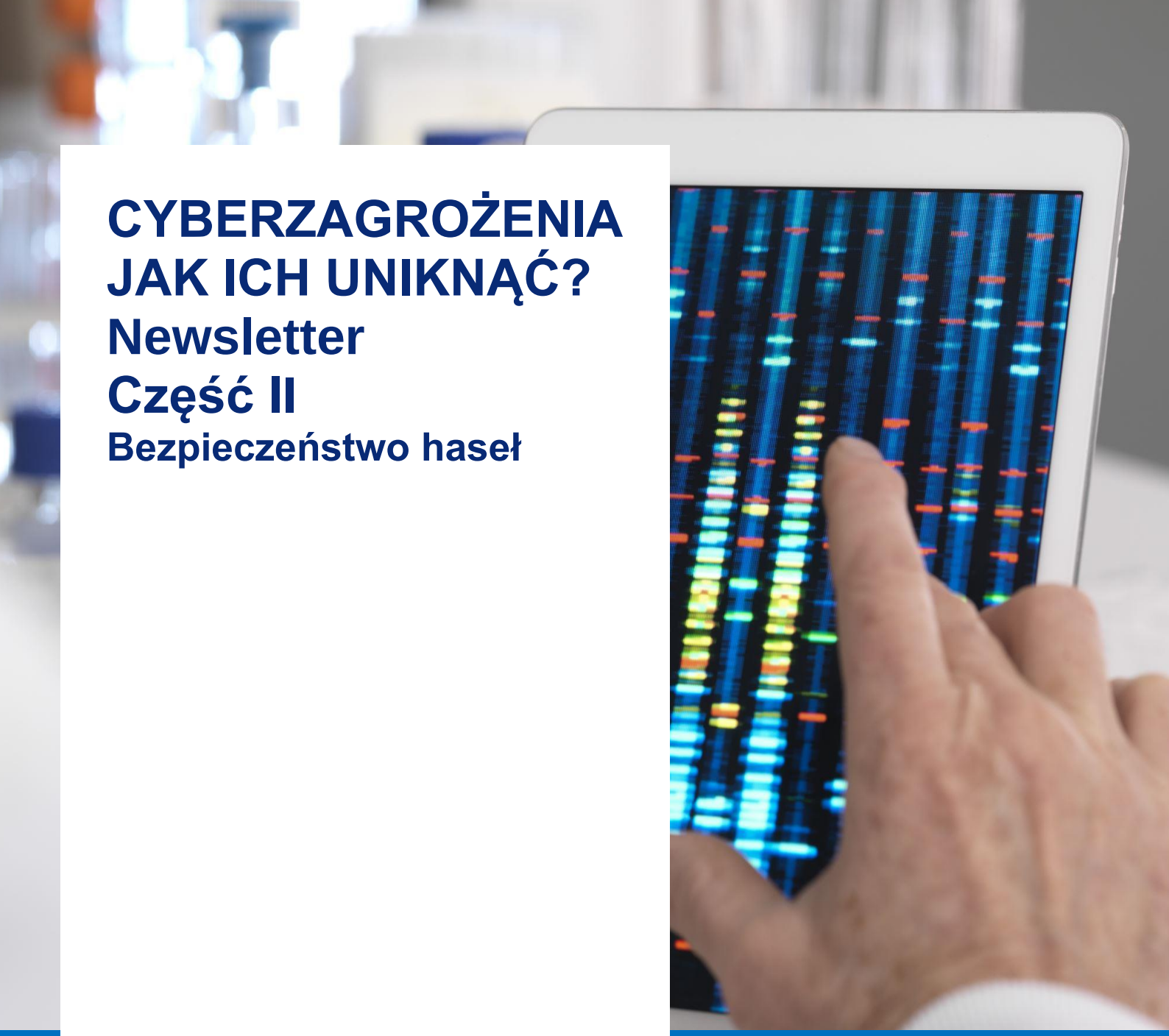

CYBERZAGROŻENIA JAK ICH UNIKNĄĆ?
Newsletter
Część II
Bezpieczeństwo haseł

Newsletter nr II

stillsec

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

Centrum Urazowe

Po co stosować bezpieczne hasła i chronić je przed ujawnieniem?

