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

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

INTERNETO SVETAINĖS TECHNINĖS SPECIFIKACIJOS SAUGUMO REIKALAVIMŲ REKOMENDACIJOS

Dokumento versija 1.0

Viešojo sektoriaus organizacijos, įsigydamos interneto svetainės kūrimo paslaugas, dažnai susiduria su sunkumais tinkamai aprašyti įsigyjamam produktui keliamus saugumo reikalavimus. Pagrindinė šio dokumento paskirtis – vienoje vietoje pateikti visą sąrašą bazinių saugumo reikalavimų, kurie turėtų būti taikomi naujai kuriamoms interneto svetainėms ir jų garantinei priežiūrai. Organizacijos, siekiančios įsigyti saugų produktą ir tinkamą jo palaikymą, turėtų įkelti šiuos rekomenduojamus reikalavimus į interneto svetainės techninės specifikacijos saugumo reikalavimų dalį. Kiekviena organizacija gali pati įvertinti šias rekomendacijas ir pasikoreguoti reikalavimus pagal savo poreikį.

REIKALAVIMAI SAUGUMUI

Paskyros ir slaptažodžiai

- Naudotojų slaptažodžiai privalo būti bent 12 simbolių ilgio.
- Neturi būti slaptažodžio sudarymo taisyklių, ribojančių leidžiamų simbolių tipą, t. y. turi būti leidžiama naudoti visus simbolius, įskaitant nelotyniškas raides, tarpus ir specialiuosius simbolius.
- Turi būti galimybė naudotojams patiems pasikeisti savo slaptažodį.
- Keičiant ar kuriant naują slaptažodį, naudotojui turi būti galimybė laikinai pamatyti visą savo įvestą užmaskuotą slaptažodį.
- Negali būti naudojamos slaptažodžio priminimo užuominos arba žiniomis pagrįstas autentifikavimas (vadinamieji „slapti klausimai“, angl. *secret questions*).
- Prisijungimo duomenų atkūrimo funkcionalumas negali atskleisti dabartinio naudotojo slaptažodžio.
- Naudotojų slaptažodžiai duomenų bazėje turi būti saugomi naudojant saugius kriptografinius maišos algoritmus.
- Negali būti bendro naudojimo paskyrų, kuriomis naudotųsi daugiau nei vienas asmuo.
- Negali būti paskyrų su naudotojo vardais (angl. *username*) pagal nutylėjimą (pvz. „admin“, „administrator“, „administratorius“, „user“, „naudotojas“ ir pan.).

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

- Negali būti naudojami naudotojų vardai ir slaptažodžiai, kuriuos Paslaugų teikėjas naudoja kitose savo ar klientų sistemose. Pvz. negali būti naudojamas paskyros arba duomenų bazės vardas ar slaptažodis, kurį Paslaugų teikėjas naudoja pas kitą klientą.
- Negali būti naudojami naudotojų vardai ir slaptažodžiai, kurių sudarymo algoritmas būtų nuspėjamas. Pvz. kuomet naudotojo vardas ar slaptažodis skirtingiems Paslaugų teikėjo klientams skiriasi tik keliais simboliais.
- Negali būti naudojami naudotojų vardai ir slaptažodžiai, kuriuos sudarytų bet kokie Perkančiosios organizacijos požymiai ar jų dalys (pvz. pavadinimas, adresas, įmonės kodas ar jų dalys).

Prieigos kontrolė

- Viešas turinio administravimo pasiekiamumas turi būti apribotas, nuotolinę turinio administravimo prieigą suteikiant tik personalui iš konkrečių dedikuotų IP adresų. Esant viešo pasiekiamumo būtinybei, administravimo naudotojų paskyrų autentifikavimui turi būti naudojamas bent dviejų faktorių autentifikacijos funkcionalumas.
- Turi būti apsauga nuo slaptažodžių parinkinėjimo atakų, nenaudojant paskyrų blokavimo (angl. *account lockout*) funkcionalumo (pvz. sukuriant pauzes tarp bandymų prisijungti ir didinant jos trukmę po kiekvieno nepavykusio prisijungimo arba naudojant efektyvų CAPTCHA sprendimą).
- Turi būti funkcionalumas, leidžiantis apriboti prieigą pagal IP adresus tiek prie svetainės, tiek prie jos administravimo.
- Naudotojams ar jų grupėms turi būti suteikiamos tik tokios administravimo ir turinio pasiekiamumo teisės, kurios jiems yra būtinos atlikti numatytas funkcijas.
- Turi būti uždrausta naršyti interneto svetainės aplankuose (angl. *directory browsing*), nebent tokiam funkcionalumui yra numatytas pagrįstas poreikis.

