BULETIN JAVOR
15-19 PRILL 2024

Shprehja e javës

"Informacioni është oksigjeni i epokës moderne. Ai depërton nëpër muret me tela me gjemba, ai përhapet përtej kufijve të elektrizuar."

Ronald Reagan

Përmbajtja:

Shqipëria, anëtare e besueshme e NATO-s për stabilitet e siguri

Në takimin me delegacionin e Komisionit për Demokraci dhe Siguri të Asamblesë Parlamentare të NATO-s, pranë Kryesisë së Kuvendit Shqiptar, z. Igli Tafa, Drejtor i Përgjithshëm i Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurisë Kibernetike (AKCESK), në fjalën e tij ndau arritjet e Shqipërisë në përmirësimin e hapësirës kibernetike. Në këtë takim u theksua mungesa e ekspertëve të sigurisë kibernetike dhe roli i Autoritetit në reduktimin e këtij boshllëku përmes një plani të qartë trajnimesh.

U prezantuan gjithashtu nevojat teknologjike dhe një sërë përpjekjesh për të rritur standardet në ekosistemin kibernetik të Shqipërisë. Një vend të veçantë në këtë diskutim zunë edhe sulmet kibernetike drejt vendit tonë si dhe marrja e masave të nevojshme për rritjen e rezistencës kibernetike.

Z. Franc Zylyftari, Shefi i Departamentit të Sigurisë Kibernetike pranë National Agency of Information Society/Agjencia Kombëtare e Shoqërisë së Informacionit, solli në vëmendje principin 'Zero Trust' që përdor AKSHI për mbrojtjen e hapësirës kibernetike qeveritare shqiptare ndaj kërcënimeve të huaja kibernetike. Ky model sigurie përqëndrohet në mbrojtjen e hapësirës kibernetike shqiptare nga kërcënimet transnacionale dhe ndërhyrjet e huaja.

Takimi i AKCESK me përfaqësues të USAID & CPR

AKCESK ka zhvilluar një takim të frytshëm me përfaqësues të USAID Europe & Eurasia dhe përfaqësues të Programit CPR, të fokusuar në zhvillimin e strategjive të efektshme në cloud, si dhe në fuqizimin e kapaciteteve institucionale, veçanërisht të SOC Kombëtar.

Ky bashkëpunim shënon një hap të rëndësishëm në implementimin e asistencës teknike dhe strategjike nga partneri ynë strategjik, SHBA, si dhe dëshmon angazhimin e AKCESK për rritjen e nivelit të sigurisë në infrastrukturat e informacionit në nivel kombëtar.

Pjesëmarrja aktive e AKCESK në aktivitetin e OSCE mbi "Klasifikimin kombëtar të incidenteve kibernetike"

Pjesëmarrja aktive e AKCESK në aktivitetin e OSCE mbi "Klasifikimin kombëtar të incidenteve kibernetike" përforcon angazhimin tonë në rritjen e nivelit të sigurisë kibernetike. Gjatë këtij aktiviteti, AKCESK ndau praktikat kombëtare lidhur me hartimin dhe zbatimin e sistemit kombëtar për klasifikimin e incidenteve kibernetike, duke përfshirë kuadrin ligjor, aktet nënligjore dhe sfidat kryesore. Theks i veçantë u vendos në rëndësinë e bashkëpunimit ndërkombëtar, për adresimin e sfidave globale në sigurinë kibernetike.

Ky angazhim në Organizatën për Siguri dhe Bashkëpunim në Evropë dëshmon përkushtimin e vazhdueshëm të AKCESK për të garantuar një mjedis digjital të sigurt për të gjithë.

Rruga "Papa Gjon Pali II", Nr.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039

BULETIN JAVOR
15-19 PRILL 2024

Shprehja e javës

"Informacioni është oksigjeni i epokës moderne. Ai depërton nëpër muret me tela me gjemba, ai përhapet përtej kufijve të elektrizuar."

Ronald Reagan

Përmbajtja:

Frontier Communications mbyll sistemet pas sulmeve kibernetike

Ofruesi amerikan i telekomunikacionitit *Frontier Communications* po rikthen sistemet pasi një grup i krimit kibernetik shkeli sistemet e tij të IT-së. Kompania, e cila ofron shpejtësi gigabit interneti në 25 shtete, mbylli pjesërisht disa sisteme për të parandaluar që aktorët e kërcënimit të hynin ne rrjet.

Pavarësisht incidentit, Frontier pretendon se sulmuesit mund të kenë akses në disa informacione personale të identifikueshme. Një ndërprerje e rrjetit shkatërroi faqet, aplikacionet dhe platformat e shitjes me shumicë të Frontier. Frontier vazhdon të hetojë dhe ka angazhuar ekspertë të sigurisë kibernetike.

Link: Lexo më shumë

Cherry Health goditet nga sulmi i ransomware

Cherry Health, një ofrues i kujdesit shëndetësor me bazë në SHBA, ka pësuar një sulm ransomware, duke rezultuar në aksesin e gabuar të të dhënave personale të 185,000 pacientëve.

Të dhënat përfshijnë emrat dhe mbiemrat, adresat, numrat e telefonit, datat e lindjes, informacionin e sigurimit shëndetësor, numrat e identifikimit të pacientit, emrat e ofruesit, datat e shërbimit, informacionin e diagnozës/trajtimit, informacionin e recetës, informacionin e llogarisë financiare dhe numrat e sigurimeve shoqërore. Ofruesi i kujdesit shëndetësor paralajmëron individët e prekur që të jenë vigjilentë për vjedhjet e mundshme të identitetit dhe incidentet e mashtrimit.

Link: Lexo më shumë

Nexperia - Data Breach

Prodhuesi i çipeve Nexperia është vënë në shënjestër të hakerëve pasi Dark Angels, një grup ransomware, pretendoi se kishte vjedhur 1 TB të dhëna nga sistemet e tyre.

Këtu përfshihen të dhënat të kontrollit të cilësisë, dosje klientësh për gati 900 kompani, të dhëna konfidenciale të projektit, të dhëna të prodhimit industrial dhe informacione të korporatës. Kriminelët kibernetikë kanë bërë publike disa skedarë si provë, por kërcënojnë të nxjerrin të gjitha të dhënat e vjedhura nëse nuk paguhet një shpërblim. Nexperia ka shkëputur sistemet e prekura dhe ka nisur një hetim përsa i përket çështjes.

Link: Lexo më shumë

PATCHING ALERT

Cisco - Patching Alert

Cisco ka publikuar *patches* për një cënueshmëri të Kontrolluesit të Menaxhimit të Integruar (IMC) me rrezikshmëri të lartë që i lejon sulmuesit lokalë të përshkallëzojnë privilegjet në rrënjë (privileges to root).

Vulnerabiliteti prek pajisjet që ekzekutojnë versione vulnerabël IMC në konfigurimet e paracaktuara, duke përfshirë Sistemet e Llogaritjes së Rrjetit të Ndërmarrjeve 5000 (ENCS), Catalyst 8300 Series Edge uCPE, UCS C-Series Rack Servers në modalitetin e pavarur dhe Serverët UCS E-Series. Kompania ka paralajmëruar gjithashtu për një fushatë të kredencialeve në shkallë të gjerë që synon shërbimet VPN dhe SSH në pajisje të ndryshme.

Link: Lexo më shumë

Rruga "Papa Gjon Pali II", Nr.3
info@cesk.gov.al
Autoriteti Kombëtar për CESK
autoriteti_kombetar_cesk
+35542221039