Informacja dla użytkowników usługi kluczowej świadczonej przez Gdańskie Przedsiębiorstwo Eneregtyki Cieplnej Sp. Z o.o. w zakresie zagrożeń cyberbezpieczeństwa i stosowania skutecznych sposobów zabezpieczania się przed nimi

W obliczu narastających zagrożeń związanych z cyberbezpieczeństwem pragniemy uświadomić Państwa, na co szczególnie zwracać uwagę, aby uniknąć potencjalnych zagrożeń. Zgodnie z postanowieniami Ustawy o Krajowym Systemie Cyberbezpieczeństwa (UKSC), chcielibyśmy poruszyć kilka istotnych kwestii dotyczących bezpieczeństwa w świecie online:

- Phishing – Jak go rozpoznać i nie dać się oszukać
  - Poniższy e-mail jest typowym przykładem próby phishingu, mającej na celu wyłudzenie danych, pieniędzy lub zainfekowanie komputera.
    "Dzień dobry,
    W związku z ostatnią transakcją, prosimy o pobranie faktury za zakupione usługi. Proszę kliknąć w poniższy link, aby pobrać dokument: [link]

    Pozdrawiamy,
    Zespół Obsługi Rozliczeń"
  - Opis zagrożenia
    - To schematyczne przedstawienie typowego ataku phishingowego, który wykorzystuje społeczną inżynierię i manipulację, aby wyłudzić dane od nieświadomych ofiar.
  - Przebieg
    - **Przesłanie sugestywnej wiadomości e-mail:** Atak rozpoczyna się od wysłania do ofiary e-maila, który wydaje się być autentyczny i sugeruje pilną potrzebę działania. Może to być na przykład fałszywa faktura lub informacja o rzekomej zmianie danych konta.
    - **Manipulacja linkiem:** E-mail zawiera link, który sugeruje konieczność kliknięcia w celu uzyskania szczegółowych informacji lub wykonania jakiejś czynności. Ten link prowadzi do fałszywej strony internetowej.
    - **Przekierowanie do fałszywej strony:** Po kliknięciu linka ofiara zostaje przekierowana do strony internetowej, która jest wierną kopią oryginalnej strony, na przykład strony dostawcy usług czy banku. Ta fałszywa strona jest starannie zaprojektowana, aby wyglądać autentycznie, często zawiera grafiki, logo i kolorystykę zbliżoną do oryginału.
    - **Wyłudzenie danych:** Na fałszywej stronie ofiara jest proszona o wprowadzenie swoich danych osobowych, takich jak loginy, hasła, dane karty kredytowej itp. Te informacje są przesyłane przestępcom, którzy następnie mogą je wykorzystać do kradzieży tożsamości lub dokonania oszustw finansowych.
  - Zapobieganie
    - **Ostrożność podczas uruchamiania linków:** Użytkownicy powinni być ostrożni przy klikaniu na linki w e-mailach, zwłaszcza gdy wiadomość wydaje się być podejrzana lub pochodzi od nieznanych nadawców. Należy unikać klikania w linki zawierające prośby o podanie poufnych danych lub podejrzane treści.
    - **Weryfikacja nadawcy:** Przed podjęciem jakichkolwiek działań należy zweryfikować tożsamość nadawcy wiadomości e-mail. Upewnienie się, że nadawca jest autentyczny, może pomóc w uniknięciu kliknięcia na linki do fałszywych stron.
    - **Sprawdzanie adresu URL:** Przed podaniem jakichkolwiek danych na stronie internetowej należy sprawdzić adres URL, aby upewnić się, że jest on zgodny z adresem

oryginalnej strony. Fałszywe strony często mają podobne, ale nie identyczne adresy URL.

- **Uważne czytanie treści e-maila:** Należy dokładnie czytać treść e-maila, zwłaszcza jeśli zawiera ona prośby o natychmiastowe działanie, groźby lub obietnice nagród. Podejrzane lub nietypowe treści mogą wskazywać na próbę phishingu.
- **Stosowanie filtrów antyspamowych:** Korzystanie z oprogramowania antyspamowego może pomóc w wykryciu i blokowaniu e-maili zawierających potencjalnie szkodliwe treści, w tym próby phishingu.
- **Używanie uwierzytelnienia wieloskładnikowego (MFA):** Aktywowanie dwuetapowej weryfikacji dla kont online może dodatkowo zabezpieczyć konto przed nieautoryzowanym dostępem, nawet jeśli haker uzyskał dostęp do loginu i hasła.

- Strona internetowa: autentyczna czy fałszywa?
  - Opis zagrożenia
    - To zagrożenie dotyczy sytuacji, gdy użytkownik odwiedza stronę internetową, ale nie ma pewności, czy jest ona autentyczna, czy też fałszywa. Fałszywe strony internetowe są często tworzone przez hakerów w celu przechwycenia poufnych informacji, takich jak dane logowania, informacje finansowe itp.
    - Zagrożenie związane z autentycznością stron internetowych wymaga ostrożności ze strony użytkowników oraz stosowania się do praktyk bezpieczeństwa online, aby uniknąć potencjalnych konsekwencji związanych z wyłudzeniem danych.
  - Przebieg
    - **Odwiedzenie strony:** Użytkownik wchodzi na stronę internetową, która wydaje się być autentyczna, na przykład stronę banku, sklepu internetowego lub platformy społecznościowej.
    - **Brak pewności:** Użytkownik może nie być w stanie jednoznacznie określić, czy strona jest autentyczna. Fałszywe strony często są bardzo podobne do oryginalnych, z grafiką, logiem i treściami, które są łudząco podobne do tych na prawdziwej stronie.
    - **Ryzyko wyłudzenia danych:** W przypadku, gdy użytkownik wprowadzi swoje dane osobowe, takie jak loginy, hasła, dane karty kredytowej itp., na fałszywej stronie, są one przechwytywane przez hakerów. To może prowadzić do kradzieży tożsamości, oszustw finansowych lub innego rodzaju nadużyć.
  - Zapobieganie
    - **Sprawdzanie adresu URL:** Użytkownicy powinni zawsze sprawdzać adres URL strony internetowej, aby upewnić się, że jest on zgodny z adresem oryginalnej strony.
    - **Uważne obserwowanie:** Zwracanie uwagi na wszelkie podejrzane elementy na stronie, takie jak błędy w pisowni, brak certyfikatów bezpieczeństwa SSL itp.
    - **Używanie oprogramowania antywirusowego:** Instalacja oprogramowania antywirusowego może pomóc w wykryciu i blokowaniu dostępu do fałszywych stron internetowych.
    - **Uczestnictwo w szkoleniach z zakresu bezpieczeństwa internetowego:** Edukacja użytkowników na temat technik phishingowych i sposobów rozpoznawania fałszywych stron internetowych może być skuteczną metodą ochrony przed tym zagrożeniem.