ZŁOWIENI PRZEZ OSZUSTÓW

CO ZROBIĆ, GDY PADŁEM OFIARĄ SMS-OWEGO PHISHINGU?

OPŁATA ZA PRZESYŁKĘ KURIERSKĄ, ODŁĄCZYMY CI PRĄD ORAZ INNE HACZYKI

W ostatnim czasie można zaobserwować wzrost aktywności hakerów w ramach tzw. phishingu czyli oszustw skoncentrowanych na wydobycie wrażliwych danych poprzez podszywanie się pod rozmaite instytucje – banki, popularne platformy streamingowe, spółki energetyczne.
Phishing nie jest nową formą oszustwa, a jego ofiarą paść może każdy, nawet duże podmioty gospodarcze. O jednej z takich spraw zakończonych happy endem dzięki interwencji kancelarii pisaliśmy tutaj:

NIEZWŁOCZNE ODCIĘCIE OSZUSTÓW OD NASZYCH DANYCH

- POINFORMOWANIE BANKU O ZAISTNIAŁYM ZDARZENIU Z WNIOSKIEM O 72-GODZINNĄ BLOKADĘ RACHUNKU OSZUSTA
- ZMIANA DANYCH LOGOWANIA NAZWA UŻYTKOWNIKA + HASŁO + MAIL
- WŁĄCZENIE UWIERZYTELNIANIA DWUSKŁADNIKOWEGO NP. MAIL + SMS
- UNIEWAŻNIENIE DOWODU OSOBISTEGO PRZEZ INTERNET, W URZĘDZIE GMINY/MIASTA/DZIELNICY, W KONSULACIE
- ZASTRZEŻENIE LUB TYMCZASOWA BLOKADA KARTY PŁATNICZEJ W PLACÓWCE BANKU, PRZEZ TELEFON LUB POPRZEZ BANKOWOŚĆ ELEKTRONICZNĄ

Brysiewicz Bokina Sakławski
KANCELARIA PRAWNA

ZAWIADOMIENIE ORGANÓW ŚCIGANIA W NAJBLIŻSZEJ JEDNOSTCE POLICJI LUB PROKURATURY

W JAKI SPOSÓB ZGŁOSIĆ PRZESTĘPSTWO?
Ustnie lub pisemnie, w najbliższej jednostce policji lub prokuratury.

DLACZEGO WARTO POWIADOMIĆ ORGANY ŚCIGANIA?
Postępowanie prowadzone przez policję/prokuratora wraz z naszym zaangażowaniem może zmaksymalizować szanse na ujęcie oszustów i odzyskanie pieniędzy.

CO ORGANY MOGĄ ZROBIĆ, ABY NAM POMÓC?
Prokurator w szczególności może wystąpić o udostępnienie i zabezpieczenie danych informatycznych (art. 218a KPK), zablokować transakcję bankową (art. 106a Prawa bankowego), a po namierzeniu sprawcy i przedstawieniu zarzutów może nastąpić zabezpieczenie majątkowe (art. 291 KPK) na poczet m.in. zwrotu pieniędzy pokrzywdzonemu przestępstwem.

OSTRZEŻ INNYCH UŻYTKOWNIKÓW

CSIRT[1] DZIAŁAJĄCY PRZY NASK[2] TO ZESPÓŁ SPECJALISTÓW ODPOWIEDZIALNYCH ZA CYBERBEZPIECZEŃSTWO. ICH DZIAŁANIA MAJĄ PRZYCZYNIAĆ SIĘ DO ZWIĘKSZENIA BEZPIECZEŃSTWA UŻYTKOWNIKÓW SIECI.

Formularz zgłoszenia incydentu na stronie WWW: www lub przez wysłanie wiadomości SMS do instytutu 799-448-084 umożliwia zgłaszania do CSIRT podejrzanych wiadomości, domen internetowych lub innych niebezpiecznych treści

W oparciu o weryfikowane zgłoszenia użytkowników, CSIRT aktualizuje listę niebezpiecznych domen WWW. Warto ją przejrzeć zanim klikniemy w nieznany link pochodzący z podejrzanego źródła: www

[1] COMPUTER SECURITY INCIDENT RESPONSE TEAM.
[2] NAUKOWA I AKADEMICKA SIEĆ KOMPUTEROWA – PAŃSTWOWY INSTYTUT BADAWCZY.

Brysiewicz Bokina Sakławski
KANCELARIA PRAWNA

CZY DA SIĘ ODZYSKAĆ PIENIĄDZE Z PHISHINGU?

W TEORII JEST TO JAK NAJBARDZIEJ MOŻLIWE. FAKTYCZNY SKUTEK ZALEŻY JEDNAK OD BIEGŁOŚCI SPRAWCÓW W ZESTAWIENIU Z ZAANGAŻOWANIEM NASZYM ORAZ ORGANÓW ŚCIGANIA.

DROGA SĄDOWO-PROKURATORSKA

- zabezpieczenie majątkowe tytułem przyszłego zwrotu majątku pokrzywdzonemu
- wniosek o naprawienie szkody wyrządzonej przestępstwem
- naprawienie szkody na drodze cywilnej

PROCEDURA CHARGEBACK

- oferowana przez większość banków
- zgłasza się nieautoryzowane płatności twoją kartą lub pobory z rachunku (np. poprzez formularz internetowy, infolinię)
- po przeprocesowaniu reklamacji wystawca karty może podjąć decyzję o zwrocie pieniędzy na nasze konto

NIE DA SIĘ UKRYĆ, ŻE POSTĘPOWANIA W PRZEDMIOCIE OSZUSTW INTERNETOWYCH CZĘSTO KOŃCZĄ SIĘ FIASKIEM. JEDNAKŻE, NIE JEST TO BEZWZGLĘDNA REGUŁA. CO JAKIŚ CZAS MOŻEMY PRZECZYTAĆ O UJĘCIU SPRAWCÓW CYBER-WYŁUDZEŃ DANYCH I PIENIĘDZY.

Brysiewicz
Bokina
Sakławski
KANCELARIA PRAWNA