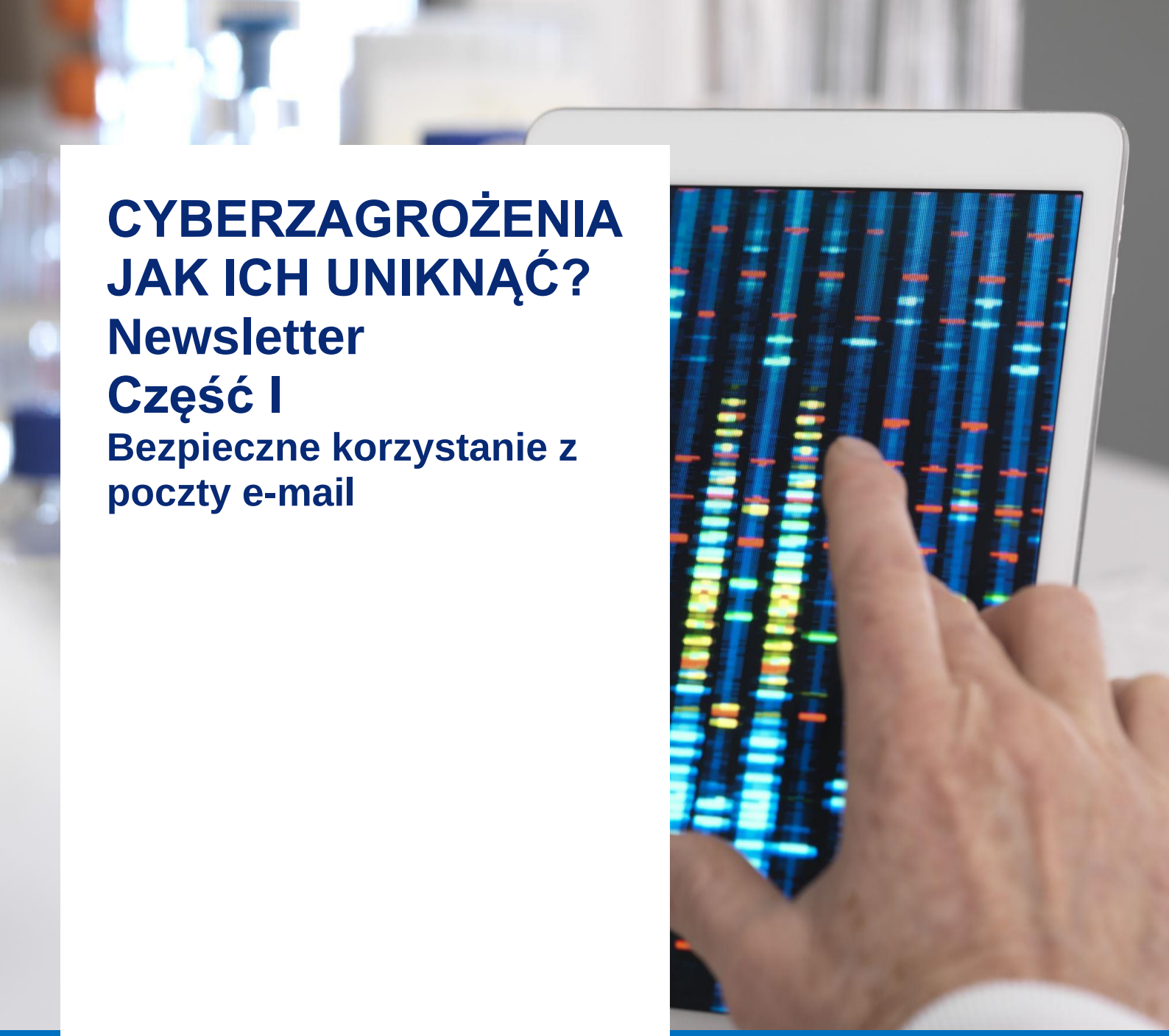

CYBERZAGROŻENIA JAK ICH UNIKNĄĆ?

