# BULETIN JAVOR
# 17-21 KORRIK 2023

Shprehja e javës

*"Të argumentosh se nuk të intereson e drejta e privatësisë sepse nuk ke asgjë për të fshehur nuk është ndryshe nga të thuash se nuk të intereson liria e fjalës sepse nuk ke çfarë të thuash."*

Përmbajtja:

- **Siguria kibernetike në sektorin Akademik**
- **Workshopi: "Cyber Defence Strategy Development"**

## Siguria kibernetike në Sektorin Akademik

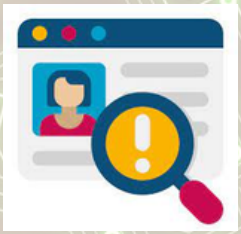
***"Studentët lindin praktikisht me teknologjinë në duart e tyre, por nuk kanë mjaftueshëm informacion për sigurinë"***

***CISO nga një universitet i madh në Kanada.***

Ndërsa mësimi online është përhapur shumë dhe ofron kaq shumë mundësi pozitive për nxënësit dhe mësuesit, është më e rëndësishme se kurrë të forcohen mbrojtjet e sigurisë kibernetike për të përballur sulmet e reja dhe ato në zhvillim.

Sulmuesit kibernetikë po zbulojnë vazhdimisht shfrytëzime dhe strategji të reja për të kompromet uar përdoruesit. Këtu janë pesë praktikat më të mira të sigurisë kibernetike për studentët, për t'ju ndihmuar të mbroheni prej tyre:

**1. Shmangni ndarjen e informacionit personal:**
Jini të vëmendshëm për informacionin që zbuloni në internet – si emrin e shkollës, adresën e emailit, adresën e shtëpisë dhe numrat e telefonit.



**2.Investoni në mbrojtjen nga viruset:**
Sigurohuni që të keni antivirus të instaluar në të gjitha pajisjet (desktop, laptop, tablet, etj.). Vendoseni atë të përditësohet automatikisht dhe ekzekutoni skanimet e viruseve të paktën një herë në javë.

**3. Mbani softuerin të përditësuar:**
Sigurohuni që të mbani sistemin tuaj operativ, dhe aplikacionet të përditësuara plotësisht .


**4.Jini të kujdesshëm për sulmet phishing:**
Mos hapni bashkëngjitjet në email nga burime jo legjitime. Ju mund të merrni email nga anëtarët e grupit ose mësuesit, por kini kujdes kur hapni ndonjë bashkëngjitje.

**5. Jini të kujdesshëm se çfarë klikoni:**
Shmangni vizitën e faqeve të panjohura të internetit ose shkarkimin e softuerëve nga burime të pabesueshme. Këto sajte mund të kenë malware që i kompromet ojnë kompjuterin tuaj.


## Workshopi: "Cyber Defence Strategy Development"

Në datat 18-21 Korrik 2023, Instituti për Qeverisjen e Sigurisë i Agjencisë së Bashkëpunimit të Sigursë së Mbrojtjes së SHBA-së, organizoi pranë ambjenteve të Shtabit të Përgjithshëm të Forcave të Armatosura, workshopin "Cyber Defence Strategy Development".

Pjesëmarrës në këtë workshop ishin përfaqësues nga Ministria e Mbrojtjes, Shtabi i Përgjithshëm i Forcave të Armatosura, Njësia Ushtarake e Sigurisë Kibernetike, Agjencia Kombëtare e Shoqërisë së Informacionit dhe AKCESK.

Qëllimi i workshopit ishte zhvillimi dhe zbatimi i strategjisë së mbrojtjes kibernetike, për të mbështetur misionin dhe harmonizuar prioritetet, strukturat, vendimet dhe objektivat e Ministrisë së Mbrojtjes, për mbrojtjen e hapësirës kibernetike shqiptare.


Në kuadër të ngritjes së kapaciteteve teknike të Infrastrukturave Kritike, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike mori pjesë në trajnimin katër ditor të zhvilluar nga USEA dhe Catalisto së bashku me asistimin e USAID në Tiranë.

Fokusi i programit ishte thellimi i njohurive të avancuara në menaxhimin e incidenteve kibernetike në infrastrukturat publike dhe private në Shqiperi si dhe vlerësimin e implementimit të masave të sigurisë bazuar në standardet më të njohura ndërkombëtare.

Pjesëmarrja aktive në këtë trajnim i shërben AKCESK drejtpërdrejt në krijimin e kapaciteteve të qëndrueshme për të adresuar krizat e mundshme përmes forcimit të strategjive, inovacionit dhe sigurinë kibernetike.

