Vidinio tinklo administravimo paslaugos teikimo taisyklės

1. BENDROSIOS NUOSTATOS

1.1. Paslaugos „Vidinio tinklo administravimas" (toliau - Paslauga) teikimo taisyklėse (toliau – Taisyklės) apibrėžiama paslaugos teikimo apimtis, kokybės užtikrinimo standartai bei kitos sąlygas, susijusias su Paslaugos įdiegimu ir teikimu.
1.2. Taisyklės taikomos tik Sutartims, sudarytoms ar pratęstoms po šių Taisyklių įsigaliojimo.
1.3. Paslaugos mokesčiai nurodomi Paslaugos Užsakyme.
1.4. Bendrosios Paslaugos teikimo sąlygos pateikiamos Penki Verslui paslaugų teikimo sutarties bendrojoje dalyje.

2. STANDARTINĖ PASLAUGOS APIMTIS BEI TEIKIMO SĄLYGOS

2.1. Vidinio tinklo administravimo paslauga apima Užsakyme suderintos Užsakovo tinklo infrastruktūros valdymą, įskaitant tinklo įrangos administravimą, ryšio saugos užtikrinimą, prieigos kontrolės priemones bei reagavimą į tinklo incidentus. Reakcija į incidentus neapima detalių analitinių veiksmų, tokių kaip pilna tinklo srauto analizė, nebent dėl to susitarta atskirai.
2.2. Paslauga teikiama tik tai įrangai, tinklo segmentams ar infrastruktūros komponentams, kurie aiškiai nurodyti Užsakyme arba Sutartyje. Paslaugos teikėjas neatsako už paslaugos kokybės pablogėjimą, jei Užsakovas savavališkai prijungia papildomą įrangą ar atlieka sistemos pakeitimus be išankstinio suderinimo.
2.3. Paslaugos teikimo laikotarpiu visa prieiga prie administruojamos tinklo įrangos, įskaitant administratoriaus teises, lieka išimtinai Paslaugos teikėjo dispozicijoje. Užsakovui administratoriaus teisės ar prieigos, leidžiančios keisti konfigūraciją, valdyti naudotojus ar kitaip daryti įtaką sistemos veikimui, nesuteikiamos, nebent dėl to aiškiai susitariama raštu. Tokiu atveju Paslaugos teikėjas neprisiima jokios atsakomybės už galimus įrangos ar tinklo veikimo sutrikimus, saugumo pažeidimus, duomenų praradimą ar kitus incidentus, kylančius iš Užsakovo veiksmų ar neveikimo. Visi tokio pobūdžio incidentai ar jų pasekmių šalinimas nėra įtraukiami į įprastos priežiūros apimtį ir yra vykdomi pagal atskirą susitarimą, taikant galiojantį valandinį paslaugų įkainį.
2.4. Administravimas vykdomas nuotoliniu būdu. Fizinių veiksmų atlikimas galimas tik pagal iš anksto suderintą atskirą susitarimą.
2.5. Pasiruošimas administravimo paslaugų teikimui apima šiuos veiksmus:
2.5.1. Tinklo infrastruktūros auditas – paslaugos teikimo pradžioje atliekamas Užsakovo tinklo įrenginių inventorizavimas ir bendros infrastruktūros apžvalga, kurios metu identifikuojami tinklo įrenginiai, dokumentuojama jų būsena bei sudaromas administruojamos įrangos sąrašas. Šiame etape tinklo įrenginių konfigūracija detaliai nevertinama, todėl Paslaugos teikėjas neprisiima atsakomybės už incidentus ar trikdžius, kylančius dėl paveldėtos (perimtos) konfigūracijos netikslumų, klaidų ar saugumo spragų.
Paslaugos teikėjas prisiima atsakomybę už perimtą tinklo konfigūraciją tik tuo atveju, jei Užsakovas papildomai užsako tinklo konfigūracijos auditą, kuris vykdomas kaip atskira paslauga pagal atskirą susitarimą.
2.5.2. Tinklo topologijos dokumentavimas – paslaugos teikimo pradžioje parengiama arba atnaujinama esamos vidinės tinklo infrastruktūros schema, kurioje žymimi administruojami įrenginiai, jų tarpusavio ryšiai bei esminiai tinklo segmentai. Ši schema naudojama kaip pagrindinis informacinis šaltinis tinklo priežiūrai ir sprendimų priėmimui. Užsakovas įsipareigoja pateikti turimus esamos tinklo topologijos dokumentus (schemas), jei tokie egzistuoja. Užsakovui prijungus naują įrangą ar atlikus struktūrinius tinklo pakeitimus, jis privalo informuoti Paslaugos teikėją dėl schemos atnaujinimo. Tuo atveju, jei tokie pakeitimai atliekami savavališkai ir apie juos neinformuojama, Paslaugos teikėjas neprisiima atsakomybės už kilusius

tinklo veikimo sutrikimus ar incidentus. Šių incidentų analizė ir sprendimas gali būti vykdomi tik pagal atskirą susitarimą, taikant galiojantį valandinį paslaugų įkainį.

