

Nuo tada, kai nusikaltimai persikėlė ir į internetinę erdvę bei atsirado programišiai, interneto svetainės tapo pagrindiniu jų taikiniu. Kibernetiniai nusikaltimai prasidėjo dar praeitame amžiuje, bet jau 2003 metais pasiekė tokį lygį, kad vidutiniškai kas 39 sekundes internete buvo įvykdoma ataka prieš įvairias svetaines, kaip rodo to meto tyrimai. Per beveik 20 metų interneto bei apsaugos technologijos smarkiai patobulėjo, o šiandien interneto tinklalapį gali susikurti visi - netgi darantys tai pirmą kartą. Kita vertus, programišiai taip pat tobulėja, o jų atakų mastai - didėja. Skaičiuojama, kad prasidėjus pandemijai, internetinių atakų grėsmė padidėjo 6 kartus lyginant su ligšioliniais skaičiais. Taigi, ką daryti, jei į jūsų svetainę buvo bandoma įsilaužti ir kaip nuo to tinkamai apsisaugoti?

„Šiandien turime ir naudojamės tikrai neribotomis interneto teikiamomis galimybėmis. Pavyzdžiui, galima vos per dieną susikurti savo interneto tinklalapį, jį patalpinti ir pasiekti norimą auditoriją. Kita vertus, klaidinga manyti, kad mažų ar naujų tinklalapių programišiai nepastebi ir puola tik didelius. Tiesa tokia, kad programišiai dažniausiai ieško spragų ir naudojami tomis galimybėmis, kuriomis pasinaudoti nereikia daug pastangų ir laiko sąnaudų. Todėl visiškai nesvarbu, ar jūsų svetainė turi didelę vartotojų bazę ir yra sudėtinga, ar joje norite suburti, pavyzdžiui, šunų mylėtojų bendruomenę - vienodai pažeidžiami yra absoliučiai visi interneto tinklalapiai. Žinoma, tuo atveju, jeigu jie nesisaugo ir nesilaiko bent jau esminių tinklalapių priežiūros principų“, - sako Elidijus Čypas, „Interneto vizijos“ kokybės užtikrinimo specialistas.

Kokie yra svarbiausi dalykai, kuriuos turint savo interneto tinklalapį, gali ir turi reguliariai daryti norintys išvengti programišių atakų?

Įsilaužimai ne visada pastebimi

Nors ir ne į visas svetaines įsilaužiama, laukti, kol tai kada nors įvyks ir tik tada imtis veiksmų - ydinga. Pasak E. Čypo, kartais įsilaužimo pėdsakas apskritai neaptinkamas.

„Svarbu pradėti nuo to, kad šiandien nebėra tikslo stebėti, ar svetainė - nulaužta ir ar į ją kas nors buvo įsilaužę. Šiais laikais būtina visas pastangas dėti tam, kad galimų įsilaužimų į svetainę apskritai išvengtume. Nes tam tikrų įsilaužimų galima ir visai nepastebėti, tad svetainės kūrėjai ar savininkai net nežinos, kad kažkas ne taip. Pavyzdžiui, vieni įsilaužėliai iškart vietoje savininko svetainės įkelia savo svetainę ar nukreipimus į kitus puslapius. Tokius pakeitimus labai lengva pastebėti net ir neturint IT žinių. Bet jeigu svetainė nulaužta ir įsilaužėliai tiesiog prikūrė papildomų puslapių, nepatikrinus serveryje esančių failų tai pastebėti bus sudėtinga. Todėl pradėti visada reikėtų ne nuo pirmojo įsilaužimo, bet nuo prevencijos“, - pabrėžia ekspertas.

Interneto svetainė - kaip asmeninis kompiuteris

Kaip teigia E. Čypas, viena esminių klaidų, kurias daro vartotojai - įsitikinimas, kad jei svetainė sukurta, jai nebūtina priežiūra ar jokie kiti papildomi veiksmai.

„Kalbant apie interneto svetaines ir jų priežiūrą, geriausias palyginimas, kuris šauna į galvą - asmeninis kompiuteris. Kai tik visi pradėjo jais naudotis, taip pat buvo manančių, kad kompiuterį nusiperki ir jam nereikia kasdienės priežiūros. Tuo metu šiandien jau daugelis žino, kad naudojantis kompiuteriu - būtini atnaujinimai, juos reikia diegti iš karto, kai tik pasirodo, naudoti ugniasienes, periodiškai kompiuterį skenuoti ir t. t. Taigi, būtent taip pat reikėtų elgtis ir su savo interneto svetaine. Ją būtina kuo dažniau atnaujinti ir tą daryti, kai tik išeina sistemos ar įskiepio atnaujinimai. Taip pat, jei tik įmanoma, rekomenduojame įsidiegti papildomas ugniasienes ir profilaktiškai nuskenuoti svetainę ar serverį naudojant antivirusinę programą. Įpratus savo svetainę prižiūrėti kaip asmeninį kompiuterį bei pakeitus mąstymą - tai jau bus pirmas platus žingsnis išvengiant programišių pinklių“, - išskiria E. Čypas.