Newsletter

Część I

Bezpieczne korzystanie z poczty e-mail

Newsletter nr I

stillsec

Wojewódzki Szpital Specjalistyczny nr 5
im. Św. Barbary w Sosnowcu

Centrum Urazowe

Cyfryzacja sektora opieki zdrowotnej

Nowy front cyberbezpieczeństwa

We współczesnym świecie wraz z rozwojem technologii, cyfryzacji i każdego elementu życia społecznego, zmienia się także profil, rodzaj oraz skala obecnych cyberzagrożeń. W ostatnich latach nowym frontem walki z cyberprzestępcami na całym świecie stały się urządzenia końcowe takie jak smartfony, tablety, laptopy, komputery stacjonarne, drukarki, urządzenia wielofunkcyjne, a nawet apartura diagnostyczna, jak również wyroby medyczne (np. rozruszniki serca, pompy insuslinowe). Dziś sprzęt ten jest niezbędnym elementem funkcjonowania Szpitali. Jednocześnie jego rosnąca powszechność powoduje, że jest on coraz bardziej wystawiony na ryzyko wykorzystania przez cyfrowych przestępców. Hakerzy bowiem nieustannie szukają najsłabszych elementów i ogniw, które mogą być podatne na przeprowadzenie skutecznego cyberataku.

Włamanie się do urządzenia końcowego – laptopa, komputera smartfonu, tabletu – podłączonego do sieci, używanego przez personel to prosta droga dla hakera do kradzieży danych i informacji należących do Szpitala, a nawet możliwość zagrożenia funkcjonowania całego Szpitala. Aby tego dokonać cyberprzestępcy używają coraz bardziej wyrafinowanych metod, często bazując na **nieuwadze i nieostrożności** w wykorzystywaniu poczty e-mail przez użytkowników.

Najsłabszym ogniwem jest człowiek – nawet najlepsze systemy nie uchronią nas przed cyberzagrożeniami, jeżeli nie będziemy przestrzegać podstawowych zasad bezpieczeństwa!

Wybrane rodzaje cyberzagrożeń

1. Malware

To automatycznie instalujące się lub nieumyślnie instalowane przez pracownika złośliwe oprogramowania mające na celu przejęcie kontroli nad systemem lub kradzieżą danych. Mogą ono zostać aktywowane, np. **w momencie otworzenia wiadomości e-mail lub załącznika do niej lub kliknięcia w link pochodzący z niezweryfikowanego źródła.**

2. Phishing i pharming

To podszywanie się pod zaufane źródło, np. znaną instytucję lub osobę (np. dyrektora Szpitala, administratora sieci, przełożonego, inspektora ochrony danych) w celu wyłudzenia poufnych informacji. **Phishing głównie wykorzystuje pocztę elektroniczną - cyberprzestępcy rozsyłają maile zachęcające do kliknięcia w link (np. wskazując, że konieczna jest zmiana hasła w systemie) i zalogowania się na podstawionej przez nich stronie, łudzące podobnej do prawdziwej, np. szpitala, poczty, a w efekcie mogą uzyskać dostęp do danych, w tym danych uwierzytelniających użytkownika**. Tak samo groźny **pharming** wykorzystuje przekierowania na fałszywe strony i serwery internetowe, na które jesteśmy kierowani np. poprzez zainstalowane na urządzeniu wirusy i złośliwe oprogramowania.

3. Ransomware

To oprogramowanie, które najpierw blokuje dostęp do systemu komputerowego oraz uniemożliwia odczytanie danych, a następnie żąda od użytkownika okupu za przywrócenie do stanu pierwotnego. **Hakerzy instalują takie oprogramowanie poprzez załącznik w e-mailu lub poprzez przeglądarkę internetową w momencie odwiedzenia strony, która**

jest zainfekowana złośliwym oprogramowaniem tego typu.

Przykład: atak na klinikę „*BUDZIK*”.

