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

# NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS PRIE KRAŠTO APSAUGOS MINISTERIJOS

# INFORMACINIS BIULETENIS INTERNETO SVETAINIŲ KIBERNETINIO SAUGUMO PRIEMONIŲ VERTINIMAS IR ĮGYVENDINIMAS

Dokumento versija 1.1

Interneto svetainė – tai informacinė sistema (IS), susidedanti iš skirtingų, glaudžiai tarpusavyje susietų, skirtingo sudėtingumo technologinių sprendimų, kurių paskirtis – saugiai ir efektyviai realizuoti žiniatinklio taikomųjų programų veikimą bei užtikrinti svetainės teikiamas paslaugas lankytojams. Supaprastintai galima įsivaizduoti, kad interneto svetainė realizuojama veikiant kartu aparatinės dalies programinei įrangai ir svetainės programiniam kodui. Aparatinės dalies saugumas susijęs su svetainės kodo bei duomenų saugojimu, teisingu naršymo užklausų apdorojimu, ryšio sesijos šifravimu, o svetainės programinis kodas priklauso nuo svetainėje naudojamos programavimo platformos, turinio valdymo sistemos, pageidaujamo svetainės funkcionalumo.

Nacionalinis kibernetinio saugumo centras automatizuotomis priemonėmis vykdo periodinius Lietuvos interneto svetainių ir informacinių sistemų patikrinimus – ieškoma žinomų pažeidžiamumų, tikrinamos svetainės turinio valdymo sistemos, vertinama nuotolinio administravimo nustatymų rizika ir kt. Remdamiesi šių patikrinimų duomenimis, pateikiame interneto svetainių, viešų IS ir jas aptarnaujančių tarnybinių stočių kibernetinio saugumo priemonių įgyvendinimo rekomendacijas, kurios padidins pasirengimą kibernetinėms grėsmėms.

Kadangi svetainių pažeidžiamumo analizė vykdoma automatizuotomis priemonėmis, kurių ataskaita sudaroma tikimybiškai įvertinus aptiktų pažeidžiamumų riziką, pažeidžiamumo fiksavimas ne visais atvejais yra tiesioginis įrodymas, kad konkretus pažeidžiamumas duotojoje svetainėje egzistuoja ir gali būti išnaudotas. Tokios ataskaitos yra rekomendacinio pobūdžio, o jas vertinti turėtų svetainių ir IS valdytojai, pasitelkę į pagalbą kvalifikuotus IT specialistus ar svetainės kūrėjus, galinčius tiesiogiai patikrinti svetainės programinę įrangą bei jos parametrus

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

ir įvertinti pažeidžiamumų rizikos grėsmę. Pritaikius rekomenduojamas priemones, pasiekiamas didesnis efektas apsaugant svetainę nuo potencialių grėsmių.

**Trumpojo – vidutinio įgyvendinimo laikotarpio rekomendacijos**

1. Apribokite viešą turinio administravimo pasiekiamumą, nuotolinę turinio administravimo prieigą suteikiant tik personalui iš konkrečių dedikuotų IP adresų. Esant viešo pasiekiamumo būtinybei, sustiprinkite administravimo naudotojų paskyrų autentifikavimo priemones, pritaikydami CAPTCHA[1] ir (arba) dviejų faktorių autentifikavimą (2FA)[2].

2. Pasitikrinkite, ar nėra paliktų pirminių naudotojų (angl. *default user*) su pirminiais slaptažodžiais paskyrų, o faktui pasitvirtinus – jas pašalinkite arba pakeiskite prisijungimo duomenis. Kurdami naujas paskyras, nenaudokite standartinių naudotojų pavadinimų ir lengvai atspėjamų slaptažodžių. Nuolat vykdykite naudotojų sąrašų kontrolę (aktyvus naudotojų administravimas), minimizuokite administravimo teises naudotojams (kiekvienam vartotojui suteikiamos tik tos teisės, kurios yra būtinos jo funkcijai atlikti), įveskite periodinę slaptažodžių keitimo politiką.

3. Atlikite tarnybinių stočių ir tinklo įrenginių atvirų prievadų (angl. *port*) bei programinės įrangos auditą. Uždarykite nenaudojamus prievadus, išjunkite nenaudojamas paslaugas, apribokite vidiniams poreikiams naudojamų paslaugų viešą pasiekiamumą. Atnaujinkite pasenusias ir/ar pažeidžiamas programinės įrangos versijas.

4. Atlikite svetainės turinio valdymo sistemos (TVS), jos įskiepių (angl. *plugins/addons*) ir dizaino šablonų (angl. *theme/template*) auditą. Atnaujinkite TVS ir atskirų jos komponentų versijas, nenaudojamus komponentus pašalinkite. Įvertinkite automatinių atnaujinimų galimybes.

5. Atlikite organizacijai priklausančių IS pažeidžiamumų paiešką (nemokama NKSC žiniatinklio taikomųjų programų programinio kodo žinomų spragų patikrinimo paslauga https://site-check.cert.lt). Įvertinkite pažeidžiamumų analizės ataskaitą ir pašalinkite aptiktas spragas.

