DUOMENŲ APSAUGOS PAREIGŪNAS –

MB „Teisės labirintai“
Juridinio asmens kodas 305412893
info@teiseslabirintai.lt; +370 (630) 17 959

REKOMENDACIJA – ATMINTINĖ
VIENAS POPULIARIAUSIŲ DUOMENŲ VILIOJIMO BŪDŲ „PHISHING SCAM“

KAS YRA „PHISHING SCAM“?

Duomenų vagystė „phishing“ (angl. terminas *phishing* kilęs nuo žodžių *password fishing* - slaptažodžių žvejyba) – tai tokia sukčiavimo forma prieš organizacijas, kai pasinaudojant nepageidaujamomis elektroninio pašto žinutėmis ar falsifikuotais internetiniais tinklalapiais siekiama išgauti prisijungimo prie informacinių sistemų slaptažodžius bei kitus konfidencialius duomenis.

Paprastai ataka pradedama nuo elektroninio pašto laiškų, atrodančių taip, lyg jie būtų siunčiami banko ar kitos rimtos organizacijos. Laiško siuntėjo laukelyje esantis adresas dažniausiai būna netikras (suklastotas).

Pavyzdžiui, laiške gali būti pranešama, kad sustabdytas vartotojo sąskaitos galiojimas, ir nurodoma, kad kol jis neužpildys tam tikrų duomenų pateiktoje anketoje, jo sąskaitos galiojimas nebus atnaujintas. Arba neva keičiantis aptarnavimo sistemai ar jos konfigūracijai reikia atnaujinti prisijungimo duomenis, todėl prašoma juos pateikti ir t.t.

Pagrindinė duomenis vioiojančių (angl. *phishing*) laiškų taisyklė – įtikinama priežastis, kodėl vartotojas turi pateikti tam tikrus duomenis, ir įtikinama aplinka tiems veiksmams atlikti (oficiali laiško forma bei suklastotas organizacijos, neva siunčiančios tokį prašymą, interneto svetainė).

Dažniausiai tokiuose laiškuose pateikiama nuoroda į suklastotą interneto puslapį, neva priklausantį organizacijai, kurios vardu siunčiamas duomenis viliojantis laiškas. Verta atkreipti dėmesį, kad tinklalapio adresas kartais būna beveik identiškas tikrajam tos organizacijos svetainės adresui (gali skirtis viena raidė ar simbolis). Laiškas, be teksto ir nuorodų, gali turėti priedus su kenkėjiška programine įranga, atidarius, tokį priedą įsilaužėliai gali gauti priėjimą prie jūsų kompiuterio ir savarankiškai susirinkti jiems reikiamus duomenis iš sistemos.

DAŽNIAUSIAI NAUDOJAMI SCENARIJAI

Žinutės iš banko

Banko vardu siunčiamas elektroninis laiškas, kurio forma bei grafinis išdėstymas atrodo įtikinamai. Paprastai tokiame laiške yra nurodoma priežastis, pavyzdžiui: „Jūsų banko sąskaitos galiojimas laikinai sustabdytas, norėdami atnaujinti sąskaitos galiojimą paspauskite žemiau esančią nuorodą bei prisijunkite prie elektroninės bankininkystės svetainės“. Vartotojas paspaudęs tokią nuorodą, patenka į suklastotą, neva banko tinklalapį. Toks tinklalapis vizualiai gali nesiskirti nuo realios bankinės sistemos, tačiau tikrai skirsis jo interneto adresas – galbūt viena raide, galbūt vienu skaičiumi ar simboliu.

Prašymas iš sistemų administratoriaus

Dar vienas galimas duomenų viliojimo scenarijus yra toks: jūsų įmonės ar organizacijos IT ūkio administratoriaus vardu yra siunčiamas laiškas su prašymu paleisti prisegtą vykdomąją bylą ar atsisiųsti ją iš pateikiamos nuorodos internete. Elektroniniame laiške gali būti nurodyta tokia ar panaši įtarimo nesukelianti priežastis: „siekiant išvengti ryšio sutrikimų“,. Jei jus paleisite vykdomąją bylą, kurioje iš tiesų yra kenkėjiška programinė įranga, įsilaužėliai gaus priėjimą prie jūsų kompiuterio sistemos. Taip pat sistemų administratoriaus ar kito darbuotojo vardu gali būti prašoma atskleisti prisijungimo duomenis prie kokios nors sistemos ar pan.

