Zgodnie z Ustawą z dnia 5 lipca 2018r o krajowym systemie cyberbezpieczeństwa przekazujemy Państwu informacje dotyczące zagrożeń oraz sposobu zabezpieczania się przed nimi w przestrzeni Internetu w przypadku korzystania z systemu eXpress.

System **eXpress** to moduł umożliwiający przeglądanie informacji o kontenerach, generowanie raportów, bukowanie, awizację, zatrzymywanie oraz zwalnianie kontenerów przez służby graniczne. Jest on dostępny bezpośrednio przez naszą stronę Internetową.

Spółka Gdynia Container Terminal Sp. z o.o. i jej służby IT sprawują nadzór nad prawidłowym funkcjonowaniem systemów udostępnianych użytkownikom i stosują odpowiednie zabezpieczenia i polityki w celu minimalizacji zagrożeń w cyberprzestrzeni. Nie mniej jednak, bez wsparcia użytkowników, ich świadomości i właściwego zachowania nie zawsze jesteśmy w pełni zapewnić bezpieczeństwo informacji. Dlatego też, zachęcamy Państwa do zapoznania się z informacjami poniżej, tak abyśmy wspólnie zapobiegali niepożądanym incydentom.

Głównymi zagrożeniami w przestrzeni Internetu w przypadku korzystania z systemu eXpress są:

- podszycie się atakującego pod legalną stronę internetową (tak zwany *phishing*), do której link został wysłany do Państwa drogą elektroniczną za pomocą *spamu*;
- złośliwe oprogramowanie zainstalowana na Państwa komputerze, które wykrada hasała do systemów czy do kont bankowych (*malware, wirusy, robaki itd.*.);
- kradzież tożsamości;
- blokowanie dostępu do usług;
- zaszyfrowanie danych na komputerze przez złośliwe oprogramowanie.

Prosimy o stosowanie się do podstawowych zasad bezpieczeństwa:

- korzystanie z aktualnego oprogramowania antywirusowego z firewallem;
- wykonywanie systematycznych kopii bezpieczeństwa;
- chronienie przed osobami nieupoważnionymi swych loginów, haseł, PIN-ów oraz innych narzędzi służących do uwierzytelniania i autoryzacji;
- stosowanie trudnych do złamania i odgadnięcia haseł do logowania (najlepiej wykorzystać generator haseł); można również korzystać z dodatkowego rozwiązania jakim jest aplikacja menadżera haseł;
- nieprzesyłanie loginów i haseł za pomocą poczty e-mail lub przez telefon; pracownicy działu IT Gdynia Container Terminal Sp. z o.o. nigdy nie proszą użytkowników o podawanie danych tego rodzaju;
- częsta zmiana haseł służących do uzyskania dostępu do kont w internecie lub oprogramowaniu;
- niepodawanie w sieci danych osobowych oraz haseł, jak również nie przesyłanie i umieszczanie swoich zdjęć;
- niezapisywanie haseł bezpośrednio w przeglądarce internetowej, a wykorzystywanie do tego celu menadżera haseł;
- nieklikanie na linki w poczcie elektronicznej pochodzącej z nieznanych i podejrzanych źródeł;
- chronienie swoich kont na serwisach społecznościowych;
- nie pobieranie plików z nieznanych źródeł (nie otwieranie plików w poczcie elektronicznej z nieznanego źródła);
- zwracanie uwagi na wiadomości e-mail pochodzące z nieznanych nam adresów lub których nadejścia się nie spodziewaliśmy;
- sprawdzane każdego pobranego pliku z Internetu systemem antywirusowym;

- niepodłączanie do komputera nieznanych urządzeń (np. znalezionego urządzenia typu pendrive ’a);
- wchodząc na daną stronę internetową zweryfikowanie czy jest zabezpieczona certyfikatem SSL (ikona kłódki przy adresie strony) wydanym dla właściciela danej witryny internetowej;
- zwracanie uwagi czy strona internetowa, którą chcemy odwiedzić ma właściwy adres (np. czy nie ma podmienionej jednej litery tak, aby łudząco przypominać właściwy adres) i czy składa się on z liter, a nie z pliku graficznego reprezentującego litery;
- systematyczne skanowanie swojego komputera w celu wykrycia nie pożądanych aktywności i wirusów, ponieważ oprogramowanie antywirusowe nie zawsze wykrywa w pełni złośliwe oprogramowanie;
- czytanie regulaminów, polityk bezpieczeństwa oraz warunków korzystania z usług dostępnych w internecie;

Dodatkowe informacje na temat sposobów zabezpieczania się przed zagrożeniami można znaleźć pod następującymi linkami:

  - Cztery proste kroki dla własnego bezpieczeństwa: https://www.sans.org/sites/default/files/2019-09/201910-OUCH-October-Polish.pdf;
  - Oszustwa za pośrednictwem mediów społecznościowych:
  - https://www.sans.org/sites/default/files/2019-09/201909-OUCH-September-Polish.pdf;
  - Jak uniknąć błędów korzystając z poczty e-mail ?: https://www.sans.org/sites/default/files/2018-10/201810-OUCH-October-Polish_1.pdf;
  - Tworzenie haseł w prostszy sposób: https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Polish.pdf;
  - Ochrona przed złośliwym oprogramowaniem: https://www.sans.org/sites/default/files/2018-06/201806-OUCH-June-Polish.pdf.

W sytuacji wykrycia incydentu bezpieczeństwa, anomalii w funkcjonowaniu systemu eXpress lub dalszych pytań prosimy o kontakt pod adresem: cyberbezpieczenstwo@gct.pl