INFORMATIKOS IR RYŠIŲ DEPARTAMENTO
PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS
INFORMACIJOS SAUGOS SKYRIUS

REKOMENDACIJOS DĖL UŽKRĖTIMO KENKSMINGA PROGRAMINE ĮRANGA PREVENCIJOS IR VEIKSMŲ APTIKUS KENKSMINGĄ PROGRAMINĘ ĮRANGĄ AR KIBERNETINĖS ATAKOS ATVEJU

Kas yra kenksminga/kenkėjiška/žalinga programinė įranga

Kenksminga programinė įranga yra kenkėjiška programa, sukurta ir skirta įvairiais būdais pakenkti kompiuteriui (įskaitant išmaniuosius įrenginius) ar jo naudotojui (įskaitant jo atstovaujamą įmonę, instituciją ar visą valstybę) bei suteikti įvairaus pobūdžio naudos kenkėjiškos programos kūrėjui (asmeninio, reputacinio, finansinio, politinio, karinio ir kt.). Kenkėjiškų programų pavyzdžiai: virusai, kirminai, Trojos arkliai, šnipinėjimo programos, nuotoliniu būdu valdomų įrenginių tinklai (angl. *botnet*) ir kt.

Kenkėjiškos programos gali plisti iš vieno kompiuterio į kitą, trikdyti kompiuterio veikimą, naudoti kompiuterio resursus naudotojo nenumatytai (pvz., kriptovaliutos gavybai), nelegaliai (pvz., brukalų platinimui) ar net nusikalstamai (pvz., kibernetinėms atakoms prieš ypatingos svarbos informacinę infrastruktūrą) veiklai, panaudoti, nutekinti, sugadinti, užšifruoti, sunaikinti kompiuteryje esančius duomenis, perimti kompiuterio valdymą, plisti į kitus kompiuterius ir kt. Kenkėjiškų programų veiksmų arsenalas bei jų atsparumas apsaugos priemonėms nuolat tobulinami nusikalstamo pasaulio atstovų bei valstybių specialiųjų tarnybų, gerai motyvuotų bei disponuojančių dideliais finansiniais bei intelektiniais ištekliais.

Kenksminga programine įranga dažniausiai užsikrečiama šiais būdais:

- sąmoningai, per neapdairumą ar dėl psichologinės manipuliacijos (socialinės inžinerijos):
  - atidarius užkrėstą el. laiško priedą;
  - paspaudus nuorodą į užkrėstą interneto puslapį el. laiške;
  - paspaudus nuorodą į užkrėstą interneto puslapį naršant internete ar socialiniuose tinkluose;
  - prijungus užkrėstą USB laikmeną, išorinį kietą diską ar kitą USB įrenginį (toliau – USB įrenginiai);
  - atsisiuntus nekaltai atrodančią bylą (pvz. juokingą vaizdą, sveikinimo atviruką, ekrano užsklandą, garso ar vaizdo bylą ir pan.) iš nepatikimo šaltinio, taip pat nelegalią („nulaužtą“) programinę įrangą, kompiuterių žaidimus ir pan.;
  - prisijungus prie užvaldyto belaidžio ryšio tinklo;
- įprastai lankantis populiariose interneto svetainėse, kurios buvo užkrėstos;
- nuo užkrėsto kompiuterio vietiniame kompiuterių tinkle.

