Phishing (1)

Vložil/a czokl [1], 9 Listopad, 2005 - 17:41

- Anonymita [2]
- Hacking [3]
- Hacking method [4]
- Phishing & Pharming [5]

Tento pojem označuje poměrně novou metodu získávání hesel a jiných citlivých informací. Pokud chcete vědět, co přesně znamená, jak takový útok poznat a jak se proti němu bránit, čtěte dále.

Význam

Slovo Phising by se dalo přeložit jako "rhybholov" a souhrně označuje různé podvržené a zfalšované e-maily, webové stránky apod, které se z Vás pokoušejí dostat důvěrné informace. Respektive ne přímo ty stránky/e-maily, ale jejich majitelé/odesílatelé, kteří je potom docela ošklivě zneužívají. A podle serveru antiphising.org se jim to daří docela dobře. Útokům takovýchto podvodníků totiž podle tohoto serveru podléhá kolem 5% procent oslovených. Což, na nenáročnost a průhlednost triku, je opravdu dost. Další nepříznivou zprávou je, že počet těchto útoků neustále roste.

Jak poznat, že jde o podvod?

Daloby se říct, že phishing je takovým bratříčkem hoaxu, má i některé jeho znaky. Teď se pokusím napsat takovou phishignovou zprávu, která Vás může/mohla potkat:

```
//---
Dobrý den uživateli služby xxx,
cht?li bychom Vás upozornit, že dochází k inovaci naší databáze, ?ímž by m?lo dojít k
výraznému zlepšení služeb. Z naší nabídky namátkou vybíráme:
- bla bla bla
- lepší ochrana proti odhalení Vašeho hesla
- etc.
Z výše vypsaného d?vodu Vás tedy žádáme, abyste na adrese: <a href="http://x.y.cz"
title="http://x.y.cz">http://x.y.cz</a> vyplnil znovu Vaše p?ihlašovací
údaje(neposílejte svoje údaje jako odpov?? na tento mail), které se uloží p?ímo do
již p?ipravené nové databáze. Pokud informace nevložíte, nejsme bohužel schopni na
Vaší registraci brát z?etel a Vy budete muset projít celou registra?ní fází znovu.
P?edem d?kujeme za Vaší ochotu a t?šíme se na další spole?nou spolupráci.

Váš Admin služby xxx
---//
```

Takto nějak by mohl vypadat e-mail, který dostanete do schránky, pak už útočník pouze čeká na to jak se zachováte. Samozřejmě v podobném duchu se nese i odkaz, kde se většinou nachází formulář na vyplnění údajů, pro věrohodnost takové stránky je provázaná s originální stránkou posyktovatele služby(banka, hosting, atd.). Ale k tomu se ještě dostaneme. Z pomyslného druhého soudku je mail/web s takovýmto obsahem(účinný hlavně na freemaily):

```
//---
Vážený zákazník?,
protože se domníváme, že se na našem serveru nacházejí tkzv. mrtvá konta, což jsou
konta, které byli za poslední t?i m?síce neaktivní a proto nep?edpokládáme, že se
n?který uživatel k takovému kontu ješt? vrátí. Abychom si byli 100% jistí, prosím
```

```
vypl?te údaje na následují stránce: xxx.yyyy.zz, d?kujeme za spolupráci a doufáme, že
nám zanecháte p?íze?. Pokud nemáte s naší službou nic spole?ného, hluboce se omluváme
a tento e-mail ignorujte.
---//
```

Další, zcela odlišný typ zprávy je pokus o přemluvení uživatele aby si změnil heslo sám, mail by mohl vypadat takto:

```
//---
Vážený uživateli,
z d?vodu opravy/inovace/whatever, která bude provedena mezi dny xx.x.xxxx - xx.x.xxxx
bychom Vás cht?li požádat o zm?nu hesla na námi vygenerované: h45df4gd (prost? n?jaký
neskute?ný ?et?zec znak? a ?isel). Nu?iníte-li tak, m?žete p?ijít o svoje data.
Váš admin
---//
```

