Analýza podvodných e-mailových zpráv

pro AOBP

17. dubna 2018

VIAVIS střežíme podstatné

VIAVIS a. s. | Obránců Míru 237/35 | 703 00 Ostrava | tel.: +420 595 174 250 | e-mail: info@viavis.cz | web: www.viavis.cz

zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě | Oddíl B, číslo vložky 2249 | IČ 25848402 | DIČ CZ25848402

ID Dokumentu	ANALYZA_AOBP	**Verze**	1
Zodpovídá	Ing. Jan Bonczek	**Stav**	K předání
Klasifikace		**Určeno pro**	AOBP
Počet výtisků	1	**Výtisk číslo**	1

VIAVIS a. s. | Obránců míru 237/35 | 703 00 Ostrava | tel.: +420 595 174 250 | e-mail: info@viavis.cz | web: www.viavis.cz | zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě | Oddíl B, číslo vložky 2249 | IČ 25848402 | DIČ CZ25848402

1 Úvod

Cílem dokumentu je analyzovat phishingové e-maily, které byly rozesílány pod adresou z domény AOBP.

Tento dokument obsahuje výsledky **analýzy phishingových e-mailů**.

V této zprávě jsou popsána zjištění učiněná během analýzy i doporučení z nich vyplývající.

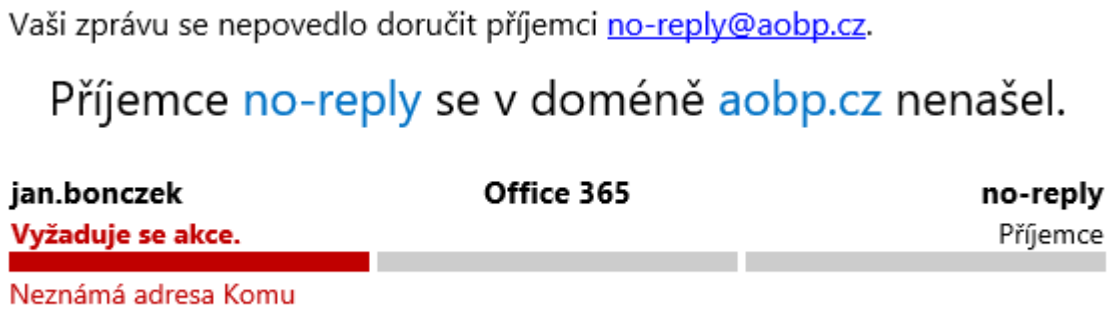
Analýza byla provedena v měsíci dubnu roku 2018. Na provedení se zúčastnili za hodnotitele:

- Ing. Jan Bonczek, konzultant

2 Zjištěné skutečnosti

Zjištění:

Jedná se o útok, kdy je podvržen odesílatel e-mailů. Tento typ útoku nevyžaduje žádné zvláštní znalosti a je tak poměrně běžným.[1] Jako odesílací adresa je uvedena no-reply@aobp.cz. Tato adresa v doméně AOBP neexistuje, což lze jednoduše ověřit pokusem o odeslání e-mailu na tuto adresu.



Zjištění:

AOBP používá externí e-mailový server společnosti Microsoft. Tento server má zavedenou ochranu SPF (Sender Policy Framework). SPF funguje jako ochrana před tím, aby nebylo možné odesílat e-maily z domény @aobp.cz z jiného e-mailového serveru než serveru, který je k tomu oprávněn. Respektive SPF pevně svazuje doménu se SMTP serverem. Nicméně je vyžadováno, aby bylo SPF podporováno odesílatel i příjemcem, respektive příjemce musí mít nastaveno, že nebude přijímat zprávy z jiného než oprávněného e-mailového serveru v opačném případě se ochrana SPF neuplatní.[2]

Zjištění:

Z dostupných informací, kdy byly u některých příjemců tyto podvodné e-maily zařazeny do SPAMu, lze usoudit, že některé servery a jejich antispamové funkce správně rozpoznaly, že se jedná o spam.

Zjištění:

V případech, kdy nedojde ke správné reakci antispamových funkci a e-mail je doručen konečnému uživateli, lze ověřit správnost odesílatele například podle hlavičky e-mailu. Tato možnost je však pro běžného uživatele komplikovaná a vyžaduje technické znalosti dané problematiky.

---

[1] https://technet.idnes.cz/e-mail-falesna-adresa-odesilatele-email-spoofing-ft6-/sw_internet.aspx?c=A160422_161912_sw_internet_pka

[2] https://www.root.cz/clanky/stop-podvrzenym-e-mailovym-adresam-ve-spamu/

Z hlaviček získaných z podvodných e-mailů, bylo možné identifikovat zdrojový server. Je však nutné upozornit, že dany server mohl být také pouze zneužit a není reálným původcem.

```
iix3.rumahweb.com ([103.247.9.3])
port=51782 helo=webmail.exit9-indonesia.com
```

Zjištění:

Z obsahu podvodné zprávy je zřejmé, že se jednalo o cílený útok na AOBP.

3 Závěr

Z formy podvodného e-mailu je zřejmé, že se jednalo o cílený útok, kdy měl útočník pravděpodobně seznam kontaktů AOBP. Jako ochrana proti těmto a dalším útokům na e-mailové služby lze použít například šifrování, nebo elektronický podpis.[3] Zjištění, co bylo zdrojem úniku e-mailových adres členů AOBP by mohlo být předmětem dalšího šetření.

V zásadě není možné tomuto typu útoku na straně odesílatele nikdy zcela zabránit, jelikož je nutné správně konfigurovat antispamové funkce na straně příjemce. Je nutné zdůraznit, že tímto způsobem je možné podvrhnout jakoukoli adresu v doméně AOBP, nikoliv pouze adresu, která neexistuje.

[3] https://www.govcert.cz/cs/informacni-servis/doporuceni/2328-podvrzene-e-maily/

4 Informační e-mail

Z technické analýzy phishingových e-mailů a dostupných informací vyplývá, že se organizace AOBP pravděpodobně stala obětí cíleného phishingového útoku. Jednalo se o tzv. „útok podvržení odesílatele“, kdy byly z podvržené e-mailové adresy no-reply@aobp.cz, rozesílány podvodné e-mailové zprávy na členské firmy AOBP, ale také např. Ministerstvu obrany ČR.

E-mailová adresa no-reply@aobp.cz, však v doméně aobp.cz neexistuje. SMTP server, který tyto podvodné e-mailové zprávy rozesílal není SMTP serverem, který používá naše organizace pro e-mailovou komunikaci. Naše organizace používá výhradně e-mailové servery společnosti Microsoft.

Pro účinnou obranu proti tomuto typu útoku je nutné adekvátní nastavení antispamových funkcí jako je například SPF (Sender Policy Framework). SPF pevně přiřazuje doméně SMTP servery, které pro ni mohou odesílat poštu a pokud je e-mail odeslán z jiného SMTP serveru, jedná se o spam. Je však nutné, aby byla tato funkce nastavena na straně odesílatele i příjemce.