BULETIN JAVOR
19-23 QERSHOR
2023

Shprehja e javës

"Siguria kibernetike është një përgjegjësi sociale. Të gjithë kemi një rol për të luajtur."

Siguria kibernetike në sektorin bankar

"Numrat e sigurimeve shoqërore, llogarive bankare dhe kartave të kreditit nuk janë vetëm të dhëna. Në duar të gabuara ata mund të fshijnë kursimet e jetës së dikujt, të shkatërrojnë kredinë e tyre dhe të shkaktojnë shkatërrim financiar."

Melissa Bean

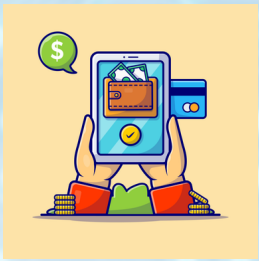
Me ofrimin gjithnjë e në rritje të sherbimeve bankare, ndërgjegjësimi i ketij sektori për sigurinë kibernetike është një proces kritik.
Në mbarë botën, bankat dhe institucionet financiare janë objekt i shpeshtë i sulmeve kibernetike; siç janë hakerimi i të dhënave të klientëve, vjedhja e identitetit, mashtrimi financiar dhe shfrytëzimi i dobësive në infrastrukturën e tyre të informacionit.
Pikërisht, sektori bankar ka qenë ketë javë në vëmendjen e shtuar të AKCESK, për të intesifikuar bashkëpunimin në terma të ndërgjegjësimit dhe rritjes së vigjilences, në funksion të mbrojtjes kibernetike të infrastrukturave të informacionit.
Prioritizimi i rritjes së kapaciteteve dhe shkëmbimi i informacionit në kohë reale kanë qenë pjesë e diskutimeve dhe takimeve të përditshme, që AKCESK ka zhvilluar gjatë kësaj jave, me ketë sektor.

"Ne jemi aty, sëbashku me ju, për t'ju pergjigjur 24/7 dhe për të adresuar të gjitha cështjet tuaja lidhur me sigurine kibernetike"- tha Drejtori i Përgjithshem i autoritetit, në takimet e drejtuara nga vete ai.
"Misioni ynë është i qartë; së bashku të ndertojmë një ekosistem kibernetik të sigurt për të gjithë, në Shqipëri"

Këshilla për të mbajtur të sigurt informacionin tuaj financiar

1. Mos i ndani sekretet tuaja.
Mos i jepni numrin tuaj të Sigurimeve Shoqërore ose informacionin e llogarisë kujtdo që ju kontakton në internet ose përmes telefonit. Mbroni kodet PIN dhe fjalëkalimet tuaja dhe mos i ndani ato me askënd.

2. Grisni letrat me përmbajtje sensitive.
Prisni faturat, deklaratat bankare dhe ofertat e kartave të kreditit të papërdorura përpara se t'i hidhni ato.



3. Përdorni platformen online të bankave për të mbrojtur veten.
Monitoroni rregullisht llogaritë tuaja financiare për transaksione mashtruese.

4. Monitoroni raportin tuaj të kreditit.
Porositni një kopje falas të raportit tuaj të kreditit çdo katër muaj

5. Mbroni kompjuterin tuaj.

Sigurohuni që antivirusi në kompjuterin tuaj të jetë aktiv dhe i përditësuar. Kur kryeni biznes në internet, sigurohuni që ikona e çelësit të shfletuesit tuaj të jetë aktive. Kërkoni gjithashtu një "s" pas "http" për t'u siguruar që faqja e internetit është e sigurt.

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

BULETIN JAVOR
19-23 QERSHOR
2023

Shprehja e javës

"Siguria kibernetike është një përgjegjësi sociale. Të gjithë kemi një rol për të luajtur."