Takovýchto vzorových e-mailů by mohlo být víc, ale nechci zbytečně protahovat článek, navíc, všechny takové podvodné e-maily mají společné znaky. Jsou to:

chyby - gramatické, slohové, překlepy... - bohudík, čast takovýchto podvodníků svoje útoky uspěchává, proto se v nich často objevují do očí bijící chyby. Je sice pravda, že takový nepovedný dopis může sesmolit i sekretářka, ale přecejen ona je za to placená, má určité vzdělání(!!!) a její sloh by měl trochu za něco stát.
neformálnost - tento znak souvisí tak trochu s prvním. Je to opět způsobeno tím, že někteří autoři (amatéři) si nepotrpí na formálnost a tak můžou používat nespisovné a neformální výrazy. což by se u profi firmy nemělo stávat.
hodně technických výrazů, obkecávání - docela používaná metoda je taky zamotání hlavy uživatele. Útočník využívá neznalosti většiny uživatelů a celou zprávu zabalí do cizích a odborných slov, kterým třeba ani sám nerozumí. Vlastně to není ani potřeba, Účelem je zmást uživatele, což se většinou podaří a procento úspěšnosti útočníka se tím pádem zvyšuje.
zprávy bez diakritiky - pokud se aspoň trochu pohybujete v nějaké komunitě lidí na i-netu, určitě víte, že většina lidí píše bez diaktritiky a to z důvodu rozdílného nastavení kódování různých uživatelů, podpory jednotlivých národních znaků v různých aplikacích apod. Ale nezasvěcený člověk(sekretářka, která by normálně dostala napsání oznámení na starost) tohle určitě neudělá. Takže pokud dostanete mail nebo uvidíte na webu text bez diaktritiky, buďte si jisti, že jde o podvod. Nebo, pokud útočník rozesílá své maily pomocí PHP bude používat (pravděpodobně)taky text psaný bez diakritiky, protože zase narazí na problém s kódováním češtiny. Samozřejmě některým nastavením hlavičky mailu jde toto odstranit, ale to je věc jiná.
vykřičníky - další varování pro Vás může být, když se na konci věty objeví dva a více vykřičníků, otazníků nebo teček. Takováhle přehnaná interpuknce se pužívá hlavně u hoaxů a jelikož je phishing hoaxům velmi podobný, může se vyskytovat i zde.
modré z nebe, metoda cukru a biče - Další věc, která by Vás měla přesvědčit je slibování různých bonusů a výhod buď v nové (fiktivní) verzi služby a nebo přímo za vyplnění choulostivých údajů (vyplňte jméno a heslo a uvidíte britney spears nahou:)) a nebo naopak různých hrozeb, nevyplníte-li to, co se po Vás žádá.
nátlak, panika - to už jsem nakousl minulým bodem, útočník se může pokoušet vyvinout nátlak, dotutit Vás panikařit, abyste nemohli racionálně přemýšlet a vyplnili to, co žádá. Obvykle se straší ztrátou dat nebo zrušení celého účtu, ale samozřejmě může to být úplně něco jiného, v kreativitě se meze nekladou.
nearograntní chování - ačkoli se může útočník pokusit o nátlak, bude vždy 100% slušný. Žádné arogantní chování, na jaké jsme zvyklí z našich státem placených úřadů čekat rozhodně nemůžete. Nakonec, je to útočník, který žádá službu, ne Vy. I když u soukromých objektů by slušnost k zákazníkovi by měla být též na předním místě, nezřídka se s arogantním a nebo povýšeným chováním můžeme zejména ze strany poskytovatelů free služeb setkat.
neodpovídat přímo na mail - jako poslední znak jsem vybral, že v každém podvodném mailu by neměla chybět hláška ve smyslu, že na mailovou adresu, ze které přišel mail v žádném případě neodpovídejte a to proto, že 99.99% procent takových mailů je zfalšovaných. Ale na to ještě dojde. I když by Vás kontaktoval skutečný poskytovatel, můžete si být 100% jistí, že uvede mail na případné dotazy, telefonní čislo a jméno osoby, kterou je třeba kontaktovat, u útočníka byste toto hledali

marně(v drtivé většině prípadů).

Příště se podíváme na technickou stránku věci.

URL článku: https://security-portal.cz/clanky/phishing-1

Odkazy:
[1] https://security-portal.cz/users/czokl
[2] https://security-portal.cz/category/tagy/anonymita
[3] https://security-portal.cz/category/tagy/hacking
[4] https://security-portal.cz/category/tagy/hacking-method
[5] https://security-portal.cz/category/tagy/phishing-pharming