Kauno fakultetas

KIBERNETINIO SAUGUMO INTERNETE ATMINTINĖ

Nepriklausomai nuo to, kokio dydžio organizacijoje dirbate ar kokį darbą atliekate, yra svarbu suprasti, kodėl galite būti pažeidžiami kibernetinėmis atakomis ir kaip galite save apsaugoti. Jei norite būti saugūs elektroninėje erdvėje, nereikia būti kibernetinio saugumo ekspertais – užtenka laikytis kibernetinio saugumo taisyklių ir savo organizacijos saugumo politikos nurodymų.

KAS VYKDO KIBERNETINIUS IŠPUOLIUS?

Internetiniai nusikaltėliai
Siekia pavogti ir parduoti organizacijos ar asmeninius duomenis arba prašyti išpirkos už informaciją ar prieigą prie Jūsų įrenginio.

Užsienio vyriausybės
Suinteresuotos gauti konfidencialią ir vertingą informaciją, kuri suteiktų strateginį ar politinį pranašumą.

Programišiai
Skirtingos kompetencijos lygį turintys asmenys, dažnai vykdantys atakas be konkretaus tikslo, pavyzdžiui, norėdami išbandyti savo įgūdžius.

Politiniai aktyvistai
Siekdami savo politinių ar ideologinių tikslų, gali atskleisti konfidencialią informaciją, diskredituoti ar sustabdyti organizacijos veiklą.

Teroristai
Suinteresuoti skleisti propagandą ir sutrikdyti procesus. Dažniausiai jie turi mažiau techninių gebėjimų, tačiau didžiausią motyvaciją.

Organizacijos darbuotojai
Išnaudodami savo prieigą prie duomenų ar tinklų gali vykdyti kenkėjišką veiklą, pavyzdžiui, pavogti konfidencialius ar svarbius duomenis ir paviešinti konkurentams.

KODĖL MANE GALI ATAKUOTI?

Norėdami gauti finansinės naudos ar dėl kitų tikslų atakuotojai gali išnaudoti viską, kas tik yra Jūsų įrenginiuose. Negalvokite, kad neturite nieko vertingo – visada įmanoma surasti būdą, kaip išnaudoti Jūsų įrenginį arba duomenis.

- Gali būti pavogti prisijungimo duomenys prie el. bankininkystės ar kitų finansinių sistemų, siekiant gauti tiesioginės finansinės naudos.
- Asmeninė informacija gali būti naudojama siekiant pavogti asmens tapatybę, Jūsų asmeninių duomenų pagrindu parengti labiau suasmenintą fišingo ataką ar parduoti informaciją kitiems nusikaltėliams.
- Organizacijos informacija gali būti vertinga konkurentams arba už ją galima paprašyti išpirkos, jei neturite atsarginių kopijų.
- Gali būti išnaudojami kompiuteriniai resursai: visiškai nieko vertingo neradus Jūsų įrenginyje, šio įrenginio resursai gali būti naudojami vykdyti kitas atakas arba „kasti“ kriptovaliutas.

KAIP SAUGOTIS NUO FIŠINGO ATAKŲ?

Fišingas yra sukčiavimo forma, skirta išvilioti konfidencialius duomenis ar priversti vartotoją paspausti kenkėjiškos interneto svetainės nuorodą, atidaryti užkrėstą laiško priedą. Fišingo laiškai, svetainės ar žinutės dažnai atrodo autentiški, tačiau iš tikrųjų gali būti suklastoti.

Fišingui naudojama viešai prieinama informacija apie Jus, taip siekiama laiškus padaryti kuo tikroviškesnius. Peržiūrėkite savo paskyrų privatumo nustatymus ir neviešinkite per daug asmeninės informacijos socialiniuose tinkluose.

Žinokite, kokia informacija prieinama apie Jus viešumoje, taip galėsite iš anksto numatyti, kas gali būti panaudota atakoms.

Atakuotojai fišingo atakos metu gali naudoti psichologinius metodus – skubinimą ar autoritetų nurodymus, verčiančius jus atlikti tam tikrą veiksmą.

