Cyberbezpieczeństwo

W celu zapewnienia odpowiedniego poziomu ochrony danych w świadczonych usługach, a także w celu spełnienia wymagań prawnych w odniesieniu do cyberbezpieczeństwa w Specjalistycznym Szpitalu Wojewódzkim w Ciechanowie został wdrożony System Zarządzania Bezpieczeństwem Informacji w oparciu o wymagania normy ISO/IEC 27001 oraz ISO 22301.

Zastosowane zabezpieczenia mają na celu zapewnienie, że pacjenci, pracownicy, wykonawcy oraz użytkownicy reprezentujący stronę trzecią rozumieją swoje obowiązki, posiadają odpowiednie kompetencje niezbędne do wyznaczonych im ról, są świadomi oraz wypełniają swoje obowiązki związane z bezpieczeństwem informacji w Specjalistycznym Szpitalu Wojewódzkim w Ciechanowie.

Zabezpieczenia mają dotyczyć przede wszystkim:

- utrzymania bezpieczeństwa informacji przetwarzanych w ramach świadczonych usług,
- ograniczenia dostępu do informacji i środków przetwarzania informacji tylko dla osób uprawnionych,
- stosowania zabezpieczeń w dostarczanych usługach zgodnie z umowami serwisowymi zawartymi z dostawcami,
- zapobieganiu utracie, uszkodzeniu, kradzieży, zakłóceniu informacji lub naruszeniu aktywów,
- ochrony przed uszkodzeniami lub zakłóceniami w odniesieniu do informacji oraz środków przetwarzania informacji,
- ochrony przed nieuprawnionym dostępem do systemów i usług, jak również ochrony przed nieautoryzowanym dostępem fizycznym,
- uczynienie użytkowników odpowiedzialnymi za zabezpieczenie informacji na odpowiednim poziomie w ich codziennej pracy.

W celu bliżej zrozumienia zagrożeń cyberbezpieczeństwa, a jednocześnie stosowania skutecznych środków zabezpieczających przed zagrożeniami, przekazujemy Państwu podstawowe zasady cyberbezpieczeństwa:

- zabezpieczaj swoje dane (takie jak PESEL, nr dowodu, nr paszportu, nr karty płatniczej),
- korzystaj z aktualnego oprogramowania antywirusowego na swoich urządzeniach,
- ogranicz dostęp do swoich urządzeń mobilnych (hasło, PIN, odcisk palca),
- potwierdzaj swoje logowanie korzystając z wieloetapowego uwierzytelniania,
- instaluj oprogramowanie z zaufanych źródeł,
- stosuj zasadę organicznego zaufania, gdy osoby lub urządzenia pytają o Twoje dane,
- nie klikaj i nie otwieraj załączników/linków jeśli Domena nadawcy emaila, jeśli Domena nadawcy jest inna,
- Nie wchodź w linki umieszczane w wiadomościach email,
- konto zostało zablokowane? Nie klikaj,
- profil w serwisie społecznościowym wymaga weryfikacji? Nie klikaj,
- ze względów bezpieczeństwa trzeba ustalić nowe hasło? Nie klikaj,
- trzeba autoryzować płatność? Nie klikaj,
- zweryfikuj czy adres strony WWW jest prawidłowy:
  - czy jest to prawidłowa domena (np. allegro.pl, a nie „allegro-payment.md”)
  - czy nie ma literówek i zmienionych znaków (np. „I” zamiast „l”, „rn” zamiast „m”)
  - czy w adresie strony nie ma „dziwnych ogonków” z innych alfabetów (np. „ķ” zamiast „k”)
- weryfikuj informację innym kanałem kontaktowym (lub samodzielnie inicjując kontakt), weryfikuj nadawcę wiadomości:
  - ktoś prosi w mailu o przelew na nowy numer konta? Zadzwoń lub napisz SMS z prośbą o potwierdzenie
  - firma czy bank dzwoni i pyta Twoje dane? Oddzwoń samodzielnie, wybierając numer ze strony WWW lub napisz na czacie na stronie firmy
  - dostajesz SMS z informacją o konieczności zapłaty? Zadzwoń (na numer ze strony WWW wpisanej ręcznie) i zapytaj o szczegóły

Bezpieczne hasło:

- łatwe do zapamiętania, zbudowane z nazw przedmiotów/czynności codziennego użytku, fragmentów ulubionych piosenek/wierszy itp.,
- nieskojarzone z nami - nie powinno zawierać imienia, nazwiska, daty urodzenia itp.,
- nie należy wykorzystywać sekwencji kolejnych liter, liczb lub innych znaków, np: abcd, 123456, QWERTY,
- nie korzystaj z opcji zapamiętywania haseł w przeglądarce ani z funkcji autologowania,
- bezpieczne hasło powinno się składać z co najmniej 12 znaków, ale im więcej tym lepiej,
- zabezpiecz wszystkie konta za pomocą uwierzytelniania dwuetapowego (2FA).