Įvesties apsauga

- Visi įvesties šaltiniai (HTML formų laukai, REST užklausos, URL parametrai, HTTP antraštės (angl. *headers*), slapukai (angl. *cookies*) ir kt.) turi būti tinkamai validuojami.
- Interneto svetainės formose, kuriose svetainės lankytojai gali įvesti tam tikrą informaciją, turi būti naudojamos apsaugos nuo robotų (pvz. naudojant efektyvų CAPTCHA sprendimą).
- Visa svetainės lankytojų įvedama informacija turi būti tinkamai išvalyta (angl. *sanitize*), apribojant leidžiamų simbolių aibę ir įvedamos informacijos dydį pagal poreikį.
- Turi būti leidžiamas tik pasirinktų tipų (plėtinių) failų įkėlimas (pvz. „jpg“, „png“, „docx“ ir pan.), tikrinant faktinį failo tipą (MIME type).
- Turi būti galimybė administruoti leidžiamų įkelti failų plėtinių sąrašą.
- Svetainė turi būti apsaugota nuo „XSS“, „CSRF“ ir „SSRF“ tipo atakų.
- Svetainė turi būti apsaugota nuo „Local File Inclusion“ (LFI) ir „Remote File Inclusion“ (RFI) atakų.
- Svetainė turi būti apsaugota nuo „SQL injection“ tipo atakų.

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

- Svetainė turi būti apsaugota nuo „XPath injection“ ir „XML injection“ tipo atakų.

Sesijos

- Sesijos prieigos raktai (angl. *token*) negali būti naudojami URL parametruose.
- Sistemos naudotojų kiekvieno naujo prisijungimo metu turi būti generuojamas naujas atsitiktinis sesijos prieigos raktas, kurio sudarymo algoritmas negali būti nuspėjamas.
- Slapukais pagrįstų sesijų prieigos raktai privalo turėti nustatytą „Secure“ atributą.
- Slapukais pagrįstų sesijų prieigos raktai privalo turėti nustatytą „HttpOnly“ atributą.
- Slapukais pagrįstų sesijų prieigos raktai privalo naudoti „SameSite“ atributą.

Žurnaliniai įrašai

- Turi būti saugoma registruotų sistemos naudotojų atliktų veiksmų istorija (prisijungimai, atsijungimai, turinio redagavimai, failų įkėlimai, veiksmai su naudotojais ir pan.).
- Turi būti saugomos sistemos klaidos (angl. *error log*).
- Naudotojų prisijungimo duomenys, išskyrus naudotojo vardą, žurnaliniuose įrašuose nesaugomi.
- Turi būti saugomi nesėkmingi bandymai prisijungti.
- Žurnaliniai įrašai turi būti išvalyti ir saugomi tinkamu formatu, siekiant apsaugoti žurnalinių įrašų ir monitoringo sistemas nuo įterpimo atakų.
- Žurnaliniai įrašai turi būti apsaugoti nuo nesankcionuotos prieigos.
- Žurnaliniai įrašai turi būti apsaugoti nuo nesankcionuoto ar netyčinio pakeitimo.

Komunikacijos saugumas

- Negali būti naudojama HTTP 1.0 protokolo versija.
- Negali būti naudojamos nesaugios ar nešifruotos komunikacijos.
- Visoms svetainės komunikacijoms turi būti naudojamas TLS protokolas.
- Turi būti naudojamos tik naujausios rekomenduojamos TLS protokolo versijos (pvz., TLS 1.2 ir TLS 1.3), pirmenybę teikiant aukščiausiai versijai.

