BULETINI JAVOR
20-24 NËNTOR 2023

Shprehja e javës

"Në fund të ditës, qëllimet janë të thjeshta: mbrojta dhe siguria."

Përmbajtja:

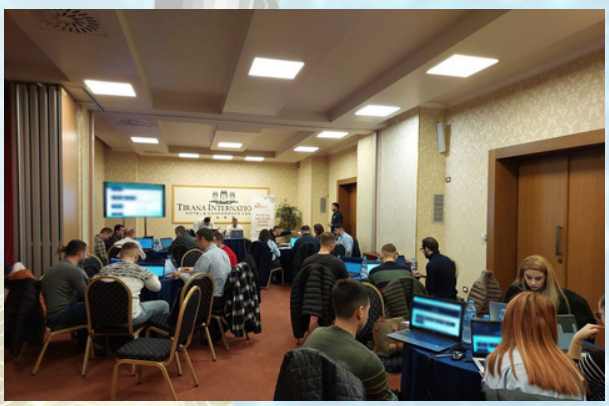
Rritja e kapaciteteve, esenciale për mbrojtjen e infrastrukturave kritike dhe të rëndësishme të informacionit

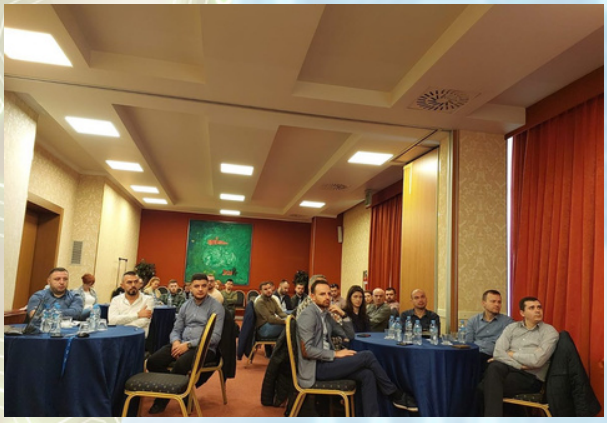
AKCESK, i fokusuar në rritjen e nivelit të sigurisë kibernetike në infrastrukturat e informacionit në nivel kombëtar, mbështet Operatorët e Infrastrukturave Kritike dhe të Rëndësishme të Informacionit, për rritjen e kapaciteteve profesionale dhe teknike.

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 JAVOR
20-24 NËNTOR 2023

Shprehja e javës

"Në fund të ditës, qëllimet janë të thjeshta: mbrojta dhe siguria."

Përmbajtja:

- **Shfrytëzimi i një vulnerabiliteti kritik i Windows Defender bëhet publik**
- **Numri i viktimave të sulmit masiv MOVEit rritet në mbi 2600 firma, 77 milionë njerëz**
- **Vulnerabiliteti i identifikuar në Sophos Web Appliance është shfrytëzuar aktivisht**
- **NJë malware i ri i identifikuar si WailingCrab, po përhapet me shpejtësi përmes emaileve**

Shfrytëzimi i një vulnerabiliteti kritik i Windows Defender bëhet publik

Aktorët e kërcënimit po shfrytëzojnë në mënyrë aktive vulnerabilitetin e identifikuar si: CVE-2023-36025 e tipit zero-day në Windows SmartScreen.

CVE-2023-36025 është vulnerabiliteti i tretë i tipit zero-day në SmartScreen që Microsoft ka zbuluar deri më tani këtë vit. Në shkurt, studiuesit në Google gjetën një aktor kërcënimi që shfrytëzonte një vulnerabilitet të panjohur më parë të SmartScreen për të instaluar ransomware-i *Magniber* në sistemet e synuara. Microsoft e identifikoi vulnerabilitetin si CVE-2023-24880 dhe publikoi një patch për të në mars.

Lexo më shumë

Numri i viktimave të sulmit masiv MOVEit rritet në mbi 2600 firma, 77 milionë njerëz

Sipas studiuesve 2,620 organizata dhe më shumë se 77 milionë individë janë prekur deri më sot, duke marrë njoftime se informacioni i tyre ishte aksesuar, pasi banda ruse e ransomware-it Clop shfrytëzoi një vulnerabilitet për të vjedhur skedarë të ndryshëm .

Antivirusi Avast është ndër viktimat e reja, të cilët së fundi zbuluan se mashtruesit kishin akses në disa "informacione personale me rrezik të ulët të klientëve".

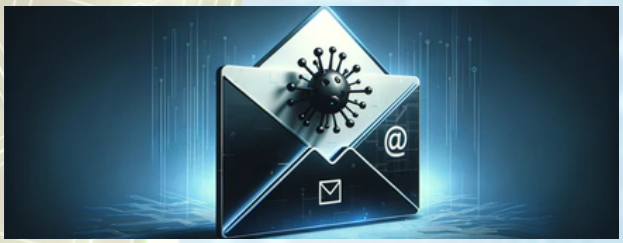
Link: Lexo më shumë

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



NJë malware i ri i identifikuar si WailingCrab, po përhapet me shpejtësi përmes emaileve

Zinxhiri i sulmit fillon me një email që përmban bashkëngjitje PDF e cila përmban URL që kur klikohen, shkarkojnë një skedar JavaScript të krijuar për të ngarkuar malware-in WailingCrab.

I mirëmbajtur në mënyrë aktive nga operatorët e tij, ky malware është vërejtur duke përfshirë veçori që i japin përparësi fshehtësisë dhe e lejon atë t'i rezistojë përpjekjeve analizuese.

Link: Lexo më shumë

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