PROJEKTAS

2023-11-24

Kibernetinio saugumo rekomendacijos

- Siekiant užtikrinti organizacijos kibernetinį saugumą ir išvengti potencialių internetinių pavojų, pateikiame šias rekomendacijas.
- Reguliarūs saugumo atnaujinimai: periodiškai atnaujinti ir tikrinti saugumo sistemas, įskaitant antivirusinius įrankius, ugniasienes, kurios atnaujinamos kartu su operacine sistema, ir kitas apsaugos priemones. Tai padės užtikrinti, kad sistemose būtų įdiegti naujausi saugumo įrankiai ir spragų būtų galima išvengti.
- Kibernetinio saugumo mokymasis: domėtis kibernetinio saugumo aktualiomis, dalyvauti organizuojamuose mokymuose apie kibernetinio saugumo grėsmes ir kitus internetinius pavojus. Ugdyti saugumo sąmoningumą siekiant užtikrinti bendrą organizacijos saugumą.
- Slaptos ir jautrios informacijos saugojimas: užtikrinti, kad slapti duomenys būtų saugomi šifruotais būdais ir saugiose vietose.
- Atsarginės kopijos: reguliariai kurti atsargines kopijas kritinės informacijos, duomenų bazių ir kitų svarbių failų. Atsarginės kopijos padeda atkurti sistemą po incidento ar duomenų praradimo.
- Stabilūs ir saugūs slaptažodžiai: naudoti tik saugius slaptažodžius (didžiosios ir mažosios raidės, specialieji ženklai), vengti lengvai atspėjamų slaptažodžių naudojimo. Taip pat dvifaktorinis autentifikavimo būdas pagerina prieigos kontrolę.
- Atnaujinta programinė įrangą: reguliariai atnaujinti visą naudojamą programinę įrangą, kad būtų ištaisytos galimos spragos. Senesnės arba nepalaikomos versijos gali tapti saugumo rizikos šaltiniu.