2.6. Tinklo įrangos konfigūravimas.

2.6.1. Užsakovo tinklo įrangai atliekamas šiose taisyklėse apibrėžtų bazinių nustatymų ir saugumo taisyklių konfigūravimas bei įgalinimas. Taisyklių įgyvendinimas yra tiesiogiai priklausomas nuo Užsakovo turimos įrangos techninių galimybių ir funkcionalumo. Visos konfigūracijos galimos tik tuo atveju, jei įranga palaiko reikalingas funkcijas ir Užsakovas yra užtikrinęs visų būtinų licencijų galiojimą. Ši nuostata taikoma visiems šiame skyriuje (2.5) nurodytiems konfigūravimo veiksmams.

2.6.2. Bevielio tinklo (Wi-Fi) stotelių konfigūravimas apima šiuos veiksmus:

2.6.2.1. Papildomų tinklo grupių atskyrimas;

2.6.2.2. Svečių politikos valdymas;

2.6.2.3. Tinklo autentifikacijos konfigūravimas;

2.6.2.4. Tinklo pavadinimo (SSID) suteikimas ar keitimas;

2.6.2.5. Wi-Fi signalo padengimo žemėlapio sudarymas – parengiamas bevielio ryšio (Wi-Fi) įrenginių išdėstymo arba signalo padengiamumo žemėlapis, remiantis Užsakovo pateiktais patalpų techniniais brėžiniais. Paslauga teikiama tik tuo atveju, jei pateikiami aktualūs patalpų planai su tiksliomis erdvių dimensijomis ir zonavimu. Paslaugos teikėjas neatsako už netikslumus ar padengimo kokybės neatitikimus, jei pateikti brėžiniai yra pasenę, neišsamūs arba kitaip neatitinkantys faktinės situacijos.

2.6.3. Komutatorių (angl. *switch*) konfigūravimas apima šiuos veiksmus:

2.6.3.1. Apsauga nuo IP *spoofing* atakų;

2.6.3.2. Bazinių komutatoriaus veikimo taisyklių konfigūravimas;

2.6.3.3. DHCP *snooping* konfigūravimas;

2.6.3.4. DAI (angl. *Dynamic ARP Inspection*) konfigūravimas;

2.6.3.5. LACP / Link Aggregation protokolų konfigūravimas;

2.6.3.6. Loop prevencijos nustatymai;

2.6.3.7. Prievadų (angl. *interface*) konfigūravimas;

2.6.3.8. Prievadų aprašymų (angl. *port description*) konfigūravimas;

2.6.3.9. ACL taisyklių konfigūravimas;

2.6.3.10. SNMP protokolo konfigūravimas;

2.6.3.11. STP BPDU/Root Guard konfigūravimas;

2.6.3.12. VLAN konfigūravimas.

2.6.4. Maršrutizatorių (angl. *router*) konfigūravimas apima šiuos veiksmus:

2.6.4.1. ACL (angl. *Access List*) taisyklių konfigūravimas;

2.6.4.2. DHCP rolės valdymas;

2.6.4.3. IP adresų ir maršrutų konfigūravimas;

2.6.4.4. IPsec (*Site-to-Site*) VPN – virtualaus privataus tinklo sukūrimas tarp skirtingų įmonės padalinių ar trečiųjų šalių;

2.6.4.5. Nuotolinės prieigos VPN (angl. *Remote Access*) konfigūravimas – nutolusių darbo vietų virtualaus privataus tinklo sukūrimas. Šio funkcionalumo konfigūravimas apima tik tinklo įrangos dalies sukonfigūravimą. Už VPN įdiegimą nutolusioje darbo vietoje atsakingas Užsakovas;

2.6.4.6. NAT (angl. *Network Address Translation*) taisyklių konfigūravimas;

2.6.4.7. Prievadų (angl. *Port Forward*) taisyklių konfigūravimas.

2.6.5. Ugniasienių (angl. *firewall*) konfigūravimas apima šiuos veiksmus:

2.6.5.1. Automatinių atnaujinimų įgalinimas – jei įranga palaiko, aktyvuojamas automatinis saugumo parašų ar programinės įrangos atnaujinimų diegimas;

2.6.5.2. IDS/IPS (angl. *Intrusion Detection/Prevention System*) funkcionalumo konfigūravimas – tinklo atakų aptikimo (IDS) ir prevencijos (IPS) sistemų konfigūravimas, atitinkamų taisyklių nustatymas;

2.6.5.3. NAT taisyklių konfigūravimas – vidinio tinklo IP adresų vertimo į viešuosius (ir atvirkščiai) taisyklių sudarymas;

2.6.5.4. Prieigos valdymo sąrašų (ACL) konfigūravimas – srauto tarp tinklo segmentų arba išorinių tinklų valdymas pagal IP adresus, protokolus ar kitus kriterijus;

2.6.5.5. Prievadų persiuntimo taisyklių sudarymas – atitinkamo srauto (*port forwarding*) nukreipimas per ugniasienę į nurodytus įrenginius ar paslaugas;

2.6.5.6. Srauto valdymo taisyklių sudarymas – leidimų ir blokavimų pagal IP adresus, portus ir protokolus kūrimas (angl. *firewall rules*);

2.6.5.7. VPN tunelių konfigūravimas – *site-to-site ir client-to-site* VPN sprendimų diegimas ugniasienėje;

2.6.5.8. Web filtravimo ir aplikacijų kontrolės konfigūravimas – interneto turinio, aplikacijų ar kategorijų filtravimo taisyklių nustatymas.

