UGNIASIENĖS VALDYMO PASLAUGA (WAF)

1. Dokumento apimtis

1.1. Šis dokumentas aprašo Paslaugų teikėjo veiklą valdant web ugniasienės incidentus ir užklausas, vykdant priežiūros ir plėtros darbus (toliau – WAF).

2. WAF Paslaugos apimtis

Techninis/saugos pažeidžiamumas (angl. Vulnerability, toliau - Pažeidžiamumas) – sistemos ar įrenginio konfigūracijos klaidos, netinkama apsauga nuo konkrečios grėsmės, galinti suteikti neautorizuotą prieigą prie informacijos, sutrikdyti sistemų patikimumą ar tikslumą.

WAF (angl. Web Application Firewall) Paslaugos teikimas skirtas tam, kad Užsakovo per web pasiekiamos sistemos būtų apsaugotos nuo Pažeidžiamumų, vykdomas nuolatinis srauto tikrinimas ir aptiktų Pažeidžiamumų šalinimo kontrolė.

Paslauga apima:

- WAF atnaujinimas kartu su vykdomais pokyčiais;
- Nuolatinis sutartų sistemų užklausų srauto tikrinimas;
- Užsakovo teikiamų Incidentų registracija ir jų sprendimo kontrolė;
- Konsultacijų susijusių su WAF Paslauga teikimas Užsakovo įgaliotiems asmenims;
- Ataskaitų teikimas.

2.1. WAF sistemos atnaujinimas kartu su vykdomais pokyčiais.

2.1.1. Siekiant, kad WAF nesiimtų blokavimo veiksmų įdiegus naują funkcionalumą, į sistemą turi nuolat būti įtraukiami skenuojamų sistemų pokyčiai. T.y. Paslaugos apimtyje Paslaugos teikėjas atnaujina WAF sistemą pagal pateikiamus plėtros užsakymus. Užsakovas įsipareigoja informuoti Paslaugos teikėją apie savarankiškai Užsakovo vystomų sistemų planuojamus pokyčius, jų diegimo datas, o Paslaugos teikėjas įsipareigoja stebėti WAF veiklą su Sistemoje atliktais pokyčiais, informuoti Užsakovą apie WAF sistemos pranešimus bei blokavimo veiksmus (incidentus) ir teikia siūlymus apie būtinus atlikti pakeitimus.

2.1.2. Gavus informaciją apie vykdomus keitimus:

2.1.2.1. Patikrinti ar pakeitimai neprieštarauja nustatytoms politikoms.

2.1.2.2. Atnaujinti sistemą, kad ši atpažintų atliktus pakeitimus ir priimtų juos.

2.2. Sistemų užklausų srauto skenavimas.

2.2.1. Vykdyti nuolatinį sistemų užklausų srauto tikrinimą.

2.2.2. Konsultacijų, susijusių su skenavimo funkcionalumu teikimas Užsakovui telefonu, elektroniniu paštu ar kitu sutartu būdu.

2.3. Incidentų registracija ir jų sprendimo kontrolė

2.3.1. Paslaugos apimtyje incidentu nelaikoma situacija, kai užklausa buvo blokuota dėl nesankcionuotos veiklos. Tai rodo, kad Paslauga veikia.

2.3.2. Paslaugos incidentu laikoma:

2.3.2.1. Jei būtų nustatyta, kad srautas nebuvo skenuojamas dėl WAF įrangos gedimo arba Paslaugų teikėjo klaidingai įvestos informacijos,

2.3.2.2. Jei įvyko pažeidžiamumas dėl laiku neatnaujintos gamintojo programinės įrangos,

2.3.2.3. Jei incidentas įvyko dėl Paslaugos teikėjo kaltės, kai vykdant skenuojamos sistemos plėtros darbus, informacija apie pokytį buvo pateikta Paslaugos teikėjui, o šis nesiėmė veiksmų įtraukti pakeitimus į WAF sistemos leidžiamų veiksmų sąrašą.

2.4. Ataskaitos

2.4.1. Užsakovui registravus blokavimo atvejį, Paslaugos teikėjas pateikia atsakymą apie blokavimo priežastį.

2.4.2. Papildoma informacija užsakoma pagal susitarimą.

2.5. Konsultacijos

2.5.1. Konsultacijų, susijusių su WAF teikimas Užsakovui.

3. Paslaugos teikimo ribos

3.1. Priedėlyje Nr. 1 nurodytos sistemos/svetainės srauto tikrinimas vyksta 24x7.

3.2. Informacija Užsakovui apie blokavimo priežastį pateikiama per 8 val. aptarnavimo laiku.

3.3. Jei užklausa į Užsakovo sistemą/svetainę buvo blokuota, Užsakovas atsakingas pateikti Paslaugos teikėjui incidento ID, kuris nurodomas pranešime blokuotam vartotojui.

3.4. Paslaugos teikėjas atsakingas pateikti blokuotos užklausos vartotojui pranešimą kur kreiptis blokavimo atveju. Už pranešimo turinį atsakingas Užsakovas.

3.5. Užsakovas atsakingas už blokuotų užklausų vartotojų kreipinių valdymą.

3.6. Pasaugos teikėjas atsakingas už Užsakovo registruotų kreipinių Paslaugų valdymo sistemoje valdymą.

Priedėlis Nr. 1 Į WAF PRIEŽIŪRĄ ĮTRAUKTŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	Sistemos pavadinimas
1.	www.nlea.lt

Paslaugų teikėjo vardu _____

Užsakovo vardu _____