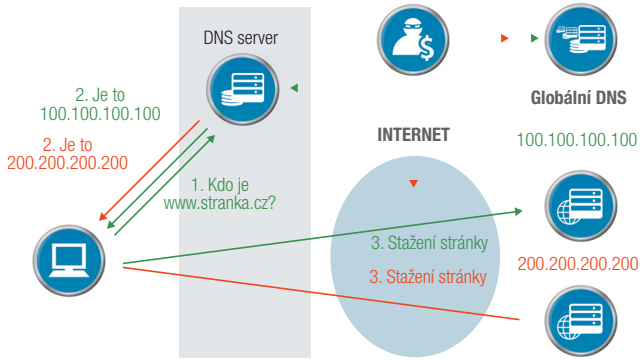
NA INTERNETU ČÍHÁ MNOHO . NA WWW.DNSSEC.CZ SPOUSTU , JAK SVOU DOMÉNU. DNSSEC, JASNÉ PRO VÁS.

O TECHNOLOGII DNSSEC

DNSSEC zvyšuje bezpečnost při používání systému doménových jmén (DNS) tím, že brání podvržení falešných, pozměněných či neúplných údajů o doménových jménech. Principem DNS je překlad jmenných internetových adres, jako například www.nic.cz nebo www.dobradomena.cz, na adresy číselné (tzv. IP adresy), kterým počítače rozumějí a jejichž pomocí dokážou zajistit zobrazování webových stránek, odesílání e-mailů, telefonování po internetu a další běžné internetové služby.

PROČ POTŘEBUJETE DNSSEC?

Jelikož DNS bylo vymyšleno podobně jako jiné základní internetové služby už před několika desítkami let v době, kdy bezpečnost nebyla nejvyšší prioritou, může se snadno stát terčem útoku. Při takovém útoku uživatelům hrozí nebezpečí, že se stanou díky tomu obětí podvodu. Mohou se totiž dostat na podvržené stránky, které budou vypadat stejně jako originální, ovšem ve skutečnosti budou patřit útočníkovi.
Za normálních okolností uživatel zadá do svého prohlížeče jmennou adresu stránky, počítač si k ní pak ze systému DNS vyhledá adresu číselnou.
U domácích uživatelů to je nejčastěji prostřednictvím serveru poskytovatele připojení (ISP). Na tuto číselnou adresu se pak připojí a v prohlížeči zobrazí příslušnou stránku. Vše probíhá zeleně označenou cestou – viz obrázek.
V případě útoku se ke stejnému jménu vrátí ze systému DNS útočníkem podvržená číselná adresa. Počítač se připojí jinam a stáhne stránku odjinud, aniž uživatel cokoliv tuší – viz červená cesta na obrázku.



Jako běžného uživatele internetu vás DNSSEC ochrání před:

- poskytnutím vašich citlivých údajů (uživatelská jména, hesla, čísla platebních karet apod.) někomu, kdo se vydává za někoho, komu věříte (tzv. phishing a pharming)
- odposlechem vašich e-mailů či jiné internetové komunikace
- manipulací prostřednictvím šíření nepravdivých informací

Jako provozovatele webových či jiných internetových služeb a stránek vás DNSSEC ochrání před:

- podvržením obsahu vašich stránek či služeb
- zneužitím důvěry vašich uživatelů k nekalým účelům
- poškozením dobrého jména vaší organizace prostřednictvím útoku na vaše doménové jméno

JSEM CHRÁNĚN POMOCÍ DNSSEC?

Aby byla ochrana před podvržením a zneužitím funkční, musí být DNSSEC zaveden jak na straně koncového uživatele, tak na straně provozovatele služby.

Zda je vámi používaná internetová služba zabezpečená pomocí DNSSEC, zjistíte nahlédnutím do registru domén www.nic.cz/whois. Zda jste jako koncový uživatel chráněn pomocí DNSSEC snadno poznáte, když navštívíte stránku www.dnssec.cz. Tam se vám zobrazí buď zelený (chráněno) nebo červený (nechráněno) klíč.

JAK SE OCHRÁNIT POMOCÍ DNSSEC

V případě koncových uživatelů ochranu DNS zapne poskytovatel internetového připojení (ISP) a v organizacích správce IT. Technicky zdatní uživatelé to mohou udělat přímo na svém počítači.

Internetové stránky a služby ochráníte vytvořením digitálních podpisů a jejich vložením do DNS buď samostatně nebo prostřednictvím poskytovatele DNS hostingu.

CZ.NIC, zájmové sdružení právnických osob | Americká 23, 120 00 Praha 2 | **Telefon:** +420 222 745 111 | **Fax:** +420 222 745 112 | **www.nic.cz**