Niekas nėra apsaugotas nuo fišingo atakų, todėl jeigu gavote įtartiną laišką, jį atidarėte ar į jį atsakius kilo įtarimas, praneškite atsakingiems asmenims (duomenų apsaugos pareigūnui, IT skyriui). Taip sumažinsite galimas fišingo atakos pasekmes.

APSAUGOKITE SAVO ĮRENGINIUS

Išmanieji telefonai ir apyrankės, planšetės, kompiuteriai gali būti išnaudoti nuotoliniu būdu arba turint fizinę prieigą. Vis dėlto Jūs galite apsaugoti šiuos įrenginius nuo labiausiai paplitusių atakų.

Neignoruokite programinės įrangos atnaujinimų – juose yra patobulinimų, kurie saugo jūsų įrenginį.

Nenaudokite piratinės programinės įrangos – kartu su ja gali būti įdiegiamas kenkėjiškas programinis kodas.

Naudokite papildomą apsaugos programinę įrangą: antivirusines programas, ugniasienes.

Užrakinkite savo įrenginį, kai juo nesinaudojate. Naudokite PIN kodą, slaptažodį, biometrinius užraktus – tai dar labiau apsunkins atakuotojams galimybę išnaudoti Jūsų įrenginį, jei paliksite jį be priežiūros, pamesite ar įrenginys bus pavogtas.

NAUDOKITE SUDĖTINGUS SLAPTAŽODŽIUS

Atakuotojai bandys prisijungti prie Jūsų paskyrų populiariausiais slaptažodžiais (pavyzdžiui: qwerty, 123456, password ir t. t.) arba naudos viešai prieinamas slaptažodžių duomenų bazes iš prieš tai atliktų atakų, todėl jei naudojate vienodą slaptažodį keliose paskyrose, visos Jūsų paskyros yra pažeidžiamos.

Sukurkite sudėtingus, tačiau įsimenamus slaptažodžius itin svarbioms paskyroms: pvz., slaptažodį iš trijų atsitiktinių žodžių. Venkite tokių nuspėjamų slaptažodžių, kaip gimimo datos, šeimos narių ar augintinių vardai ir pan.

Užsirašykite slaptažodžius tik naudodami slaptažodžių tvarkymo programinę įrangą. Niekada niekam neatskleiskite savo slaptažodžių.

Svarbioms paskyroms (el. bankininkystė, el. paštas ir soc. tinklai) naudokite dviejų faktorių autentifikaciją – 2FA. Ji suteikia papildomą būdą patikrinti, ar prisijungiantysis yra tikrai tas, kas skelbiasi.

Slaptažodžius keiskite bent kelis kartus per metus.

JEI KYLA ABEJONIŲ - KLAUSKITE

Apie incidentus praneškite savo organizacijos IT skyriui, duomenų apsaugos pareigūnui, nacionaliniam kibernetinio saugumo centrui.

Kibernetines atakas gali būti labai sunku atpažinti, todėl nedvejokite paprašyti patarimų ar pagalbos, jei kas nors atrodo įtartina, neįprasta ar neaišku.

Apie atakas praneškite kaip įmanoma greičiau – nemanykite, kad tai padarys kas nors kitas. Net jeigu padarėte, ko neturėjote padaryti (pvz., paspaudėte suklastotą nuorodą ar pateikėte informaciją), visada praneškite apie tai, kas nutiko.

Jei įtariate, jog patekote į ataką, pirmiausia pasikeiskite svarbiausių paskyrų slaptažodžius ir nuskenuokite įrenginį tam skirta antivirusine programine įranga.

PASTEBĖJOTE ĮTARTINĄ SITUACIJĄ?

Apie įtartinas situacijas, laiškus, tinklapius ar incidentus galite pranešti Vilniaus universiteto Informacijos sistemų ir kibernetinės saugos ekspertams el.paštu: incidentai@knf.vu.lt. Gausite patarimų ir konsultaciją kaip Jums reikėtų elgtis.

Kauno fakultetas

Vilniaus universitetas Kauno fakultetas

Adresas: Muitinės g. 8, LT-44280 Kaunas
Telefonas: (8 37) 422 523
El. paštas: info@knf.vu.lt

Bitdefender

Socialinis partneris