6. Nusistatykite auditavimo veiksmų periodiškumą ir vykdykite šias priemones nuolatos. Tai padės savalaikiai suvaldyti rizikas, kylančias dėl naujai atrandamų pažeidžiamumų bei

1 CAPTCHA (angl. *Completely Automated Public Turing test to tell Computers and Humans Apart*) – autentifikavimo mechanizmas skirtas apsisaugoti nuo automatizuotų sistemų prisijungimo.

2 2FA (angl. *two-factor authentication*) – naudotojo autentifikacijos metodas paremtas dviejų parametrų autentifikavimu - pasitelkiant du skirtingus tapatybės nustatymo būdus.

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

netinkamų sistemų konfigūracijų.

7. Įdiekite IS tarnybinėje stotyje SSL/TLS šifruojamo ryšio komunikaciją (HTTPS protokolas). Ši priemonė padės apsisaugoti nuo MITM[3] atakų ir jautrių duomenų nutekinimo.

8. Likviduokite IS, kurių valdytojai negali užtikrinti, kad būtų laikomasi nustatytų saugos reikalavimų ir rekomendacijų.

9. Peržiūrėkite informacinių išteklių žurnalinių įrašų (angl. *event logging*) politiką. Įvertinkite galimybes, nusistatykite poreikius ir vykdykite nuolatinį žurnalinių įrašų vertinimą. Teisingai vykdomas įvykių auditavimas ir analizė padės laiku nustatyti bandymus vykdyti kenkėjiškas veikas ir imtis tinkamų apsaugos priemonių.

10. Įvertinkite žiniatinklio ugniasienės[4] (angl. *WAF - Web Application Firewall*) įdiegimo galimybę. Tai taisyklių rinkiniu paremtas sprendimas, stebintis interneto aplikacijos komunikaciją ir užkardantis nestandartinių užklausų ar parametrų vykdymą.

11. Pasirūpinkite atsarginėmis duomenų kopijomis. Priklausomai nuo sistemos duomenų kaupimo ir atnaujinimo dažnumo, pasirinkite tinkamą kopijų kūrimo dažnumą. Priklausomai nuo duomenų kiekio ir svarbumo, pasirinkite tinkamą saugomų kopijų skaičių ir trukmę – pvz. viena kopija sukuriama kasdien, kita – kas savaitę.

**Ilgojo įgyvendinimo laikotarpio rekomendacijos**

1. Įsigyjant svetainės programavimo paslaugas, pirkimo specifikacijoje įtraukti svetainės kodo patikrinimo paslaugą pagal OWASP Top 10[5] ir (arba) SANS Top 25[6] reikalavimus. Perkančiajai organizacijai turi būti pateikiama viešai pasiekiamų sistemų/paslaugų kibernetinės saugos audito ataskaita bei aptiktų spragų pašalinimo planas.

---

3 MITM (angl. *Man in the middle*) atakos leidžia piktavaliams šnipinėti komunkacijos srautą bei perimti duomenis.

4 Žiniatinklio ugniasienių pavyzdžiai: ModSecurity, Cloudflare, Akamai

5 Open Web Application Security Project Top 10 - identifikuoja 10 kritiškiausių interneto technologijų aplikacijų saugumo rizikų remiantis daugelio skirtingų veiklos sektorių organizacijų svetainių patikrinimais (https://owasp.org/www-project-top-ten/).

6 CWE/SANS Top 25 Software Errors – viso pasaulio saugumo ekspertų ir organizacijų sudarytas labiausiai paplitusių ir kritinių programinės įrangos spragų sąrašas (https://www.sans.org/top25-software-errors/).

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

2. Planuoti finansavimą programinės įrangos naujinimui ir palaikymui. Įvertinti naudojamos ir perkamos programinės įrangos palaikymo kaštus ir numatyti lėšų šioms paslaugoms įsigyti.

3. Priklausomai nuo svetainės svarbos, planuoti finansavimą atsparumo kibernetinėms grėsmėms patikrinimo vykdymui, kurio imtis suderinama su perkančiąja organizacija, pateikiant patikrinimo metu gautus rezultatus ir numatomus vykdyti programinės įrangos pakeitimus, siekiant kaip įmanoma greičiau sumažinti aptiktų kibernetinių grėsmių rizikas.

4. Interneto svetainės pirkimo dokumentuose įtraukti nuostatą, kad palaikymo paslaugų teikimo ir garantinių įsipareigojimų metu sukurtoje svetainėje nustačius OWASP Top 10 arba SANS Top 25 periodiškai skelbiamuose aktualiuose dokumentuose nurodytų pažeidžiamumų, paslaugos teikėjas įsipareigoja juos kaip įmanoma skubiau pašalinti, prieš tai pateikęs ir suderinęs su perkančiąja organizacija šių pažeidžiamų pašalinimo planą.

5. Interneto svetainės pirkimo dokumentuose įtraukti nuostatą, kad palaikymo paslaugų teikimo ir garantinių įsipareigojimų metu paslaugų teikėjas naujina svetainėje naudojamus komponentus (TVS, įskiepiai, šablonai ir kiti programiniai komponentai), o nebepalaikomus komponentus, jeigu juose nustatyta pažeidžiamumų, pakeičia analogiško funkcionalumo komponentais arba pašalina apskritai.