Përmbajtja:

- Hackerët shënjestrojnë serverët Linux SSH duke përdorur sulme Tsunami DDoS
- Loja e trojanizuar Super Mario e përdorur për të instaluar malware të Windows
- ChatGPT Data breach CFortinet -
- Patching Alert

Hackerët shënjestrojnë serverët Linux SSH duke përdorur sulme Tsunami DDoS

Një fushatë sulmi është zbuluar kohët e fundit, ku serverët Linux SSH të keqkonfiguruara janë në shënjestër duke u sulmuar me Tsunami DDoS Bot.

Kur përdoruesit përdorin informacione bazë si emri i përdoruesit dhe fjalëkalimi,Linux mund të lejojë një person të jashtëm të hyjë në sistem duke hamendësuar me forcë ose duke përdorur një listë të parapërgatitur fjalëkalimesh të zakonshme.

Pasi hyjnë në sistem, sulmuesi ekzekuton një komandë për të shkarkuar lloje të ndryshme malware. Një nga malware-ët e instaluar është një skript i quajtur skedari "kyç", i cili vepron si një shkarkues dhe instalon më shumë malware.

Për të gjithë përdoruesit e Linux këshillohet që të përdorin fjalëkalime të forta ose çelësa SSH për t'u mbrojtur nga sulmet si edhe të ndërmarrin hapat e nevojshëm për të kufizuar aksesin në server duke lejuar vetëm një gamë specifike të adresave IP.

Link: Lexo më shumë

Loja e trojanizuar Super Mario e përdorur për të instaluar malware të Windows

Një instalues i trojanizuar për lojën popullore Super Mario 3: Mario Forever për Windows ka infektuar pajisjet e shumë lojtarëve me infeksione të shumta malware.Loja e infektuar është promovuar në forumet e lojërave, grupet e mediave sociale duke bërë të mundur instalimin nga shumë lojtarë.Të dhënat e vjedhura përfshijnë informacione të ruajtura në shfletuesit e uebit, si fjalëkalime dhe *cookies* të ruajtura që përmbajnë kredenciale për Discord, Minecraft, Roblox dhe Telegram.

Këshillohet për të gjithe dashamirësit e lojrave se kur shkarkoni lojëra ose ndonjë softuer, sigurohuni që ta bëni këtë nga burime zyrtare si faqja e internetit e botuesit ose platformat e besueshme të shpërndarjes së përmbajtjes dixhitale.

Gjithmonë skanoni ekzekutuesit e shkarkuar duke përdorur programin tuaj antivirus përpara se t'i lançoni ato dhe mbani të përditësuara mjetet tuaja të sigurisë.

Link:Lexo më shumë

Mbi 100,000 llogari ChatGPT të vjedhura përmes sulmeve malware

Më shumë se 101,000 llogari përdoruesish ChatGPT janë vjedhur nga sulmet malware , sipas të dhënave të *darkweeb*

Këto lloje malware janë të njohur për vjedhjen e kredencialeve të ruajtura në shfletuesit e uebit duke i nxjerrë ato nga baza e të dhënave SQLite.Këto kredenciale, dhe të dhëna të tjera të vjedhura, përdoren nga sulmuesi për qëllime keqdashëse

Këshillohet qe punojnë me informacione jashtëzakonisht të ndjeshme nuk duhet t'i besojnë futjes së tij në ndonjë shërbim të bazuar në renë kompjuterike, por vetëm në mjete të siguruara të ndërtuara në vend dhe të vetë-strehuara.

Link: Lexo më shumë

PATCHING ALERT

Përditësim sigurie nga Kompania Fortinet mbi një vunerabilitet të vlerësuar si kritik

Kompania e zgjidhjeve të sigurisë kibernetike Fortinet ka përditësuar së një vulnerabilitet që sulmuesit mund të përdorin për të ekzekutuar kode dhe komanda.

Vulnerabiliteti identifikohet si CVE-2023-33299 i vlerësuar si mjaft kritik dhe mund të cojë në ekzekutimin e kodit në distancë (remote).

Kompania nuk ka dhënë asnjë këshillë për zbutjen e defektit, kështu që veprimi i rekomanduar është të zbatohen përditësimet e disponueshme të sigurisë.

Link:lexo më shumë

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