BULETINI JAVOR
18-22 DHJETOR 2023

Sprehja e javës

"Për të kryer me kompetencë shërbimin e sigurisë, janë të nevojshëm dy elementë kritikë të reagimit ndaj incidentit: informacioni dhe organizimi."

Robert Davis

Përmbajtja:

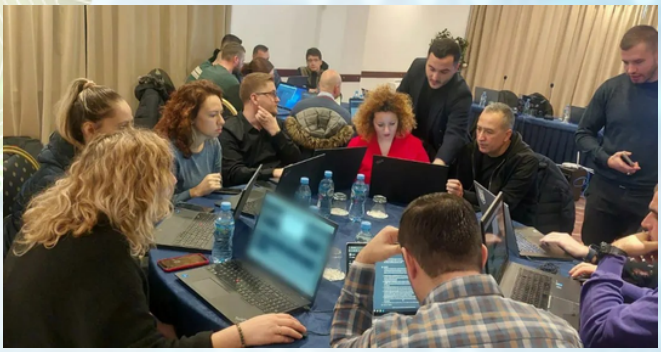
- **"Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës" për Institucionet e Pavaruara, Sektorin UK, AKSHI dhe Policinë e Shtetit.**

"Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës" për Institucionet e Pavaruara, Sektorin UK, AKSHI dhe Policinë e Shtetit.

Në vazhdim të objektivës së AKCESK për rritjen e kapaciteteve si një ndër shtyllat kryesore për mbrojtjen e infrastrukturave të informacionit me mbështetjen e partnerit tonë Risi Albania/Helvetas dhe kontributin e çmuar të ekspertëve të Autoritetit, zhvilloi në datat 20, 21 dhe 22 Dhjetor 2023, trajnimin e parashikuar me temë "Politikat e Sigurisë Kibernetike dhe Menaxhimi i Krizës" për Institucionet e Pavaruara, Sektorin UK, AKSHI dhe Policinë e Shtetit.

Për vetë rëndësinë që këta sektor kanë përsa i përket infrastrukturave të informacionit që ata administrojnë, gjatë këtij trajnimi tre 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 zhvillimin i tre skenarëve të ndryshëm TTX, për menaxhimin e incidentit kibernetik. Gjithashtu u zhvilluan 2 ditë stërvitje kibernetike (Cyber Drill) me ushtrime konkrete mbi menaxhimin e incidentit kibernetik, nëpërmjet platformës FISA.al.



Në përmbushje të objektivave për të arritur standartet ndërkombëtare në fushën e sigurisë kibernetike, AKCESK do të vazhdoje të organizojë trajnime për të gjithë sektorët që administrojnë infrastruktura kritike dhe të rëndësishme të informacionit me qëllim ndërtimin e një ekosistemi kibernetik të qëndrueshëm në Shqipëri.

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

BULETINI JAVOR
18–22 DHJETOR 2023

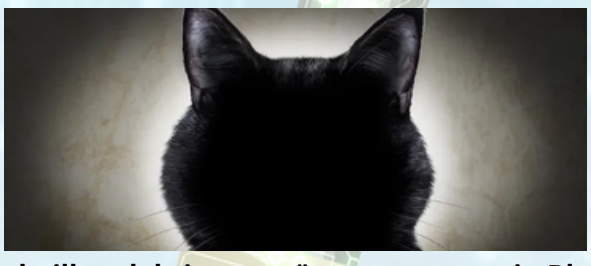
Sprehja e javës

"Për të kryer me kompetencë shërbimin e sigurisë, janë të nevojshëm dy elementë kritikë të reagimit ndaj incidentit: informacioni dhe organizimi."

Robert Davis

Përmbajtja:

- **FBI zhvillon dekriptues për ransomware-in BlackCat**
- **Xfinity - data breach**
- **Një sulm i ri phishing vjedh kodet rezervë në Instagram**
- **Google - patching alert**



FBI zhvillon dekriptues për ransomware-in BlackCat

FBI ka krijuar një mjet deshifrimi për ransomware-in e përdorur nga banda e njohur si BlackCat ose AlphV, si pjesë e një fushate të gjerë kundër mashtruesve kibernetik.

Ekzistenca e dekriptuesit u zbulua në një njoftim nga Departamenti i Drejtësisë i Shteteve të Bashkuara që raporton se FBI ua ka ofruar dekriptuesin mbi 500 organizatave që ishin sulmuar duke bërë të mundur shmangien e pagesës së shpërblesës.

Lexo më shumë

Një sulm i ri phishing vjedh kodet rezervë në Instagram

Një fushatë e re phishing që pretendon të jetë një email me subjekt "shkelje e të drejtës së autorit" përpiqet të vjedhë kodet rezervë (backup codes) të përdoruesve të Instagram, duke lejuar hakerat të anashkalojnë autentifikimin me dy faktorë të konfiguruar në llogari.

Emailet më të fundit të phishing imitojnë Metën, kompaninë mëmë të Instagramit, duke paralajmëruar se përdoruesit e Instagramit kanë marrë ankesa për shkelje të të drejtave të autorit. Email-i më pas kërkon përdoruesin të plotësojë një formular për të zgjidhur problemin.

Link: Lexo më shumë

Xfinity - data breach

Kompania e telekomunikacionit Xfinity ka zbuluar së fundmi se sulmuesit kibernetik që shkelën një nga serverët e tij Citrix vodhën gjithashtu informacione të ndjeshme ndaj klientit nga sistemet e saj duke prekur 35,879,455 njerëz.

Xfinity thotë se u ka kërkuar përdoruesve të rivendosin fjalëkalimet e tyre dhe të aktivizojnë autentifikimin me dy ose me shumë faktorë për të mbrojtur llogaritë e prekura.

Link: Lexo më shumë

PATCHING ALERT

Google - patching alert

Google ka publikuar një përditësim urgjent për të adresuar një vulnerabilitet të ri të tipit zero-day, të identifikuar si CVE-2023-7024, në shfletuesin Chrome.

Vulnerabiliteti është adresuar me publikimin e versionit 120.0.6099.129 për Mac, Linux dhe 120.0.6099.129/130 për Windows, i cili do të dalë gjatë ditëve/javëve në vijim.

Link: Lexo më shumë

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