Hasła stosowane są w celu ochrony przed nieautoryzowanym dostępem do miejsc (na przykład medycznych baz danych), w których są przetwarzane kluczowe infromacje. Zawsze istnieje ryzyko włamania do systemu i wycieku danych, ale odpowiednio zbudowane hasła do systemu oraz dodatkowe środki bezpieczeństwa minimalizują to ryzyko.

Znane są także włamania do systemów w skutek których wyciekły dane uwierzytelaniające użytkowników.

Przykładowe informacje o włamaniach z ostatnich lat:

- Uber ujawnił informacje, że zapłacił okup atakującym, którzy w 2016 roku wykradli dane 57 milionów użytkowników;
- Doszło do nieautoryzowanego dostępu do baz danych PKW, wykradziono hasła i dokumenty z GPW;
- wyciekło 7 milionów haseł do serwisu Dropbox;
- opublikowano 450 000 haseł użytkowników Yahoo.

Niebezpieczeństwa, jakie może nieść wyciek haseł do danego systemu, to m.in. możliwość uzyskania nieautoryzowanego dostępu do naszego systemu, w tym na przykład możliwość dokonania nieautoryzowanej zmiany w dokumentacji medycznej – co może nieść duże zagrożenie dla zdrowia i życia naszych pacjentów, nieautoryzowany dostęp może również skutkować kradzieżą danych – co również wiąże się możliwością wystąpienia wielu negatywnych skutków – wyobraźmy sobie, że włamywacz udostępnia bazę pacjentów zarażonych wzw typu c, czy też wirusem HIV.

Bezpieczne hasło i przestrzeganie bezpiecznych zasad korzystania z niego, to kolejny podstawowy element w trosce o bezpieczeństwo. Hasła bronią dostępu do naszych danych systemów, czyli wszędzie tam gdzie gromadzimy istotne i cenne informacje!

Podstawy, czyli jak budować i chronić swoje hasło?

Budowa hasła

Stosuj hasło składające się z:

- kombinacji liter,
- znaków specjalnych
- cyfr.

Hasło, którego używasz powinno być **unikalne**, dlatego bądź kreatywna/kreatywny.
W top 10 światowych haseł są takie hasła jak: *12345678*, *qwerty*, *password*.
Nie stosuj hasła, które łatwo można z Tobą powiązać (np. Twoje imię i nazwisko z dodatkową cyfrą, imię Twojego psa, Twój ulubiony zespół muzyczny, imię Twojej żony/ imię Twojego męża itp.). Zawsze istnieje szansa, że atakujący choć trochę zna swoją ofiarę, czyli Ciebie, dlatego stosowanie haseł kojarzących się z nami nie jest dobrym pomysłem.

Haker zawsze może posłużyć się atakiem socjotechnicznym.

Ulubione piosenki, ulubione cytaty, imiona osób bliskich, pewne nawyki, imię Twojego zwierzęcia – wszystko to może być wykorzystane przeciwko Tobie.

Ochrona hasła

Tak, samo jak dobrze zbudowane hasło jest ważna jego ochrona dlatego kieruj się poniższymi zasadami:

- Nie zapisuj swojego hasła na karteczkach, w notatniku, na urządzeniu.
- Nigdy **nie podawaj osobom postronnym swojego hasła, w tym również współpracownikom**. Pamiętaj, że administrator **NIGDY** nie prosi Cię o potwierdzenie Twojego hasła 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**.

- Wpisując hasło sprawdzaj, czy nikt nie stoi za Twoimi plecami albo nie nagrywa tego co robisz.
- Stosuj różne hasła do różnych kont, ponieważ atak i wyciek danych z systemu zawsze jest możliwy. Jeżeli nastąpi taki wyciek lub ktoś pozna Twoje hasło, będziesz musiała/musiał zmienić hasło we wszystkich systemach, dlatego, jeśli masz problem z zapamiętywaniem, stwórz bazowy ciąg, do którego będziesz dodawać różne wersje znaków, słów.