KAIP ATPAŽINTI DUOMENŲ VILIOJIMĄ?

- **Kas siuntė el. laišką?**

Pirmiausia patikrinkite, kam buvo siųstas el. laiškas. Atkreipkite dėmesį į tai, ar laukelyje „Cc“ arba „To“ yra daugiau adresatų, kurių Jūs nepažįstate. Jeigu tokių adresatų yra, gautą el. laišką reikėtų vertinti atsargiai ir įtariai.

- **Niekada nespauskite nuorodų**

Niekada nespauskite nuorodų, gautų el. paštu. Ypač jei tos nuorodos yra el. aiškuose, kurių nelaukėte. Rankiniu būdu suveskite tinklalapio adresą į naršyklę ir ieškokite reikiamos informacijos. Pavyzdžiui, jei gavote el. laišką iš siuntų bendrovės, kuriame teigiama, kad Jūsų siunta sėkmingai pristatyta arba dingo, eikite tiesiai į siuntų gabenimo įmonės internetinį tinklalapį ir ieškokite informacijos ten.

- **Skaityti domeno vardą atidžiai**

Skaitykite domeno vardą įdėmiai. Daugelis nusikaltėlių naudoja adresus labai panašius į tikruosius, pvz., *Paypal.com, ctibank.com, Factbook.com*. Iš pirmo žvilgsnio jie gali pasirodyti teisingi, bet atidžiau pažiūrėjus galima pamatyti spąstus.

Teisės labirintai
+370 630 17 959
info@teiseslabirintai.lt
www.teiseslabirintai.lt

REKOMENDACIJOS

- Visų pirma labai atsargiai įvertinkite elektroninius laiškus, kuriuose prašoma pateikti konfidencialią informaciją;
- Žinokite, kad patikimos kompanijos, o ypač bankai, niekada neprašo tokios informacijos pateikti elektroninio pašto laiškais;
- Neatsakinėkite į aukščiau aprašytus požymius atitinkančius duomenis viliojančius laiškus ir nesinaudokite pateikiamomis nuorodomis į internetinius tinklalapius, kadangi tai gali būti užmaskuoti duomenų viliojimo tinklalapiai arba kenkėjiška programinė įranga, skirta slapta rinkti duomenims, esančius jūsų kompiuteryje;
- Jeigu nusprendėte prisijungti, tai atlikite atskirame naršyklės lange, rankiniu būdu įvesdami savo elektroninės bankininkystės sistemos adresą, kurį paprastai naudojate (o ne tą, kuris pateikiamas el. laiške);
- Neįvedinėkite svarbios informacijos į iššokančius (angl. *pop-up*) langus;
- Naudokite antivirusinę sistemą, kuri neretai yra paskutinis gynybos ruožas, apsaugantis nuo pažeidžiamumo išnaudojimo galimybės. Net jei ir naudojate pažeidžiamą programinę įrangą, antivirusinė sistema gali pastebėti ir sustabdyti pažeidžiamumo išnaudojimo bandymą. Atnaujinkite antivirusinės sistemos duomenų bazes. Antivirusinių programų gamintojai išleidžia atnaujinimus beveik kasdien, todėl atnaujinę bazes visuomet būsite pasiruošę atremti naujausias grėsmes;
- Įsitikinkite, kad puslapis naudoja SSL ryšį. Puslapio adresas turi prasidėti ne http://, o https://, be to, naršyklės vartotojo sąsajoje atsiranda specialus ženklelis, kurį paspaudus galima patikrinti šifravimui naudojamą SSL sertifikatą;
- Reguliariai atnaujinkite kompiuterio operacinę sistemą bei programinę įrangą. Laiku atsinaujinant sumažėja tikimybė, jog įsilaužėliams pavyks pasinaudoti įvairiais pažeidžiamumais.

Teisės labirintai
+370 630 17 959
info@teiseslabirintai.lt
www.teiseslabirintai.lt