Komponentai

- Visi svetainės komponentai (turinio valdymo sistema, papildiniai/įskiepiai, šablonai, bibliotekos ir kt.), turi būti gamintojo palaikomos, pageidautina – naujausios, versijos.
- Nenaudojamas svetainės funkcionalumas turi būti išjungtas, nenaudojami komponentai ir konfigūracijos – pašalinti.
- Svetainėje naudojami trečiųjų šalių komponentai turi būti siunčiami tik iš oficialių šaltinių.
- Interneto svetainė ir visi jos komponentai turi būti suderinami su svetainės veikimui naudojamos programinės įrangos (žiniatinklio serverio, programavimo kalbos, duomenų bazės, operacinės sistemos ir kt.) stabiliomis palaikomomis versijomis, kurioms gamintojas

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

yra numatęs palaikymą (įskaitant saugumo pataisas) ne trumpesnį nei 24 mėn. po svetainės paleidimo datos.

HTTP saugumo antraštės (angl. *HTTP security headers*)

- Turi būti naudojamos „Content Security Policy (CSP)“ antraštės.
- Turi būti naudojama „X-Content-Type-Options: nosniff“ antraštė.
- Turi būti naudojama „Strict-Transport-Security“ antraštė.
- Turi būti naudojama „Referrer-Policy“ antraštė.
- Turi būti naudojama apsauga nuo svetainės turinio įterpimo (angl. *embed*) į trečiųjų šalių svetaines, jeigu nenumatyta kitaip. Šiam tikslui turi būti naudojamos „Security-Policy: frame-ancestors“ ir „X-Frame-Options“ antraštės.

Duomenų kopijos

- Reguliariai turi būti sukuriamos svetainės atsarginės kopijos. Kopijų kūrimo dažnumas, kiekis ir saugojimo trukmė turi būti suderinta su Perkančiąja organizacija (priklausomai nuo svetainės atnaujinimo dažnumo, duomenų kiekio ir svarbumo. Pvz. dalinė kopija sukuriama kasdien, pilna – kas savaitę).
- Turi būti įgyvendintas funkcionalumas, leidžiantis atkurti svetainę iš atsarginės kopijos.
- Duomenų kopijos turi būti apsaugotos nuo nesankcionuotos prieigos ar pakeitimo.

Kiti saugumo reikalavimai

- Duomenų bazės viešas tiesioginis prieinamumas turi būti apribotas, nebent tokiam funkcionalumui yra numatytas pagrįstas poreikis.
- Duomenų bazės valdymo įrankių (pvz. „phpMyAdmin“ ir pan.) viešas pasiekiamumas turi būti apribotas arba apsaugotas dviejų faktorių autentifikacija.
- Turi būti įgalinti automatiniai turinio valdymo sistemos ir jos komponentų saugumo atnaujinimai arba turi būti peržiūrima dėl saugumo atnaujinimų ne rečiau kaip kartą per mėnesį.
- Jeigu naudojama atviro kodo turinio valdymo sistema, kuriai yra sukurtų palaikomų žiniatinklio ugniasienės (angl. *Web Application Firewall (WAF)*) arba panašaus funkcionalumo komponentų, būtina tokį įdiegti.
- Svetainės derinimo (angl. *debug*) funkcionalumas turi būti išjungtas arba apribotas viešas jo pasiekiamumas, prieigą suteikiant tik asmenims, kuriems tokia informacija yra būtina.
- Rekomenduojama vengti perteklinės serverio, žiniatinklio programų ir svetainės komponentų informacijos viešinimo (pvz. per ServerTokens, ServerSignature, expose_php ir kt. parametrus).

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

Saugumo auditai

- Prieš svetainės paleidimą Paslaugų teikėjas turi atlikti patikrinimą dėl svetainės funkcionalumo atitikimo techninėje specifikacijoje nurodytiems kibernetinio saugumo reikalavimams. Nustatyti neatitikimai turi būti pašalinti iki svetainės viešo paleidimo. Perkančiajai organizacijai turi būti pateikta šio patikrinimo ataskaita.
- Po svetainės viešo paleidimo Paslaugų teikėjas turi atlikti kibernetinės saugos išorės auditą ir pašalinti aptiktas saugumo spragas. Auditas turi būti atliktas ne vėliau kaip per mėnesį nuo svetainės paleidimo, iš anksto suderinus su Perkančiąja organizacija. Perkančiajai organizacijai turi būti pateikta išsami kibernetinės saugos audito ataskaita.
- Perkančioji organizacija turi teisę bet kuriuo metu atlikti saugumo auditus. Šiems darbams Perkančioji organizacija gali pasitelkti trečiąsias šalis. Paslaugų teikėjas privalo suteikti visas reikiamas teises tinkamam svetainės, jos atskirų komponentų ir svetainę aptarnaujančių sistemų (jeigu šios priklauso Paslaugų teikėjui ar jo subrangovui) patikrinimui.