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

# BULETIN JAVOR
# 17-21 KORRIK 2023

Shprehja e javës

*"Të argumentosh se nuk të intereson e drejta e privatësisë sepse nuk ke asgjë për të fshehur nuk është ndryshe nga të thuash se nuk të intereson liria e fjalës sepse nuk ke çfarë të thuash."*

Përmbajtja:



**Microsoft: Hakerët i kthejnë serverët Exchange në qendra kontrolli malware**

Microsoft paralajmëron për sulme të reja nga grupi i hakerëve Turla i sponsorizuar nga shteti rus, të cilët synojnë industrinë e mbrojtjes dhe serverët e Microsoft Exchange duke përdorur një backdoor malware të ri 'DeliveryCheck'.

Sulmet fillojnë me email phishing i cili përmban bashkëngjitur dokumente në EXEL që përmbajnë makro kedashëse. Kur aktivizohen, këto makro ekzekutojnë një komandë PowerShell, duke krijuar në këtë mënyrë një rrjedhë detyrash të planifikuara të cilat imitojnë shfletuesin Firefox.

Ky malware është një mjet spiunazhi kibernetik që lejon aktorët e kërcënimit të lëshojnë javascript në pajisje, të vjedhin të dhëna nga regjistrat e ngjarjeve, të vjedhin informacione në lidhje me skedarët e sistemeve dhe të vjedhin kredencialet nga një shumëllojshmëri programesh, duke përfshirë shfletuesit, klientët FTP, softuerin VPN, KeePasok, Outlook, Az, dhe Azure.

[Lexo më shumë]


**GitHub paralajmëron për hakerat e Lazarus**

GitHub paralajmëron për një fushatë sulmi që përdorin inxhinierinë sociale dhe synon llogaritë e zhvilluesve në sektorët e blockchain, kriptomonedhës, lojërave të fatit në internet dhe sektorët e sigurisë kibernetike për të infektuar pajisjet e tyre me malware.

Sipas GitHub Lazarus Group po komprometon llogaritë legjitime ose po krijon persona të rremë që pretendojnë se janë zhvillues dhe rekrutues në GitHub dhe media sociale.

Pasi viktimat i besojnë ata, aktorët e kërcënimit i ftojnë të bashkëpunojnë në një projekt gjatë të cilit shkarkojnë malware në pajisjet e viktimave.

Një fushatë e ngjashme u krye në mars 2021 ku hakerët krijuan një faqe interneti për një kompani të rreme të quajtur SecuriElite dhe e përdornin për të infektuar pajisjet e viktimave me malware

[Lexo më shumë]

**VirusTotal ekspozon disa detaje të klientëve të regjistruar**

Të dhënat e lidhura me një nëngrup klientësh të regjistruar të VirusTotal, duke përfshirë emrat dhe adresat e tyre të emailit, u ekspozuan pasi një punonjës ngarkoi pa dashur informacionin në platformën e skanimit të malware.

I lançuar në vitin 2004, VirusTotal është një shërbim popullor që analizon skedarët dhe URL-të e dyshimta për të zbuluar llojet e malware dhe përmbajtjeve me qëllim të keq duke përdorur motorë antivirus dhe skaner të faqeve të internetit.

VirusTotal kërkoi ndjesë për incidentin e fundit të ekspozimit të të dhënave të klientit, duke deklaruar se ai u shkaktua nga një punonjës që ngarkoi aksidentalisht një skedar CSV në platformë më 29 qershor 2023, që përmbante informacione në lidhje me klientët e llogarisë së tij Premium, veçanërisht emrat e tyre,dhe adresat e emailit të administratorëve të grupit.

[Lexo më shumë]

## PATCHING ALERT


**Oracle lançon 508 përitësime të reja sigurie**

Oracle publikoi së fundmi 508 *patching alerts* të sigurisë në të cilat më shumë se 350 adresojnë vulnerabilitete që mund të shfrytëzohen remote, pa autentifikim. Disa nga këto dobësi ndikojnë në produkte të shumta.

Gjigandi i teknologjisë lëshoi gjithashtu buletinin Solaris të korrikut 2023, i cili përfshin 17 *patching* sigurie, duke përfshirë 11 për dobësitë që janë të shfrytëzuara remote si dhe njoftoi gjithashtu lëshimin e 42 *patching* të sigurisë si pjesë e buletinit të tij Linux të korrikut 2023.

Klientët këshillohen të aplikojnë patchet e disponueshme në kohën e duhur, ose të bllokojnë aksesin në rrjet në aplikacionet e papatchuara, për të zvogëluar rrezikun e një sulmi.

[Lexo më shumë]


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