Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

„LIEMSIS ”KIBERNETINIO INCIDENTO ATASKAITA
Vilnius

TLP: WHITE

Kibernetinio incidento reikšmė: Vidutinės svarbos **Tyrimo data:** 2021-03-15

Kibernetinio incidento apibūdinimas:

2021 m. kovo 11 dieną internetiniame forume su ribota prieiga buvo paskelbti Vilniaus kolegijos studentų asmens duomenys: vardas, pavardė, lytis, asmens kodas, namų adresas, miestas, mokykla, mokyklos baigimo metai, gimimo data, tautybė, studijų kryptis, studijų programos kodas, studijų pradžios data, studijų baigimo data, fakultetas ir mokslo įsitaigos pavadinimas. Kažkuriuo momentu anksčiau šie duomenys buvo neteisėtai pasisavinti, pavogti ar prieiga prie jų gauta įvykdžius kibernetinį incidentą. Forume taip pat skelbiama, kad piktavalis turi ir kitų švietimo įstaigų duomenų susijusių su https://www.liemsis[.lt] informacine sistema.

Kibernetinio incidento tyrimo pavadinimas: nesankcionuota prieiga prie duomenų bazės ir(arba) įsilaužimo į serverį incidento aplinkybių tyrimas.
Kibernetinio incidento pradžia (data / laikas): Tikslus laikas nenustatytas
Kibernetinio incidento pabaiga (data / laikas): 2020-03-11

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Santrauka

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) 2021-03-11 gavęs pranešimą apie Vilniaus kolegijos (toliau – VIKO) studentų duomenų paviešinimą programišių forume, iniciavo tyrimą, siekdamas nustatyti ar duomenų atskleidimas buvo įvykdžius kibernetinį incidentą, kaip ir kokiais būdais asmens duomenys buvo neteisėtai pasisavinti, pavogti ar prieiga prie jų gauta išnaudojus saugumo spragas.

Tyrimo metu buvo identifikuotos keturios aukštosios mokyklos, galimai susijusios su kibernetiniu incidentu (1 lentelė).

1 lentelė. Lietuvos aukštųjų mokyklų sąsajos su LIEMSIS informacine sistema

Nr.	Aukštoji mokykla	Sąsaja su incidentu
1.	Vilnius Tech	https://www.liemsis[.lt] nuoroda nukreipia į https://vilniustech[.lt]
2.	Vilniaus kolegija (VIKO)	Nutekinti šios kolegijos studentų duomenys, VIKO teikia informaciją į LIEMSIS informacinę sistemą
3.	Kauno Technologijos Universitetas	Administruoja LIEMSIS ir EDINA informacinę sistemą
4.	Vilniaus Universitetas	Turi integracijas su LIEMSIS

Tyrimo metu nepavyko gauti faktais pagrįstos informacijos, kad duomenų nutekėjimas buvo sąlygotas kibernetinio incidento, tačiau nustatyta kad incidento priežastis galėjo būti tinkamai neapribotos prieigos prie internetu pasiekiamų informacinių išteklių. Taip pat nėra aišku iš kurios informacinės sistemos buvo nutekinti studentų duomenys, nes buvo nustatytas nekontroliuojamas aukštųjų mokyklų informacinių išteklių išsiplėtimas (angl. *system sprawl*). LIEMSIS informacinė sistema, kuriai VIKO teikia duomenis, nėra tinkamai įteisinta pagal Valstybės informacinių išteklių valdymo įstatymo nuostatas:

1. nėra su atsakingomis institucijomis suderintų ir patvirtintų aktualiausių informacinės sistemos nuostatų bei saugos nuostatų;
2. nėra su atsakingomis institucijomis suderintų ir patvirtintų aktualiausių informacijos saugumą įgyvendinančios politikos dokumentų: saugaus elektroninės informacijos tvarkymo taisyklių, veiklos tęstinumo valdymo plano, naudotojų administravimo taisyklių, techninės specifikacijos;
3. nėra teikiama informacija apie kibernetinio saugumo rizikas bei jų valdymo priemones valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemoje;
4. nėra aišku kaip yra užtikrinamas organizacinių ir techninių kibernetinio saugumo reikalavimų, patvirtintų Lietuvos Respublikos Vyriausybės 2018-08-13 nutarimu Nr. 818 „Dėl kibernetinio saugumo įstatymo įgyvendinimo", įgyvendinimas.