Kaip apsisaugoti nuo kenksmingos programinės įrangos

- ✓ **Pagrindinė taisyklė: <u>Jei abejojate – nedarykite.</u>** Neatidarykite el. laiško priedo, nespauskite nuorodos el. laiške, neprijunkite USB įrenginio, nesijunkite prie nežinomo belaidžio ryšio tinklo, neteikite prašomos ar reikalaujamos informacijos nežinomam asmeniui ir pan.
- ✓ Nepasiduokite netikėtumui, skubinimui, spaudimui, smalsumui, abejingumui, patiklumui ir pan. efektams, nes būtent tai ir yra psichologinės manipuliacijos tikslas. Jei yra galimybė – pasitikslinkite, susisiekite su el. laiško siuntėju (ne el. paštu, o telefonu ar betarpiškai), kad išsklaidytumėte abejones.
- ✓ Niekam, jokiomis aplinkybėmis neatskleiskite savo prisijungimo duomenų, slaptažodžių.
- ✓ Būkite susipažinę su Jūsų institucijos saugos politikos dokumentais ir vykdykite jų reikalavimus.
- ✓ Kompiuterinėje darbo vietoje naudokite, prijunkite tik tarnybinius USB įrenginius. Šiuos įrenginius naudokite tik tarnybos reikmėms, tarnybinei informacijai.
- ✓ Atminkite, kad Jūsų kompiuteryje, nešiojamame kompiuteryje, planšetiniame kompiuteryje ar kitame išmaniajame įrenginyje (toliau – įrenginiai) įdiegtos ir tinkamai naudojamos apsaugos priemonės sumažina užkrėtimo galimybę, tačiau visiškai jos nepašalina.
- ✓ Esant klausimų – pasikonsultuokite su vietinio kompiuterių tinklo administratoriumi, saugos įgaliotiniu, Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos Informacinių ir telekomunikacinių technologijų pagalbos grupe (toliau – ITT Pagalbos grupė).

Ką daryti aptikus kenksmingą programinę įrangą

Jei įtariate, kad Jūsų įrenginys užkrėstas kenksminga programine įranga (sulėtėjo įrenginio darbas, padaugėjo pranešimų apie klaidas, padaugėjo langų su reklama, pakeistas interneto naršyklės pradinis puslapis, pakeista interneto paieškos sistema, nebeveikia saugos priemonės (antivirusinė programinė įranga, vietinė ugniasienė ar kt.) ir pan.), kreipkitės į ITT Pagalbos grupę ir vykdykite jos nurodymus.

Jei Jūsų įrenginys užvaldytas (negalite prisijungti prie įrenginio, negalite naudoti įrenginio kaip įprasta, reikalaujama išpirkos ir pan.), nedelsiant kreipkitės į ITT Pagalbos grupę ir tiksliai vykdykite jos nurodymus.

Kibernetinės atakos požymiai

- be išankstinio perspėjimo neveikia internetas, kitos įprastinės paslaugos (el. paštas, dokumentų valdymo sistema ir pan.);
- nepavyksta prisijungti prie informacinių sistemų ir registrų;
- sugadinti, dingę, sunaikinti ar neprieinami įrenginiuose esantys duomenys, dokumentai, informacija;
- neveikia įrenginių saugos priemonės;
- užvaldyti įrenginiai;
- paaiškėja, kad be Jūsų žinios Jūsų vardu teikiama informacija ar prašymai ją pateikti ir pan.;
- kiti reiškiniai, susiję su informacinėmis ir komunikacinėmis technologijomis, liudijantys piktavališką išorinį poveikį institucijai, jos valdomai bei tvarkomai informacijai bei įrangai;
- minėti reiškiniai įgyja masinį pobūdį institucijoje.

Atkreipkite dėmesį, kad šie reiškiniai gali būti ne tik kibernetinės atakos, bet ir įrangos gedimo, paslaugos sutrikimo, žmogiškosios klaidos požymiai.

Ką daryti kibernetinės atakos atveju

Elkitės ramiai ir dalykiškai.

Informuokite vietinio kompiuterių tinklo administratorių ar saugos įgaliotinį, o negalint to padaryti – praneškite ITT Pagalbos grupei.

Atminkite, kad jei kibernetinė ataka iš tikrųjų vyksta, šie asmenys greičiausiai jau yra informuoti ir bando šią ataką kuo greičiau suvaldyti, todėl teikiama jiems informacija turėtų būti tiksli, aiški ir neperteklinė.

ITT Pagalbos grupės kontaktai:

Telefonai: (8 5) 271 7777, 57777, +370 686 80746

El. paštas: ittpagalba@vrm.lt

Interneto svetainė: https://ittpagalba.vrm.lt/