BULETIN JAVOR
10-14 KORRIK 2023

Shprehja e javës

"Kur funksionaliteti është gjithçka që ka rëndësi, siguria shpesh neglizhohet."

Përmbajtja:

- Fëmijë të sigurtë onlinë
- Ballkani Perëndimor: Bashkëpunimi Transatlantik dhe Rajonal- Ndërtimi i Aleancave të Forta
- Workshop: "Qeverisja e krizës kibernetike"

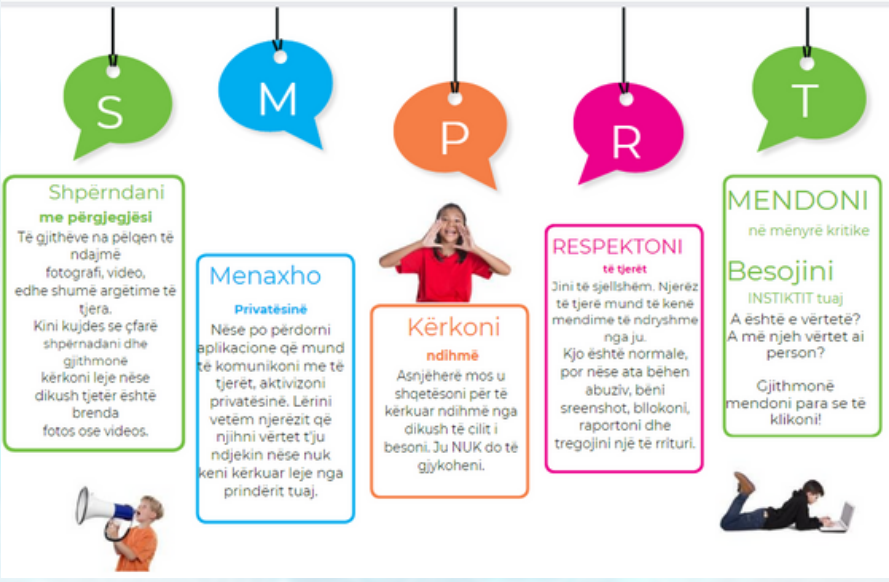
Fëmijë të sigurtë onlinë

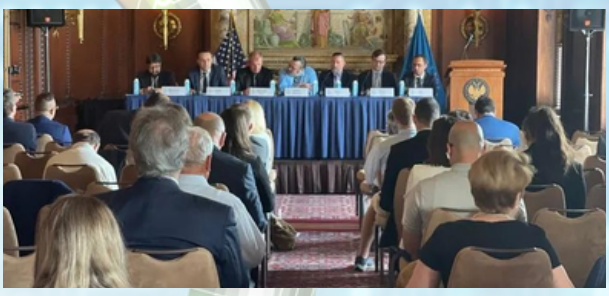
"Interneti është një mjet i shkëlqyeshëm informacioni dhe mund të jetë një vend ku fëmijët mësojnë, por ne duhet të kujtojmë se kur fëmijët janë online, ata janë në publik."

Mark Kennedy

Cdo ditë, më shumë se 175,000 fëmijë hyjnë online për herë të parë- pra një fëmijë çdo gjysmë dite.
Ky aksesor dixhital i ekspozon fëmijët për një numër të madh përfitimesh dhe mundësish, por gjithashtu një mori rreziqesh dhe dëmesh, për përmbajtjen e dëmshme, abuzimin seksual dhe shfrytëzimin, cyberbullying dhe keqpërdorimin e informacionit privat.

Mbrojtja e fëmijëve online si një nga ***shtyllat kryesore të strategjisë së sigurisë kibernetike***, është në fokus të vazhdueshëm të AKCESK duke rritur ndërgjegjësimin e vazhdueshëm në Shqipëri për të përmbushur përgjegjësinë e plotë në formimin e një bote më të sigurt dixhitale për fëmijët.