Zabezpieczony plik

- wykorzystaj narzędzie do kompresji plików (np. 7zip) z opcją nadania hasła do archiwum,
- korzystaj z narzędzi z wbudowanym mechanizmem szyfrowania (np. Word, Excel),
- korzystaj z dedykowanych narzędzi szyfrujących dane/plik (np. PGP),
- pamiętaj!!!: hasło do pliku zawsze wysyłaj odbiorcy innym kanałem niż przekazany był plik, np. SMS-em.

Jakich zagrożeń możemy spodziewać się w internecie

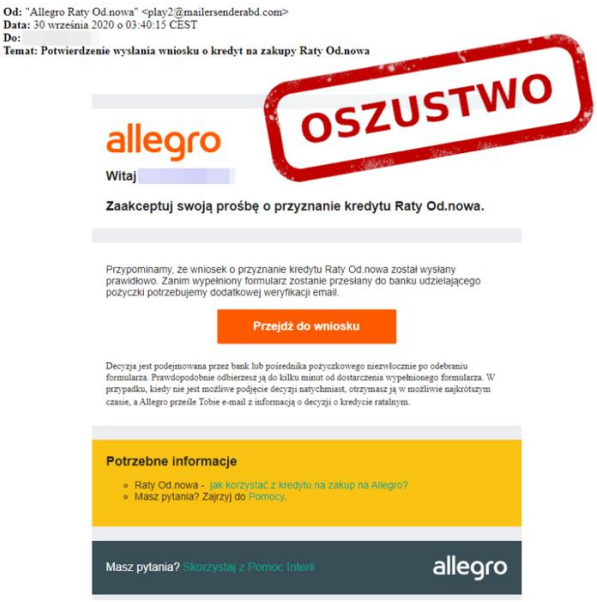
Przestawiamy zagrożenia z którymi mogą się Państwo spotkać w internecie, najpoważniejsze zagrożenia w internecie to phishing i ransomware, wyłudzenia danych do bankowości internetowej oraz wszelkie inne oszustwa, które prezentujemy poniżej:

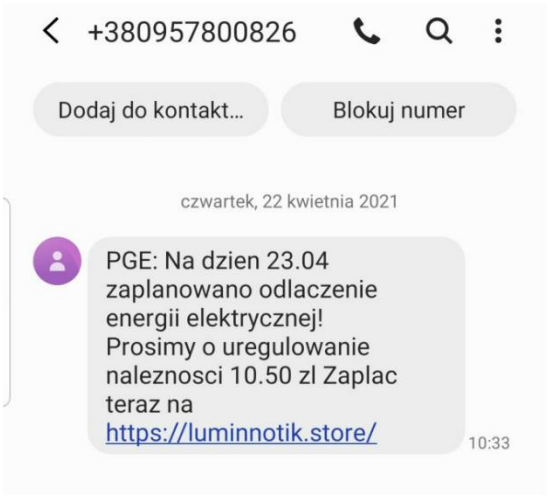
Phishing
To rodzaj oszustwa polegającego na podszywaniu się pod inną osobę lub instytucję w celu wyłudzenia informacji. Do ataków typu phishing wykorzystywane są wszystkie formy komunikacji elektronicznej, wiadomości e-mail, SMS-y, wiadomości na komunikatorach (np. WhatsApp), wiadomości prywatne w serwisach społecznościowych (np. na Facebook, Instagramie), rozmowy telefoniczne.
Oprócz wyżej wymienionych form komunikacji, tego typu ataki phishingowe mają miejsce w praktycznie każdym możliwym miejscu.
Na Messengerze czy innym komunikatorze (możesz np. dostać wiadomość z prośbą o opłacenie zamówienia „od znajomego", któremu przestępca przejął konto i wcześniej poznał Waszą historię rozmów).
Na Facebooku czy Instagramie (gdzie np. ktoś, podszywając się pod Zespół Techniczny, będzie starał się przekonać Cię, że Twoje konto czy fanpage mogą zostać usunięte lub zablokowane, jeśli nie podejmiesz jakiejś akcji).
Na OLX czy Vinted (gdzie osoba potencjalnie zainteresowana zakupem będzie chciała przenieść rozmowę poza ten serwis albo w inny sposób przesłać Ci link do fałszywego „odbioru płatności").

Jak rozpoznać phishing
Większość masowych ataków ma kilka cech, na które warto zwrócić szczególną uwagę:

- wiadomości często są pełne błędów językowych, gramatycznych i nie są pisane poprawną polszczyzną,
- zazwyczaj wiadomości zmuszają do pilnego i szybkiego działania i grożą nieprzyjemnymi konsekwencjami (konto zablokowane, weryfikacja, usunięty fanpage, wyłącznie prądu itd.),
- mogą zawierać dziwny numer, adres lub nazwę nadawcy,
- zawierają odnośnik, który nie jest w domenie firmy czy instytucji, np. allego-platnosci24[.]pl zamiast allegro.pl,
- zawierają załączniki w niestandardowym formacie, np. .zip, ,.xls, .xlsx, .rar, .iso czy .doc zamiast zwykłej faktury w PDF.