Placówka padła ofiarą złośliwego ataku ransomware. Kampania rozpoczęła się od tajemniczych maili, które trafiały na skrzynkę kliniki. Hakerzy podszywali się w nich pod uznane instytucje, informując o **niezapłaconych fakturach**. W treści wiadomości znajdowały się zainfekowane linki. Na skutek incydentu cały system informatyczny placówki został zablokowany, co uniemożliwiło sporządzenie obligatoryjnego raportu dla NFZ. Brak spełnienia tego wymogu mógł pozbawić instytucję funduszu niezbędnego do opłacenia kosztów funkcjonowania placówki. Cyberprzestępcy zażądali 30 tys. zł za odblokowanie systemów.

Jak się nie dać się oszukać?

Przykładowa wiadomość e-mail:

„Dzień dobry, po awarii Twoje konto zostało zablokowane ze względu na nieautoryzowany dostęp: potwierdź swoją tożsamość, wprowadzając kod autoryzacyjny. Przejdź na stronę [link].”

Tego rodzaju e-maile to typowy przykład narażenia użytkownika na phishing, czyli próbę wyłudzenia danych. Dostajemy na naszą skrzynkę e-mailową wiadomość: **ktoś próbował włamać się na nasze konto! Twoje konto straci ważność! Twoje konto zostało zablokowane!** Musimy tylko kliknąć w przesłany link i podać swoje dane. Rzecz w tym, że **nadawcą takiego maila nie jest administrator**, lecz grupa przestępcza. Podane przez nas informacje posłużą im do błyskawicznego przejęcia naszego konta.

Schemat działania jest zazwyczaj podobny:

1. Otrzymujemy na naszą skrzynkę alarmujący e-mail, a w nim link do strony i żądanie zalogowania.
2. Po kliknięciu linka, przekieruje on nas do fałszywej strony internetowej, do złudzenia przypominającej oficjalną stronę. Na dodatek strona ta może zawierać elementy graficzne (np. logo i kolorystykę), komunikaty bezpieczeństwa, które mają wzmagać u nas poczucie zaufania.
3. Kiedy już zalogujemy się na fałszywej stronie, przestępcy otrzymają nasze dane niezbędne do zalogowania się na naszym prawdziwym koncie (login, hasło).

O co nie zapyta Administrator?

Pamiętajmy, że administrator **NIGDY** nie prosi o potwierdzenie naszych poufnych danych w e-mailach, smsach czy w trakcie rozmów telefonicznych. W szczególności nigdy nie zażąda od nas podania hasła do konta **– hasło jest znane tylko i wyłącznie nam**.

Administrator nie wysyła także: e-maili z linkami kierującymi do strony do zalogowania się na konto internetowe, smsów z odsyłaczami do logowania, aplikacji lub certyfikatów bezpieczeństwa. Jeżeli otrzymałeś taką wiadomość, to znaczy, że ktoś – z pewnością **NIE** administrator – próbuje zainfekować Twoje urządzenie złośliwym oprogramowaniem.

Zasady bezpieczeństwo poczty e-mail

Zabronione jest:

- Wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu).
- **Otwieranie załączników od nieznanych nadawców, w szczególności z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.**
- Czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika (**nie udostępniaj swojego loginu i hasła innym pracownikom**)

- Posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych.
- Wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej, niż wynikającej z potrzeb Szpitala lub do poszukiwania dodatkowego zatrudnienia.
- W przypadku konieczności dokonania wysyłki korespondencji masowej poza Szpital, wysyłający powinien ukryć listę odbiorców (**pole BCC lub UDW**).
- **Dokonując wysyłki korespondencji z załącznikiem zawierającym w swojej treści dane osobowe, poufne informacje lub informacje mogące stanowić tajemnicę przedsiębiorstwa należy opatrzyć takie dokument hasłem autoryzacyjnym.** Hasło do pliku powinno zostać przesłane za pomocą **innej formy komunikacji** np. krótkiej wiadomości tekstowej SMS.