BEZPEČNÁ DOMÉNA

Jak na bezpečnost internetových domén

Přinášíme několik tipů, jak zabezpečit své doménové jméno proti krádeži či zneužití.

Doména je jen časově omezený záznam v databázi centrálního registru, který nese informace o objednateli, administrátorovi, nameserverech a registrátorovi. S doménou pojí držitele kontakt a informace v něm obsažené. Je tedy velice důležité hlídat si aktuálnost těchto údajů. Jedna z cest, jak zamezit možným problémům, je registrovat všechny domény na jeden kontakt, který nebude tak těžké udržovat vždy aktuální. Vzhledem k tomu, že každý NIC (centrální registr) má trochu odlišný systém evidence, je dobré zaznamenat si dobře všechny klíčové domény a v případě jakékoli změny údajů požádat o změnu na všech těchto kontaktech. Problémům s autorizací změny údajů na kontaktech nejsnáze předejdete, když o změnu požádáte ještě v době, kdy je stávající kontakt platný, tedy před změnou e-mailu či adresy. Pokud jste firma, uvádějte do kontaktních údajů vždy jméno firmy a vyplňte DIČ/IČ – tyto údaje vám pomohou v případě, že váš e-mail již není platný, nebo při změně adresy.

Na co si dát pozor

Právě e-mail je klíčem k většině akcí na doménách, a je proto velice důležité udržovat e-mailovou adresu, která je vedena na jednotlivých kontaktech, vždy aktuální a hlavně dobře zabezpečenou. Kontakt u registrátora a kontakt v databázi centrálního registru totiž není totožný záznam a jakékoliv změny je nutné provádět v obou databázích. E-mail se ve spojení s doménou stává klíčem k většině úkonů včetně změny držitele nebo registrátora. U většiny domén změníte registrátora i další údaje na základě AUTH INFO kódu (hesla), který je možné zaslat přímo z centrálního registru právě na e-mailovou adresu držitele z whois (NIC).

AUTOR
Martin Dlouhý
produktový manažer, Active24 s. r. o.

Formy zneužití

Nejčastější potíže s doménou – krádež nebo ztráta z důvodu neobnovení domény – vznikají právě v důsledku toho, že kontaktní údaje nejsou aktuální a majitel, který má aktuálně doménové jméno v pronájmu, proto nezaznamená probíhající změny. Méně častým případem krádeže domén jsou pak neshody s administrátory, kteří mají přístup k heslům a mohou je zneužít. Mezi další formy zneužití doménového jména můžeme počítat cybersquatting, tedy registraci/provoz domény porušující práva duševního vlastnictví třetích osob, které probíhá například jako robotické odchytávání neobnovených doménových jmen a následné vydírání původních držitelů. Patří sem také spory o vlastnické právo na doménu při rozpadu společností či rozchodu obchodních partnerů a v neposlední řadě kyberšikana, kde doména slouží jako nástroj „skrytého" boje proti politickým či obchodním konkurentům, bývalému zaměstnavateli apod.

Co dělat v případě, že jste se do jedné ze zmíněných situací již dostali? Respektujte následující pravidla:

- neplaťte vyděračům
- kontaktujte vždy aktuálního a původního registrátora domény
- doložte veškeré informace k danému doménovému jménu, které máte k dispozici (faktury, smlouvy)
- spolupracujte s registrátorem a centrálním registrem (NIC)
- podejte trestní oznámení

Pokud se vám nedaří získat doménu zpět, zbývá možnost obrátit se s žádostí o předběžné opatření na civilní soud nebo rozhodčí soud, který se doménovou kriminalitou zabývá. Jak se chránit při nákupu existující domény? Pokud jste zjistili, že je vaše vysněná doména na prodej a rozhodli jste se pořídit si tuto doménu, dbejte následujících rad:

- vždy sepište kupní smlouvu, ideálně s úředně ověřenými podpisy
- ověřte si identitu protistrany
- ověřte si stav domény podle whois, případně i podle obsahu na doméně (kontakt)
- ověřte historii obsahu na doméně např. na web.archive.org nebo v archivu vyhledávačů.

I když máte nyní možná pocit, že je správa domén složitější, než jste si mysleli, věřte, že když se budete řídit zmíněnými pravidly, budou vaše domény v bezpečí. Veškeré zásady se dají shrnout do několika rad.

Konsolidujte doménové portfolio pro snazší přehled a aktualizaci. To samé učiňte, pokud možno, u svých kontaktů a udržujte je co nejpřesnější a aktuální. Pokud to daný registr podporuje, zablokujte (zamkněte) změny na důležitých doménách, klíčové jsou zejména změny registrátora držitele a nameserverů. U registrátora požadujte skrytí kontaktních údajů ve whois (vždy to není možné, tato služba je podporována jen u některých registrů). U domén uvádějte reálná data, nepoužívejte falešná (smyšlená) data do kontaktů, která nelze ověřit. Pokuste se neuvádět v kontaktech freemailové adresy, které jsou při nečinnosti automaticky ukončovány, ale zároveň se vyhněte uvádění e-mailu, který je přímo na dané doméně. Nepředávejte třetím osobám přístup k „plné" administraci vašich domén. V případě, že existuje u registrátora služba upozornění na nechtěné neprodloužení doménového jména, připlaťte si tuto službu aspoň pro vaše klíčové domény. Využijte možnosti předplatného na více let, ideálně zkombinujte předplatné s upozorněním – není nic nepříjemnějšího než vrátit se z dovolené a zjistit, že vaše doména je z důvodu neprovedené úhrady v rukou někoho jiného. Nevybírejte registrátora jen podle ceny, využívejte registrátora, který zná rizika a je schopen vám rychle pomoci. ■