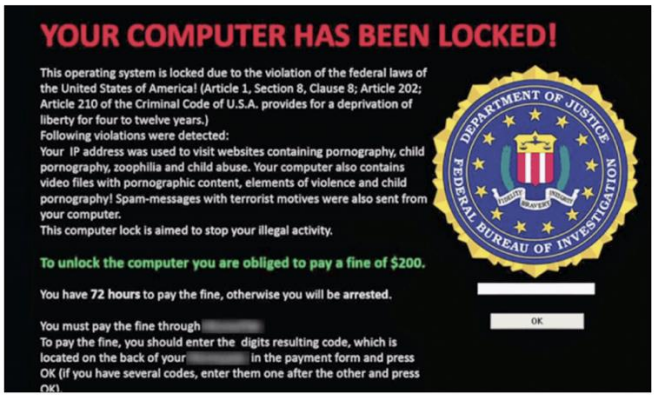
Phishing — przykłady





Ransomware

To rodzaj złośliwego oprogramowania, którego zadaniem jest zablokowanie właścicielowi/użytkownikowi dostępu do komputera/systemu/plików itp. W zamian za odzyskanie dostępu hakerzy żądają zapłaty w postaci pieniędzy – tradycyjnych lub kryptowalut.



Ochrona przed ransomware

- korzystaj z oprogramowania antywirusowego wykrywającego zagrożenie typu ransomware i pamiętaj o jego aktualizacji,
- regularnie twórz kopie zapasowe swoich najważniejszych plików (back-up).

Hasła zapamiętane w przeglądarce - pozwalamy zapamiętywać przeglądarkom internetowym hasła i korzystamy z funkcji autologowania to tylko z pozoru praktyczne działanie, które może poskutkować otwarciem przysłowiowej „puszki Pandory”, gdy nasz komputer lub smartfon wpadnie w niepowołane ręce.

Spam - niechciana poczta, bo tym jest spam, w tych pozornie nieszkodliwych treściach kryją się niebezpieczne szkodniki. Cyberwłamywacze liczą, że przez pomyłkę lub z ciekawości otworzymy zainfekowany załącznik.

Bezpieczeństwo danych w sieci - korzystanie z usług chmurowych, obarczone jest pewnym ryzykiem, że przechowywane w sieci dane zostaną utracone (na przykład w wyniku awarii pamięci serwera) lub przejęte przez nieautoryzowane osoby.

Literówki w adresach WWW - wpisując szybko adres strony internetowej na klawiaturze nietrudno o pomyłkę. Otworzenie witryny o podobnie brzmiącej nazwie czasem prowadzi do nic nieznaczącej strony z reklamami, ale czasem może kompletnie zablokować komputer.

Naruszenie prywatności, stalking - słowo prywatność nabrało dużego znaczenia i tak jak silnie walczymy o jej nienaruszanie, tak samo często sami wystawiamy ją bez obaw na forum publiczne udostępniając szczegółów dotyczących naszego życia. Takie informacje mogą wykorzystać cyberprzestępcy czy stalkerzy podszywając się pod znajomych. Również nasze zdjęcia mogą być wykorzystane przez innych użytkowników sieci, by zaszkodzić na przykład naszemu wizerunkowi.

Gdzie należy zgłosić incydent

Dla zdarzeń dotyczących Specjalistycznego Szpitala Wojewódzkiego w Ciechanowie

Dane kontaktowe Zespołu Cyberbezpieczeństwa - w sytuacji zagrożenia lub incydentu cyberbezpieczeństwa prosimy o kontakt wysyłając wiadomość na adres e-mail **incydenty@szpitalciechanow.com.pl**

Prosimy o zawarcie w zgłoszeniu następujących informacji, jeśli występują:

- dane kontaktowe i informacje organizacyjne,
- imię i nazwisko oraz nazwa i adres organizacji,
- adres e-mail,
- numer telefonu,
- adresy IP, screeny i każdy inny odpowiedni element techniczny wraz z powiązaną obserwacją wyniki skanowania lub dowolny wycinek logów pokazujący problem.

Dla zdarzeń niedotyczących Specjalistycznego Szpitala Wojewódzkiego w Ciechanowie

W sytuacji zagrożenia lub incydentu cyberbezpieczeństwa, mogą Państwo pomóc innym i zgłosić taką próbę w odpowiednie miejsce, jakim jest strona https://incydent.cert.pl/ prowadzona przez CERT Polska.

Prosimy o zawarcie w zgłoszeniu następujących informacji, jeśli występują:

- dane kontaktowe i informacje organizacyjne,
- imię i nazwisko oraz nazwa i adres organizacji,
- adres e-mail,
- numer telefonu,
- adresy IP, screeny i każdy inny odpowiedni element techniczny wraz z powiązaną obserwacją,
- wyniki skanowania lub dowolny wycinek logów pokazujący problem.

Zespół CERT oprócz wydania ostrzeżeń przed każdym nowym atakiem lub odmianą ataku np. phishingowego, stara się aktywnie przeciwdziałać takim atakom, blokując strony WWW, wykorzystywane w atakach np. phishingowych za pomocą DNS, z których korzystają niektórzy polscy operatorzy i dostawcy internetu.