Tel. 1843
El. p. cert@nksc.lt
https://www.nksc.lt

Esant tokioms aplinkybėms, sistemos valdytojui nėra sąlygų užtikrinti kibernetinio saugumo rizikų identifikavimui ir prevencijai prieš kibernetinius incidentus. Pažymėtina, kad VIKO taip pat nėra įteisinusi ir kitų savo naudojamų informacinių sistemų. Dėl šios priežasties, NKSC vertinimu, egzistuoja tikimybė, kad duomenys gali būti pasisavinti ir iš kitų VIKO informacinių išteklių .

Faktinės situacijos analizė parodė, jog šis incidentas buvo nulemtas kompleksinių aplinkybių, nes analizuotos informacinių sistemų sąsajos, procesai, institucijų atsakomybės nėra aiškiai reglamentuotos ir apsaugotos pagal Valstybės informacinių išteklių valdymo, Kibernetinio saugumo įstatymų nuostatas. Nereglamentavus aukštųjų mokyklų informacijos saugumo organizavimo, nenustačius kibernetinio saugumo atsakomybių ir nesiėmus būtinų kibernetinio saugumo užtikrinimo veiksmų, tokio pobūdžio kibernetiniai incidentai, NKSC vertinimu, yra tikėtini ir ateityje. Atsižvelgiant į tai, NKSC teikia kibernetinio saugumo rekomendacijas, kurias turi įgyvendinti sistemos valdytojas.

Išvados:

1. Neteisėtas Vilniaus kolegijos studentų asmens duomenų pasisavinimas galimai įvyko dėl neapribotos ir internetu pasiekiamos sistemos prieigos ir netinkamai organizuoto www.liemsis[.lt] kibernetinio saugumo. Tyrimo metu buvo identifikuota, kad incidento priežastis taip pat galėjo būti neapribotos prieigos prie kitų internetų pasiekiamų informacinių išteklių.
2. Iš tyrimo metu disponuotos ribotos informacijos nebuvo galima nustatyti, kada tiksliai ir iš kokios sistemos buvo pasisavinta Vilniaus kolegijos studentų duomenų bazė. To nebuvo galima padaryti dėl nekontroliuojamo aukštųjų mokyklų informacinių išteklių išsiplėtimo (angl. *system sprawl*).
3. Nustatytas galimai netinkamas asmens duomenų tvarkymas. Tarp nutekintų 7 tūkst. Vilniaus kolegijos studentų duomenų buvę asmens kodai buvo saugomi atviru tekstu (angl. *plaintext*).

Rekomendacijos:

1. Įteisinti informacines sistemas LIEMSIS ir EDINA pagal Lietuvos Respublikos valstybės informacinių išteklių valdymo ir Kibernetinio saugumo įstatymo nuostatas.
2. Įgyvendinti Lietuvos Respublikos Vyriausybės nutarimu Nr. 818 „Dėl kibernetinio saugumo įstatymo įgyvendinimo“ nustatytus kibernetinio saugumo reikalavimus.
3. Organizuoti ir atlikti trečiųjų šalių auditą bei nustatyti aukštųjų mokyklų kibernetinio saugumo rizikų šaltinius bei rizikų kontrolės priemonių efektyvumą;.
4. Periodiškai vykdyti privilegijuotų naudotojų paskyrų auditą.
5. Periodiškai vykdyti lokalių bei išorinių sistemų ir jų duomenų mainų auditą.
6. Nesaugoti perteklinių asmens duomenų.
7. Šifruoti saugomus jautrius duomenis patikimais kriptografiniais algoritmais.