Hrozí vám exekuce, oprášili podvodníci starý trik

Na pozoru by se měli mít lidé před e-maily, ve kterých se kybernetičtí podvodníci vydávají za zaměstnance exekutorského úřadu. V posledních dnech se s nimi totiž doslova roztrhl pytel, jak varoval Národní bezpečnostní tým CSIRT.CZ, který je provozován sdružením CZ.NIC.

„V předchozích dnech byl zaznamenán podvodný e-mail vyzývající k úhradě dlužné částky a vyhrožující případným exekučním řízením," podotkl Pavel Bašta, bezpečnostní analytik CSIRT.CZ.

Podle něj se snaží kyberzločinci touto cestou nalákat důvěřivce na podvodné webové stránky. „Kromě podrobného návodu k platbě dlužné částky vede navíc uživatele na webovou stránku imitující skutečný web jednoho z exekutorských úřadů a zde ke stažení a spuštění malwaru," zdůraznil Bašta.

Motivace počítačových pirátů je tak zřejmá. Jednak se snaží z důvěřivců pod pohrůžkou exekuce vymámit finanční prostředky, jednak chtějí propašovat do počítače důvěřivců nezvaného návštěvníka – počítačový virus.

Neklikat na odkazy, neotvírat přílohy

„Odkaz vede na doménu exekutor.site místo executor.cz. V těle e-mailu se mimo jiné doporučuje nedbat na varování antivirového softwaru," doplnil bezpečnostní analytik. Sluší se nicméně podotknout, že podvodné zprávy mohou být rozesílány klidně i ze zcela jiných adres.

Od podvodných zpráv se již distancoval i exekutorský úřad. „Neotvírejte přílohy a neklikejte na odkazy obsažené v tomto podvodném e-mailu. Náš úřad nikdy nerozesílá výzvy e-mailem, ale pouze v papírové podobě nebo datovou schránkou," uvedli zástupci Exekutorské komory.

Prakticky totožný trik s exekuční výzvou zkoušeli počítačoví piráti už před dvěma roky. Tehdy český internet zaplavily doslova tisíce podvodných e-mailů, ve kterých kyberzločinci vyzývali příjemce k úhradě neexistujících pohledávek. [celá zpráva]

Desatero bezpečného internetu

1. Důležité jsou pravidelné aktualizace celého počítače. Ty je nutné stahovat pro operační systém, bezpečnostní bránu (firewall), antivirus i další programy.
2. Některé viry dokážou bezpečnostní software v PC zablokovat. Proto je vhodné pravidelně kontrolovat, zdali funguje.
3. Škodlivé programy se často šíří prostřednictvím nevyžádané pošty. Pokud nevíte, od koho e-mail je, nikdy nestahujte jeho přílohu a neklikejte na žádné odkazy.
4. Pozor je nutné dávat na e-maily, v nichž odesílatel požaduje, abyste se přihlásili na nějakou webovou stránku a aktualizovali informace o vašem účtu.
5. Při zadávání přístupových hesel na internetových stránkách je nutné kontrolovat, zda je web zabezpečený. To poznáte například podle ikonky zámečku na liště internetového prohlížeče nebo tak, že adresa webové stránky začíná zkratkou https, kde „s" znamená bezpečná.
6. Citlivé osobní informace zadávejte vždy pouze na internetových stránkách, které bezpečně znáte.
7. Do e-mailů nepatří důvěrné informace, jako je například číslo kreditní karty nebo heslo k bankovnímu účtu. Elektronickou poštu totiž může zachytit útočník.
8. Firewall dovoluje lépe zabezpečit operační systém. Méně zkušení uživatelé by jej rozhodně neměli vypínat. Při nedostatečných znalostech je vhodné jej nechat pracovat v automatickém režimu.
9. V internetových kavárnách a na cizích počítačích se nepřihlašujte do internetového bankovnictví. V počítači mohou být nainstalované keyloggery.
10. Obezřetnost je nutná při připojení k nezašifrovaným bezdrátovým sítím. Ty totiž může kdokoliv odposlouchávat a získat tak přístup ke všem datům v cizím počítači.

mif, Novinky