

## **REKOMENDACIJOS DĖL INTERNETO SVETAINIŲ IR JŲ ĮRANGOS KIBERNETINIO SAUGUMO GERINIMO**

1. patikrinti ugniasienių, per kurias kontroliuojamas naudotojų prisijungimas iš viešųjų elektroninių ryšių tinklų, sąrankų (konfigūracijų) atitiktį gamintojų siūlomoms praktikoms;
  2. sukonfigūruoti ugniasienes taip, kad prie tinklalapių turinio valdymo sistemų būtų galima jungtis tik iš vidinio institucijos tinklo arba nustatytų IP adresų;
  3. uždaryti nenaudojamus prievadus ir nuolat kontroliuoti prisijungimus per naudojamus prievadus;
  4. uždrausti prisijungimą prie serverių visais prievadais ir protokolais, išskyrus tuos, kurie būtini tinklalapiui funkcionuoti;
  5. vykdyti pažeidžiamumą paiešką nuolat tikrinant interneto svetainių, duomenų bazių saugumą su skenavimo programine įranga;
  6. naudoti technines apsaugas nuo žinomų kibernetinių atakų prieš interneto svetaines priemonės (angl. *web applicatin firewall*);
  7. likviduoti interneto svetaines, kurių valdytojai negali užtikrinti, kad būtų laikomasi nustatytų saugos reikalavimų ir rekomendacijų.
-