BULETIN JAVOR
3-7 KORRIK 2023

Shprehja e javës

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

Përmbajtja:

- **Siguria kibernetike në sektorin shëndetësor. Këshilla të vlefshme**
- **Takimet e vazhdueshme të AKCESK me Infrastrukturat e Rëndësishme të Informacionit mbi rritjen e vigjilencës dhe forcimin e masave të sigurisë**

Siguria kibernetike në sektorin shëndetësor. Këshilla të vlefshme

"Industritë e tjera mund të mbështeten më shumë në sigurinë duke izoluar të dhëna të ndjeshme në mënyrë që të mos jenë të lidhura me internetin, por kjo nuk vlen për kujdesin shëndetësor modern."

Christopher Porter – Shefi i Inteligjencës së Kërcënimeve në Google Cloud

1: Trajnoni punonjësit për sigurinë e të dhënave

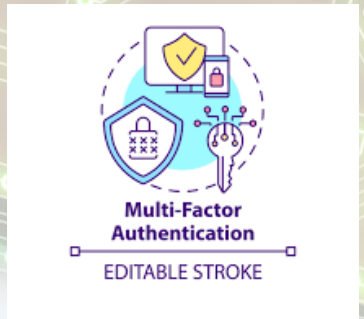
Trajnimi i punonjësve tuaj për rëndësinë e sigurisë së të dhënave, politikat për mbrojtjen e të dhënave dhe pasojat e një shkeljeje të të dhënave mund të ndihmojë të siguroheni që të dhënat e kujdesit shëndetësor të mbeten konfidenciale dhe të sigurta. Dhënia e punonjësve të mjeteve dhe njohurive që u nevojiten për të njohur dhe për t'iu përgjigjur kërcënimeve të mundshme të sigurisë mund të ndihmojë në zbutjen e çdo rreziku dhe nuk është diçka për t'u marrë lehtë.

2: Kryeni vlerësimet e rrezikut në mënyrë rutinore

Vlerësimet e rregullta të rrezikut janë thelbësore për të mbrojtur të dhënat, jo vetëm të dhënat e kujdesit shëndetësor. Është e rëndësishme të marrësh kohë për të rishikuar dhe audituar sistemet e kujdesit shëndetësor, bazat e të dhënave dhe sigurinë e rrjetit për të identifikuar rreziqet e mundshme të sigurisë dhe për të siguruar që të gjitha masat e nevojshme janë në vend për të zbutur ato rreziqe.

3: Autentifikimi me shumë faktorë (MFA)

MFA shton një shtresë shtesë sigurie duke kërkuar verifikim shtesë përveç një emri përdoruesi dhe fjalëkalimi. MFA mund të zvogëlojë në mënyrë dramatike rrezikun e humbjes së të dhënave ose aksesit të paautorizuar dhe është një domosdoshmëri absolute për organizatat që merren me informacione të ndjeshme të kujdesit shëndetësor.



Auditimi & Monitorimi

Auditimi dhe monitorimi përfshin zbulimin, analizimin dhe përgjigjen ndaj ngjarjeve të mundshme të sigurisë brenda sistemeve të kujdesit shëndetësor. Kjo përfshin ekzaminimin e aksesit të përdoruesit në të dhënat e ndjeshme dhe verifikimin e saktësisë së të dhënave të ruajtura

Takimet e vazhdueshme të AKCESK me Infrastrukturat e Rëndësishme të Informacionit mbi rritjen e vigjilencës dhe forcimin e masave të sigurisë

Në kuadër të ndërgjegjësimit të infrastrukturave kritike dhe të rëndësishme të informacionit, Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike në vazhdimësi të takimeve të mëparshme, ka organizuar një sërë takimesh gjatë ditës së sotme me te gjithë sektoret për të rritur vigjilencën dhe për të forcuar masat e sigurisë kibernetike në infrastrukturat e tyre dhe për të diskutuar mbi problematikat e mundshme në këta sektorë.

Në takim u theksua rëndësia e ndarjes së informacionit në kohë reale, me qëllim shpërndarjen e masave të duhura në të gjitha infrastrukturat e tjera për të krijuar një mjedis kibernetik sa më të sigurtë.

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

BULETIN JAVOR
3-7 KORRIK 2023

Shprehja e javës

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

Përmbajtja:

- **Agjencia e Bashkimit Evropian për Sigurinë Kibernetike (ENISA) publikon raportin e saj të parë të peizazhit të kërcënimeve kibernetike për sektorin e shëndetësisë.**
- **Zbulohen 2 Aplikacione të Android që mblidhnin të dhëna private pa autorizim.**
- **Microsoft- Data breach**
- **Android- Patching Alert**

Agjencia e Bashkimit Evropian për Sigurinë Kibernetike (ENISA) publikon raportin e saj të parë të peizazhit të kërcënimeve kibernetike për sektorin e shëndetësisë.

