



## Valdomo saugumo paslauga

### Paslaugos privalumai

Valdomo saugumo paslauga (VSP) - tai integruota duomenų saugumo paslauga, tenkinanti visos kompanijos poreikį saugiai keisti duomenimis tiek su vidinėmis, tiek su išorinėmis grupėmis, taip pat ir Internetu. Valdomo saugumo paslauga sertifikuota pagal ISO standartus. Kiekvienas sprendimas yra individualus ir adaptuotas specifiniams kiekvienos kompanijos poreikiams.

### Kas yra valdomo saugumo paslauga vartotojui/klientui:

- Ugniasienės, VPN, AntiVirus, Antispam sprendimas;
- aukštos kvalifikacijos profesionalų palaikymas ir konsultacijos 24/7 (24 val. / parą, 7 d. / sav.);
- Visuomet atnaujinama saugumo politika;
- Instaliacija, kontroliuojama patyrusių specialistų;
- Pilnai dokumentuota saugumo politika;
- 24/7 sprendimo stebėjimas.

Valdomo saugumo paslauga apima visus būtinus saugumo politikos komponentus ir saugumo valdymą, kuris dažnai lieka užmirštas mažose ir vidutinio dydžio kompanijose dėl nepakankamos IT specialistų patirties bei laiko trūkumo.

### VSP susideda iš sekančių komponentų:

- Saugumo politikos vystymas;
- Vartotojų ir vartotojų teisių kontrolė, vartotojų teisių suderinimas su pasirinkta saugumo politika;
- Prieigos taisyklės skirtingiems resursams;
- Periodinė saugumo rizikų analizė;
- Viso sprendimo, atliktų pakeitimų ir modifikavimų dokumentacija.

### Valdomo saugumo paslauga – tai puikus sprendimas kompanijai, kuri:

- Nusprendė specializuotis savo verslo srityje;
- Suvokia, kad keitimuisi duomenimis reikalingas aukšto lygio saugumas, bet neturi IT saugumo ekspertų;
- Suvokia, kad keitimuisi duomenimis reikalingas aukšto lygio saugumas, tačiau bando ieškoti alternatyvų didelėms saugumo sprendimų investicijoms;
- Pageidauja papildyti saugumo valdymą, užtikrintą IT specialistų bei ekspertų palaikymu;
- Pageidauja minimizuoti riziką, susijusią su naujomis technologijomis ir sprendimais nuolat besikeičiančiame informacinių technologijų pasaulyje.



### **Kodėl naudinga valdomo saugumo paslauga:**

- Nereikia investuoti pinigų pačią pirmą dieną;
- Sumažinama rizika, susijusi su IT specialistais;
- Mokama už realų naudojimą.

### **Paslaugos teikimas**

Siekiant užtikrinti saugų keitimuisi duomenimis svarbu pastoviai stebėti ir atnaujinti saugumo sprendimus priklausomai nuo naujų technologijų vystymosi ir aptiktų atakų.

### **Dokumentavimas**

Pirmiausia saugumo politika turi būti apibrėžta ir dokumentuota pagal standartus. Saugumo politikos apibrėžimo metu:

- visi vartotojai klasifikuojami į panašios veiklos grupes, remiantis jų teisėmis ir naudojamais resursais;
- kompanijos resursai klasifikuojami remiantis tuo, kiek svarbūs yra konkretūs duomenys – verslo duomenys (pvz. finansiniai duomenys, klientų pasiūlymai ir t.t. ), IT resursai (pvz. e-paštas, web puslapis ir t.t.);
- kompanijos resursai yra klasifikuojami remiantis prieinamumu prie jų;
- vartotojai klasifikuojami pagal jų prieigos teises – prieiga tik Intraneto viduje, prieiga prie Intraneto tik iš išorės ir t.t.;
- klasifikuojama, prie kurių resursų leidžiama prieiti tik iš Intraneto, o prie kurių ir iš Intraneto, ir iš išorinio tinklo;
- apibrėžiami vartotojų autorizacijos mechanizmai ir jų saugumas.

Įmonės saugumo politika dokumentuojama remiantis viskuo kas buvo apibūdinta aukščiau, sudarant Saugumo Profilį. Tai pagrindas saugumo sprendimų reikalavimams ir parametrų specifikuoti. Saugumo Profilis nuolat tobulinamas ir atnaujinamas.

### **Sprendimas**

Pagal Saugumo Profilį parenkami optimalūs saugumo sprendimo komponentai:

- ugniasienės programinė įranga;
- ugniasienės geležinė įranga;
- Jei būtina - komponentai reikalingi sprendimo dubliavimui;
- VPN komponentai, kompanijos filialų apjungimui;
- VPN komponentai žmonėms dirbantiems iš namų ar mobiliems vartotojams;
- priemonės vartotojų autorizavimui tiek iš Intraneto, tiek iš išorinio tinklo;
- valdymo programinė įranga;
- kiti komponentai.



Specifikuotų komponentų rinkinys instaliuojamas kliento biure ir / arba filialuose ir jei būtina, žmonių, dirbančių iš namų ar mobilių darbuotojų nešiojamuose kompiuteriuose. Saugumo sprendimas paruošiamas darbui atsižvelgiant į reikalavimus nustatytus Saugumo Profilyje.

## **Paslaugos veikimas**

Paslaugos teikimo metu atliekami įvairūs kasdieninių nustatymų valdymo veiksmai:

- sprendimo stebėjimas;
- papildymas programinės įrangos atnaujinimais (updates);
- papildymas programinės įrangos atnaujinimais, kuriuos kuria patys gamintojai naujų atakų prevencijai;
- vartotojų teisių modifikavimas, atsižvelgiant į kliento pateiktas instrukcijas;
- papildymas naujais resursais, atsižvelgiant į kliento pateiktas instrukcijas;
- reguliarius saugumo politikos įvertinimas;
- naudojamos techninės įrangos atnaujinimas esant poreikiui;
- žingsniai, būtini užtikrinti paslaugos parametrus, nustatytus SLA. Pvz. įrangos pakeitimas per nurodytą laiką ir specialisto atvykimas į kliento ofisą, jei paaiškėja, kad to reikia;
- modifikavimų, kurie buvo atlikti, dokumentacija;
- saugumo Profilio pastovus atnaujinimas, atsižvelgiant į užduotis ir modifikuotą vartotojų sąrašą bei vartotojų teises;
- įrašų (logų) archyvavimas.

Priklausomai nuo kliento poreikių ir norų kai kurie valdymo komponentai gali būti padalinti tarp kliento ir paslaugos tiekėjo specialistų. Pvz. naujų vartotojų prijungimas ir vartotojų teisių modifikavimas gali būti viena iš kliento specialistų užduočių. Šiuo atveju Adventus Solutions atlieka aukščiau paminėtas funkcijas, jei kliento specialistas yra išvykęs ilgesniam laikui arba jei šios funkcijos atlikimas efektyvesnis ir greitesnis naudojantis Adventus Solutions siūloma paslauga. Tokiu atveju modifikavimų dokumentaciją atlieka Adventus Solutions.