Ballkani Perëndimor: Bashkëpunimi Transatlantik dhe Rajonal- Ndërtimi i Aleancave të Forta

Në datën 13 korrik në Washington, D.C , u organizua Konferenca Ballkani Perëndimor: Bashkëpunimi Transatlantik dhe Rajonal - Ndërtimi i Aleancave të Forta.
Konferenca mblodhi përfaqësues të rëndësishëm, me qëllim bashkëpunimin rajonal , i cili është thelbësor për vendet e Ballkanit Perëndimor në progresin e procesit të stabilizim asocimit në BE.
Gjatë sesionit "Cyber Security in the Western Balkans: Meeting the Challenges" Shqipëria, përfaqësuar nga Drejtori i Përgjithshëm i AKCESK Z. Igli Tafa, prezantoi sfidat e sigurisë duke rikujtuar sulmin e një viti më parë drejtuar Shqipërisë , ne të cilin u përvetësuan dy terma kryesore: terma teknologjik ku fokus ka qenë rritja e kapacitetve teknologjike si dhe terma strategjik ku në fokus ka qenë ngritja e kapaciteteve njerëzore.
Gjithashtu, në vijim të diskutimeve të këtij sesioni, kreu i AKCESK theksoi suportin e partnerëve strategjik dhe rëndësinë e bashkëpunimeve të vazhdueshme për të përballuar në mënyrë të qëndrueshme situata kritike.
Konferenca vijoi diskutimet duke adresuar sfidat, sulmet e vazhdueshme kibernetike ndaj institucioneve dhe individëve publikë dhe privatë dhe cilat janë masat e duhura për tu ndërmarrë në terma strategjik dhe bashkëpunimi ndërkombëtarë.

Workshop: "Qeverisja e krizës kibernetike"

Në kuadër të zhvillimit të kapaciteteve të infrastrukturave të informacionit, AKCESK në bashkëpunimin me CRDF Global dhe C3I organizuan workshopin mbi "Qeverisjen e krizës kibernetike".
Qëllimi i workshopit ishte fuqizimi i bashkëpunimit ndërsektorial në terma të qeverisjes së krizës kibernetike në nivel kombëtar, nëpërmjet skenarëve të dedikuar fiktivë.

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

BULETIN JAVOR
10-14 KORRIK 2023

Shprehja e javës

"Kur funksionaliteti është gjithçka që ka rëndësi, siguria shpesh neglizhohet."

Përmbajtja:

- CISA u jep afat agjencive civile amerikane deri më 1 gusht për të zgjidhur katër dobësi të Microsoft
- Sulmet e malware të USB drive po rriten përsëri në gjysmën e parë të 2023
- ING Bank - Data breach
- Apple - Patching Alert

CISA u jep afat agjencive civile amerikane deri më 1 gusht për të zgjidhur katër dobësi të Microsoft

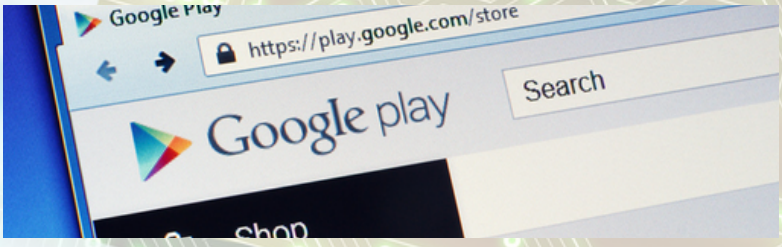
Agjencia e Sigurisë Kibernetike dhe Sigurisë së Infrastrukturës (CISA) u ka dhënë afat agjencive civile federale të SHBA-së deri më 1 gusht për të zgjidhur katër vulnerabilitete serioze zero-day të shpallura si pjesë e lëshimit mujor të Microsoft Patch Tuesday

Përfshirja e katër vulnerabiliteteve - CVE-2023-32046, CVE-2023-32049, CVE-2023-35311, CVE-2023-36874 - në katalogun e CISA do të thotë se dobësitë tashmë janë duke u shfrytëzuar nga hakerat.Katër dobësitë e përmendura të Microsoft janë ndër më shumë se 130 të shpallura nga gjigandi i teknologjisë të martën

Microsoft konfirmoi se vulnerabilitetet ishin duke u shfrytëzuar dhe preknin të gjitha versionet e Microsoft Outlook nga viti 2013 e tutje.

Përveç njoftimeve të Microsoft, disa kompani të tjera, duke përfshirë Apple, Google, SAP, Fortinet, Adobe dhe Cisco, publikuan këshilla për dobësitë e tyre.