Agjencia e Bashkimit Evropian për Sigurinë Kibernetike (ENISA) publikoi së fundmi raportin e saj të parë të peizazhit të kërcënimeve kibernetike për sektorin e shëndetësisë. Raporti identifikon kërcënimet kryesore, aktorët e kërcënimit , tendencat dhe mbulon një periudhë mbi 2 vjeçare. Dokumenti gjithashtu analizon ndikimin e sulmeve kibernetike në sektor dhe jep detaje rreth subjekteve dhe aseteve më të shënjestruara.Studimi bazohet në një total prej 215 incidentesh të raportuara publikisht në BE dhe vendet fqinje.

Sipas raportit, organizatat në sektorin evropian të shëndetësisë përjetuan një numër të konsiderueshëm incidentesh, ku ofruesit e kujdesit shëndetësor përbënin 53% të incidenteve totale, 42% e incidenteve të raportuara kishin si synim spitalet, ndërsa autoritetet shëndetësore, organet dhe agjencitë përbënin 14% dhe së fundi industria farmaceutike 9%.

Raporti thekson më tej implikimet financiare, duke zbuluar se kostoja mesatare e një incidenti të rëndësishëm sigurie në sektorin e shëndetësisë vlerësohet në 300,000 €, siç tregohet nga studimi i "*ENISA NIS Investment 2022.*"

Link: Lexo më shumë

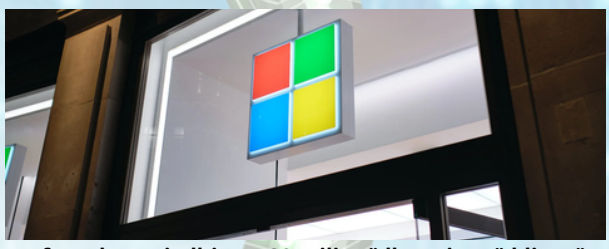
Zbulohen 2 Aplikacione të Android që mblidhnin të dhëna private pa autorizim.

Dy Aplikacione në Google Play Store janë zbuluar së fundmi të jen Spyware që dërgonin të dhënat private të 1.5mln përdoruesve në servera të dyshimtë në Kinë. Sipas raportimit nga një kompani e sigurisë së celularëve 2 aplikacionet përfshijnë:**File Recovery and Data Recovery** me mbi 1 milion instalime dhe **File Manager** me mbi 500,000 instalime

Në të dhënat e vjedhura bëjnë pjesë lista e kontakteve, audio, foto, video, lokacioni real-time, të dhënat e operatorit mobil dhe aparatit celular.

Si përdorues, është e domosdoshme të qëndroni vigjilentë, të tregoni kujdes kur shkarkoni aplikacione dhe të mbështeteni në burime të sigurta për të shkarkuar këto aplikacione në pajisjet tuaja.

Link:Lexo më shumë



Microsoft mohon vjedhjen e 30 milionë llogarive të klientëve

Microsoft ka mohuar pretendimet e të ashtuquajturve haktivistë "Anonymous Sudan" se ata kanë shkelur serverët e kompanisë dhe kanë vjedhur kredencialet për 30 milionë llogari të klientëve.

Muajin e kaluar, Microsoft pranoi se Anonymous Sudan ishte përgjegjës për ndërprerjet e shërbimit në fillim të qershorit që ndikuan në disa nga shërbimet e tij, duke përfshirë Azure, Outlook dhe OneDrive.

Haktivistët pretenduan se ata kishin "hakuar me sukses Microsoft" dhe "qasën në një bazë të dhënash të madhe që përmban më shumë se 30 milionë llogari të Microsoft, email dhe fjalëkalime".

Anonim Sudan ofroi t'ua shiste këtë bazë të dhënash palëve të interesuara për 50,000 dollarë

Për momentin është e paqartë nëse hetimi i Microsoft ka përfunduar apo është në vazhdim. Gjithashtu, mbetet për t'u parë reagimi i kompanisë ndaj publikimit të mundshëm publik të të dhënave.

Link:Lexo më shumë

PATCHING ALERT

Përditësimet e sigurisë së Android-it rregullojnë tre gabime të shfrytëzuara në mënyrë aktive

Google ka lëshuar përditësimet mujore të sigurisë për sistemin operativ Android, i cili vjen me rregullime për 46 vulnerabilitete.

Problemi më i rëndë i sigurisë që Google rregulloi këtë muaj është CVE-2023-21250, një cenueshmëri kritike në komponentin e Sistemit të Android që ndikon në versionet 11, 12 dhe 13 të Android.

Shfrytëzimi i CVE-2023-21250 mund të çojë në ekzekutimin e kodit në distancë*(remote)* pa ndërveprim të përdoruesit ose privilegje ekzekutimi shtesë

Përditësimi i sigurisë i Android i këtij muaji mbulon versionet 11, 12 dhe 13 të Android, por në varësi të fushës së dobësive të adresuara, ato mund të ndikojnë në versionet e vjetra të OS që nuk mbështeten më.

Do të ishte e këshillueshme zëvendësimi i pajisjes tuaj me një model më të ri ose instalimi i një shpërndarjeje Android të palëve të treta që zbaton përditësime sigurie për pajisjet e vjetra, megjithëse me vonesë.

Link:Lexo më shumë

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