë e tyre nën udhëheqjen e trajnuesve profesionistë të AKCESK. Stërvitja kibernetike pati në fokus realizimin dhe menaxhimin e sulmeve kibernetike të simuluara, me qëllim zhvillimin e taktikave mbrojtëse për sistemet kryesore të bizneseve në Shqipëri.

Zv. Drejtoresha e Përgjithshme e AKCESK, znj. Floreta Faber, në fjalën e saj përshëndetëse, shprehu mirënjohje për bashkëpunimin me RISI Albania në organizimin e aktiviteteve të përbashkëta dhe theksoi rëndësinë e bashkëpunimit publik-privat për adresimin e sfidave të sigurisë kibernetike në vend. Gjithashtu nënvizoi rolin kyç të AKCESK, për të ofruar mbështetje dhe bashkëpunim të vazhdueshëm ndaj bizneseve dhe të gjithë sektorëve kritikë në Shqipëri, për forcimin e sigurisë kibernetike në nivel kombëtar.

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

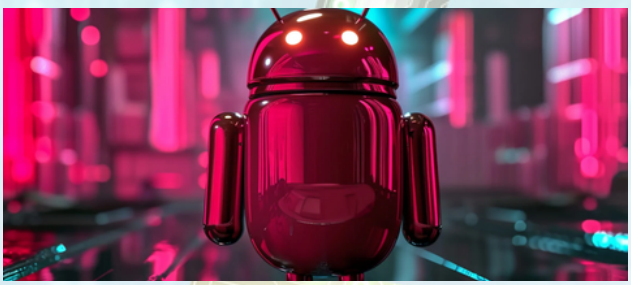
BULETIN JAVOR
5-9 SHKURT 2024

Shprehja e javës

"Si udhëheqës të sigurisë kibernetike, duhet të krijojmë një mesazh influencimi sepse siguria është një kulturë dhe duhet që biznesi të zhvillohet dhe të jetë pjesë e asaj kulture sigurie."

Britney Hommertzheim

Përmbajtja:

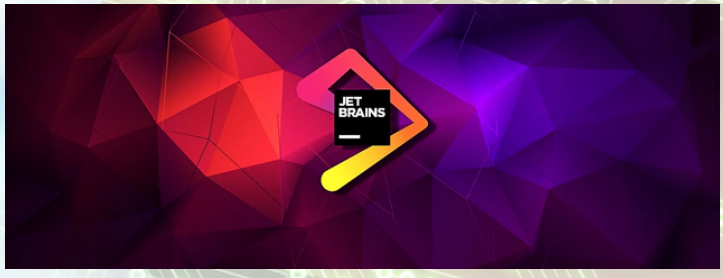


Zbulohet një version i ri i malware-it: Android XLoader

Është zbuluar së fundmi nga studiuesit e sigurisë një version i ri i malware XLoader Android që ekzekutohet automatikisht në pajisjet që ai infekton.

Studiuesit raportojnë se variantet e fundit të XLoader demonstrojnë aftësinë për t'u aktivizuar automatikisht pas instalimit. Kjo lejon që malware të funksionojë fshehurazi në sfond dhe të mbledhë informacione të ndjeshme të përdoruesit.Studiuesit e McAfee sugjerojnë përdorimin e një produkti sigurie që mund të skanojë pajisjen dhe t'i çrrënjosë këto kërcënime.

Link: Lexo më shumë



JetBrain paralajmëron për një vulnerabilitet të ri

JetBrains paralajmëron klientët që të përditësojnë serverët e tyre *TeamCity On-Premises* kundër një vulnerabiliteti kritik , i cili mund t'i lejojë sulmuesit të kenë privilegje administratori.
I identifikuar si CVE-2024-23917, ky vulnerabilitet kritik ndikon në të gjitha versionet e *TeamCity On-Premises* dhe mund të shfrytëzohet në sulmet e ekzekutimit të kodit remote (RCE) .

Të gjithë përdoruesit e *TeamCity On-Premises* këshillohen që të përditësojnë serverët e tyre në versionin 2023.11.3 për të eliminuar vulnerabilitetin

Link: Lexo më shumë

Hyundai- data breach

Prodhuesi i makinave *Hyundai Motor Europe* ka pësuar një sulm ransomware Black Basta, në të cilin aktorët e kërcënimit pretendojnë se kanë vjedhur tre TB të dhëna të korporatës.

Ndërsa nuk dihet se cilat të dhëna janë vjedhur, emrat e dosjeve të aksesuara tregojnë lidhjen e tyre me departamente të ndryshme në kompani, duke përfshirë ligjin, shitjet, burimet njerëzore, kontabilitetin, IT dhe menaxhimin.

Link:Lexo më shumë

PATCHING ALERT

Android- patching alert

Google publikoi *security patch* për Android në shkurt të 2024 për të adresuar 46 vulnerabilitete, duke përfshirë një vulnerabilitet kritik të ekzekutimit të kodit remote i identifikuar si CVE-2024-0031.

Google publikoi nivelin e patch-it të sigurisë të Android 2024-02-01 dhe 2024-02-05 për të rregulluar problemet e gjetura.
Përdoruesit duhet të aplikojnë *security patches* sapo përditësimet e software-it të jenë të disponueshme për ta.

Link:Lexo më shumë

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