Lexo më shumë



Sulmet e malware të USB drive po rriten përsëri në gjysmën e parë të 2023

Studiuesit kanë arrotur të zbulojnë dy fushata malware të ekzekutuar nëpërmjet USB ; njëra me emrin "Sogu", që i atribuohet një grupi kërcënimi spiunazhi kinez "TEMP.HEX" dhe një tjetër me emrin "Snowydrive", që i atribuohet UNC4698, e cila synon firmat e naftës dhe gazit në Azi.

Shumica e viktimave i përkasin sektorëve farmaceutikë, IT, energjisë, komunikimit, shëndetësisë dhe logjistikës, por ka viktima në të gjithë bordin.

Sogu është aktualisht fushata më agresive e spiunazhit kibernetik e asistuar nga USB, duke synuar shumë industri në mbarë botën dhe duke u përpjekur të vjedhë të dhëna nga kompjuterët e infektuar.

Ndërsa sulmet USB kërkojnë qasje fizike në kompjuterët e synuar për të arritur infeksionin, ato kanë avantazhe unike që i mbajnë ato të rëndësishme dhe në trend në 2023

Lexo më shumë

ING Bank- ka konfirmuar se informacionet e një pjese të klientëve të saj janë aksesuar nga hakerat përgjegjës për një sërë sulmesh globale që shfrytëzojnë sistemin e transferimit të skedarëve MOVEit

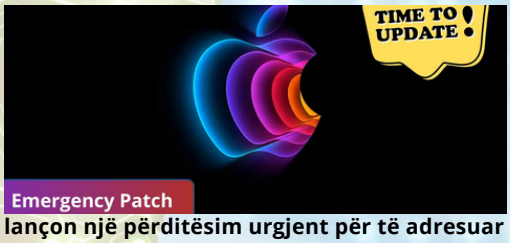
MOVEit është një kompani Amerikane që mundëson transmetimin e të dhënave në mënyre të sigurt midis kompanive dhe sistemeve të ndryshme anembanë botës. Sulmet janë kryer nga grupi kriminal kibernetikë Cl0p , i cili përdor metoda shantazhi të dyfishtë. Duke shtazhuar viktimat e tyre se pari për dekriptimin e të dhënave, e me pas për të mos publikuar të dhëna konfidenciale.

Personat e paautorizuar fituan akses në të dhënat personale që ofruesi i shërbimit përpunon me qëllim të ndërrimit të llogarive

ING tha se çdo klient i prekur do të informohet nga banka "me shkrim" për incidentin.Njoftimi i bankës do të sigurojë gjithashtu "udhëzime sigurie" për klientët e prekur për të mbrojtur më tej informacionin e tyre personal, si dhe "opsionet e kontaktit për pyetje".“Cenueshmëria përkatëse e sigurisë u mbyll nga ofruesi i shërbimit dhe autoritetet përkatëse për mbrojtjen e të dhënave dhe autoritetet e zbatimit të ligjit u informuan për incidentin.

Lexo më shumë

PATCHING ALERT



Apple lançon një përditësim urgjent për të adresuar një defekt në iOS dhe macOS

Apple sapo ka publikuar për përdoruesit e saj një përditësim urgjent për të rregulluar hapësirat e zbuluara në sistemet e sigurisë të IOS dhe MAC.

Dobësia u zbulua në motorin e shfletuesit WebKit të Apple dhe i lejon sulmuesit të marrin ekzekutimin arbitrar të kodit në pajisjet e synuara duke mashtruar përdoruesit për të hapur faqet e internetit me informacione të krijuara me qëllim keqdashës.

Përdoruesit e IOS dhe MAC të bëjnë sa me shpejt përditësimet e nevojshme dhe të mbajnë të aktivizuar në aparatet e tyre opsionin e përditësimeve automatike.

AKCESK rekomandon të gjithë përdoruesit e apple të kruejne përditësimet e nevojshme

Lexo më shumë

Rruga "Papa Gjon Pali II", No.3 info@cesk.gov.al

Autoriteti Kombëtar për CESK

autoriteti_kombetar_cesk

+35542221039