2.7. Palaikymas.

2.7.1. Esant gamintojo palaikymo paslaugoms ar trečiųjų šalių kontraktams, Paslaugos teikėjas gali tarpininkauti kontaktuojant su įrangos tiekėjais dėl suderinamumo, gedimų ar kitų techninių klausimų.

2.7.2. Paslaugos teikėjas nesaugo ir neteikia pakaitinės įrangos, nebent dėl to buvo susitarta atskirai. Įrangai sugedus, atsakomybė už jos pakeitimą ar atkūrimą tenka Užsakovui. Esant poreikiui, Paslaugos teikėjas gali parinkti tinkamiausią įrangą ir ją pasiūlyti įsigyti kaip atskirą paslaugą.

2.7.3. Gedimo ar incidento atveju Paslaugos teikėjas reaguoja pagal iš anksto sutartus reagavimo laikus, jeigu Incidentas nėra susijęs su fiziniu įrangos pažeidimu ar trečiųjų šalių poveikiu, už kurį Paslaugos teikėjas neatsako.

2.8. Paslaugos apribojimai.

2.8.1. Incidentų sprendimas ir tinklo administravimo veiksmai atliekami nuotoliniu būdu. Jei tam tikrų veiksmų atlikti nuotoliniu būdu nėra galimybės, Paslaugos teikėjas darbus vykdo Kliento patalpose, taikant iš anksto suderintą atvykimo mokestį ir valandinį darbų atlikimo įkainį.

2.8.2. Tais atvejais, kai Užsakovo naudojama įranga ar programinė įranga yra pasenusi ir nebesulaukia gamintojo techninio palaikymo, Paslaugos teikėjas neprisiima atsakomybės už su tuo susijusių veikimo sutrikimų ar incidentų sprendimą.

2.8.3. Paslauga neapima žemiau nurodytų darbų, tačiau šie darbai gali būti atliekami kaip atskiros paslaugos pagal papildomą susitarimą:

2.8.3.1. Išsami tinklo srauto analizė;

2.8.3.2. Tinklo infrastruktūros perkėlimo, migracijos plano rengimo ar naujos aplinkos paruošimo darbai;

2.8.3.3. Tinklo įrangos konfigūracijų atsarginių kopijų kūrimas;

2.8.3.4. Tinklo įrangų monitoringas;

2.8.3.5. Tinklo kabelių išvedžiojimo ir telekomunikacinių rozečių montavimo darbai;

2.8.3.6. Tinklo įrangos nuoma;

2.8.3.7. Trečiųjų šalių sutarčių administravimas ar koordinavimas;

2.8.3.8. Žiniatinklio aplikacijų ugniasienės (WAF) konfigūravimas;

2.8.3.9. VRF (angl. *Virtual Routing and Forwarding*) konfigūravimas ir valdymas;

2.8.3.10. Įvykių žurnalo (angl. logging) ir įvykių sekimo funkcionalumo įgalinimas – apima saugumo įvykių registravimą bei galimybės identifikuoti ir stebėti bandymus pažeisti saugumo politiką užtikrinimą. Šio funkcionalumo įgalinimui būtinas papildomas serveris. Užsakovas įsipareigoja užtikrinti reikiamos serverinės infrastruktūros prieinamumą. Paslaugos teikėjas gali pasiūlyti serverio sprendimą tik tuo atveju, jei dėl to susitarta atskirai.

2.8.3.11. Atliekami įrangos programinės aparatinės įrangos (angl. firmware) atnaujinimai:

2.8.3.11.1. Automatiniai – susiję su gamintojo pateikiamais saugumo ar stabilumo pataisymais;

2.8.3.11.2. Planiniai – atliekami pagal susitarimus arba gamintojo rekomendacijas.

2.8.4. Konsultacijos, dokumentacijos ruošimas ar darbas trečiųjų šalių audito tikslu atliekamas tik iš anksto suderinus, pagal papildomų darbų įkainius.

2.8.5. Prižiūrimos įrangos skaičiui didėjant, paslaugos kaina proporcingai didinama, remiantis sutartimi ar paslaugos užsakymo sąlygomis.

2.8.6. Pakeitimus ar informacijos užklausas dėl paslaugos gali registruoti tik užsakyme nurodyti Užsakovo įgalioti asmenys.