Kas programišiams yra sūris pelėkautuose?

Daugeliui ramybės neduodantis klausimas - kodėl į vienas svetainės programišiai laužiasi dažniau ar labiau nei į kitas? Kaip teigia specialistas, vieno atsakymo į šį klausimą nėra, bet galime atsekti tam tikras tendencijas.

„Viena svariausių priežasčių, kodėl vienos svetainės programišių taikiklyje atsiduria dažniau už kitas - naudojama programinė įranga. Pavyzdžiui, „Wordpress“ yra populiariausia TVS (turinio valdymo sistema), o tai reiškia, kad daugiausiai žmonių naudoja būtent šią TVS savo svetainės kūrimui. Tad atsiradus saugumo spragai, yra žymiai didesnis kiekis svetainių, kurias galima nulaužti. Svarbu žinoti, kad labai dažnai piktavalių taikinyje nėra didžiosios, gerai žinomos bendrovės. Dažniausiai yra netgi priešingai - taikomasi į mažesnio kalibro žaidėjus, kurie mažiau dėmesio skiria savo interneto svetainių apsaugai ir tam, kad juos nulaužti sugaištama mažiau laiko. Programišiai vadovaujasi paprasta logika - per tą patį laiką yra lengviau nulaužti keletą mažų bendrovių ir iš jų reikalauti mažesnių piniginių sumų nei fokusuotis į vieną didelę bendrovę. Žinoma, pagrindinis piktavalių tikslas ne visuomet yra pinigai. Dažnai interesai būna platesni: pavyzdžiui, lankytojų srauto nukreipimas į tam tikras svetaines, žalingo kodo įterpimas, prisijungimų ar kitų asmeninių duomenų vagystės ir pan.“, - teigia E. Čypas.

Interneto svetainės apsaugos atmintinė

„Interneto vizijos“ specialistai dalinasi specialia atmintine, kuri padės prisiminti svarbiausius interneto svetainės apsaugos aspektus bei laiku išvengti programišių dėmesio:

1. Interneto svetainės atnaujinimais ir priežiūra rūpintis nuolat, o ne jau patyrus ataką ar duomenų vagystę;
2. Visuomet naudoti ugniasienes – tai gali būti tiek įskiepai, tiek įvairūs trečiųjų šalių įrankiai, bet jos atlieką tą pačią funkciją, kaip ir ugniasienės, kurios saugo mūsų asmeninius kompiuterius;
3. Kuriant savo svetainę svarbu naudoti tik oficialius įskiepius ir dizaino temas. Jei internete randate įskiepį, kuris turėtų būti mokamas, bet jums siūloma jį atsisiųsti nemokamai, greičiausiai tai bus spąstai bei įdiegus tokį įskiepį padarysite savo svetainę lengvai nulaūžiama;
4. Vienas pačių reikšmingiausių patarimų vis dar yra senas kaip pasaulis – slaptažodžiai. Jie turėtų būti sudėtingi, sudaryti iš didžiųjų ir mažųjų raidžių, taip pat specialių simbolių ir skaičių bei raidžių. Jeigu slaptažodis bus pernelyg paprastas, pavyzdžiui, „admin“ arba „labas123“ – programišiams nereikės jaudintis nei dėl gerų apsaugų, nei dėl ugniasienių;
5. Labai svarbu įsirašyti papildomas svetainės apsaugas, pavyzdžiui, saugumo antraštes;
6. Jeigu svetainę kuriate ir prižiūrite patys, tokiais atvejais ypatingai reikėtų naudotis profesionaliais įrankiais, pavyzdžiui, „Interneto vizijos“ siūlomu „SiteLock“;
7. Svarbu turėti omenyje, kad jei jūsų svetainė talpinama saugiame serveryje, kuris yra prižiūrimas su visomis naujausiomis apsaugomis, tai savaime neapsaugo neatnaujinamos, senos ar saugumo spragų turinčios svetainės. Tokią svetainę galima prilyginti butui, kuris saugomas stambiausiomis šarvuotomis durimis, tačiau kurios paliktos praviros;
8. Jeigu kuriant ar jau prižiūrint savo interneto svetainę jums kyla klausimų ar įtarimų, bet jaučiate, kad ne visuomet žinote atsakymą, visuomet kreipkitės patarimų ar konsultacijos į specialistus. Ne visada įmanoma sutrikimus ar įsilaužėlių žalą pataisyti pačiam, ypač, neturint reikiamų įrankių.