Garantinė priežiūra

- Paslaugų teikėjas visos sutarties įgyvendinimo metu ir 36 mėnesius nuo galutinio paslaugų perdavimo – priėmimo akto pasirašymo dienos turi atlikti interneto svetainės garantinį aptarnavimą – taisyti visas aptiktas klaidas, kibernetinio saugumo spragas, neatitikimus šioje techninėje specifikacijoje apibrėžtiems reikalavimams ir kitus garantinės priežiūros dalyje įvardintų reikalavimų veiksmus.
- Jeigu automatiniai turinio valdymo sistemos ir jos komponentų saugumo atnaujinimai neįgalinti, Paslaugų teikėjas ne rečiau kaip kartą per mėnesį privalo atnaujinti svetainėje naudojamus komponentus, jeigu jiems yra išleistos naujos gamintojo rekomenduojamos versijos.
- Jeigu automatiniai turinio valdymo sistemos ir jos komponentų saugumo atnaujinimai įgalinti, Paslaugų teikėjas ne rečiau kaip kartą per tris mėnesius privalo patikrinti, kad šis funkcionalumas veikia tinkamai.
- Nebepalaikomus komponentus, jeigu juose nustatyta pažeidžiamumų, būtina pakeisti analogiško funkcionalumo komponentais arba pašalinti, jeigu Perkančioji organizacija tam pritaria.
- Aptiktos saugumo spragos, jeigu yra informacijos apie vykdomą šių spragų išnaudojimą, privalo būti pašalintos kuo skubiau, bet ne vėliau kaip per 1 d. d. nuo šios informacijos gavimo datos. Jeigu šių spragų per numatytą laiką pašalinti nėra galimybės dėl pagrįstos priežasties (pvz. nėra išleistos spragų pataisos (angl. *patch*)), turi būti įgyvendintos laikinos spragų užkardymo arba poveikio sumažinimo (angl. *mitigate*) priemonės.
- Aptiktos saugumo spragos, kurių balas pagal Bendrąją pažeidžiamumų vertinimo sistemą (angl. *Common Vulnerability Scoring System (CVSS)*) yra 9 arba daugiau, jeigu joms yra žinomų paviešintų išnaudojimo kodų (angl. *exploit*), bet nėra informacijos apie vykdomą šių spragų išnaudojimą, privalo būti pašalintos ne vėliau kaip per 2 d. d. nuo šios informacijos gavimo datos. Jeigu šių spragų per numatytą laiką pašalinti nėra galimybės dėl pagrįstos

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

priežasties (pvz. nėra išleistos spragų pataisos), turi būti įgyvendintos laikinos spragų užkardymo arba poveikio sumažinimo priemonės.

- Aptiktos saugumo spragos, kurių balas pagal Bendrąją pažeidžiamumų vertinimo sistemą yra nuo 7,5 iki 8,9 (imtinai), jeigu joms yra žinomų paviešintų išnaudojimo kodų (angl. *exploit*), bet nėra informacijos apie vykdomą šių spragų išnaudojimą, privalo būti pašalintos ne vėliau kaip per 5 d. d. nuo šios informacijos gavimo datos. Jeigu šių spragų per numatytą laiką pašalinti nėra galimybės dėl pagrįstos priežasties (pvz. nėra išleistos spragų pataisos), turi būti įgyvendintos laikinos spragų užkardymo arba poveikio sumažinimo priemonės.
- Aptiktos saugumo spragos, kurių balas pagal Bendrąją pažeidžiamumų vertinimo sistemą yra 7,5 arba daugiau, jeigu joms nėra žinomų paviešintų išnaudojimo kodų ir nėra informacijos apie vykdomą šių spragų išnaudojimą, turi būti pašalintos ne vėliau kaip per vieną kalendorinį mėnesį nuo šios informacijos gavimo datos.
- Žemesnio vertinimo spragos, jeigu joms nėra žinomų paviešintų išnaudojimo kodų ir nėra informacijos apie vykdomą šių spragų išnaudojimą, turi būti pašalintos ne vėliau kaip per tris kalendorinius mėnesius nuo šios informacijos gavimo datos.