

Materiały szkoleniowe dla uczestników

Szkolenie zostało poprowadzone przez: 1+1 Spółdzielnia Socjalna

Materiały szkoleniowe powstały w ramach projektu DISH DIGITAL & INNOVATION SKILLS HELIX IN HEALTH. DISH jest współfinansowane przez Program Unii Europejskiej Erasmus+, Akcję Kluczową 2 Współpraca na rzecz innowacji i Wymianę Dobrych Praktyk – Sojusze na rzecz Umiejętności Sektorowych

Cyberbezpieczeństwo w instytucjach służby zdrowia – 10 kluczowych zagadnień

1. Stwórz kulturę bezpieczeństwa
2. Chronź urządzenia mobilne
3. Utrzymuj dobre nawyki
4. Użyj zapory sieciowej (firewall)
5. Zainstaluj i aktualizuj oprogramowanie antywirusowe
6. Spodziewaj się niespodziewanego
7. Kontroluj dostęp do wrażliwych danych
8. Używaj silnych haseł i zmieniaj je regularnie
9. Ogranicz dostęp do sieci
10. Kontroluj dostęp fizyczny

1. Stwórz kulturę bezpieczeństwa

Specjaliści od bezpieczeństwa są zgodni: najsłabszym ogniwem każdego systemu komputerowego jest jego użytkownik.

Specjaliści z zakresu psychologii i socjologii użytkowników technologii informacyjnych (IT) raz po raz udowadniają, jak trudno jest podnieść świadomość ludzi na temat cyberbezpieczeństwa. Kluczowym działaniem podejmowanym przez administratorów systemów informatycznych oraz ich użytkowników powinno być zmniejszenie prawdopodobieństwa, że osobiste informacje dotyczące zdrowia pacjentów zostaną narażone na nieuprawnione ujawnienie, modyfikację, zniszczenie lub odmowę dostępu. Żadne podjęte działanie nie będzie jednak skuteczne, o ile praktyka opieki zdrowotnej nie chce i/lub nie jest w stanie ich na bieżąco stosować. Kluczowe jest egzekwowanie polityki bezpieczeństwa informacji oraz regularne szkolenia dla wszystkich użytkowników systemu informatycznego, tak by byli oni uwrażliwieni na znaczenie cyberbezpieczeństwa. Krótko mówiąc, każda praktyka opieki zdrowotnej musi zaszczepiać i wspierać kulturę organizacyjną zorientowaną na bezpieczeństwo.

Jednym z najtrudniejszych aspektów związanych z zapewnieniem cyberbezpieczeństwa jest przezwycięzenie przekonania, że „to nie może się przydarzyć mnie”. Ludzie, niezależnie od poziomu wykształcenia lub zaawansowania informatycznego wierzą, że „nigdy nie ulegną niechłujnym praktykom ani nie narażą na szwank informacji o pacjencie. To zdarza się tylko innym ludziom”.

Należy pamiętać, że przestrzegając określonych praktyk można uniknąć przynajmniej niektórych błędów wynikających z nadmiernej pewności siebie. Obowiązkiem każdej organizacji, w tym jednostek służby zdrowia, jest wspieranie właściwego bezpieczeństwa informacji poprzez ustanowienie kultury bezpieczeństwa. Każda osoba w organizacji musi zaakceptować wspólną wizję bezpieczeństwa informacji, aby nawyki i praktyki były automatyczne.

Praktyki bezpieczeństwa muszą być stosowane a nie tylko rozpisane w dokumentach dot. polityki bezpieczeństwa informacji.

Żadna lista kontrolna nie jest w stanie odpowiednio opisać wszystkiego, co należy zrobić, aby ustanowić kulturę bezpieczeństwa organizacji, ale istnieją pewne oczywiste kroki, które należy podjąć:

- Edukacja i szkolenia z tego zakresu muszą być częste i ciągłe.
- Ci, którzy zarządzają i kierują pracą innych, muszą dawać dobry przykład.
- Branie odpowiedzialności za bezpieczeństwo informacji powinno stanowić jedną z podstawowych wartości organizacji.

Ochrona pacjentów poprzez dobre praktyki bezpieczeństwa informacji powinna być na bieżąco realizowana przez jednostkę służby zdrowia, równoległe do wszystkich działań obejmujących dbanie o zdrowie pacjentów.

2. Chroń urządzenia mobilne

Urządzenia mobilne — laptopy, tablety, smartfony, przenośne nośniki pamięci w dużym stopniu ułatwiły zarządzanie informacją, także w służbie zdrowia. Jednocześnie jednak stworzyły one katalog całkowicie nowych zagrożeń dla prywatności i bezpieczeństwa informacji. Niektóre z tych zagrożeń pokrywają się z zagrożeniami charakterystycznymi dla komputerów stacjonarnych, ale niektóre są unikalne i na nich skupimy się w tym momencie.

W przypadku urządzeń mobilnych musimy zwrócić uwagę na to, że:

- Ze względu na swoją mobilność urządzenia te są łatwe do zgubienia i podatne na kradzież.
- Urządzenia mobilne są bardziej narażone na zakłócenia elektromagnetyczne niż komputery stacjonarne. Dotyczy to m.in. zakłóceń generowanych przez inne urządzenia medyczne. Interferencje te mogą w skrajnych przypadkach uszkodzić dane przechowywane na urządzeniach mobilnych.
- Ponieważ urządzenia mobilne mogą być używane w miejscach, w których mogą być widoczne dla innych, użytkownik musi zachować szczególną ostrożność, aby zapobiec nieuprawnionemu podejrzaniu informacji zdrowotnych wyświetlanych np. na laptopie.
- Nie wszystkie urządzenia mobilne są wyposażone w silne uwierzytelnianie i kontrolę dostępu. Konieczne mogą być dodatkowe kroki w celu zabezpieczenia urządzeń mobilnych przed nieautoryzowanym użyciem. Laptopy, komórki, tablety powinny być przynajmniej chronione hasłem. Jeśli natomiast ochrona hasłem nie jest zapewniona, należy podjąć dodatkowe kroki w celu ochrony elektronicznych informacji zdrowotnych na urządzeniu mobilnym, w tym dodatkowe środki ostrożności dotyczące fizycznej kontroli urządzenia.
- Laptopy i urządzenia mobilne są często używane do bezprzewodowego przesyłania i odbierania danych. Ta komunikacja bezprzewodowa musi być chroniona przed podsłuchem i przechwyceniem. Eksperti ds. cyberbezpieczeństwa zalecają, aby nie przysyłać elektronicznych informacji zdrowotnych w niezaszyfrowanych sieciach publicznych (np. w publicznych sieciach wifi, zwłaszcza takich, które nie są chronione hasłem).

Przesyłanie danych za pomocą urządzeń mobilnych jest z natury ryzykowne. W związku z tym korzystanie z urządzeń mobilnych powinno być w tym zakresie szczególnie uzasadnione wyższą koniecznością. Sam argument o większej wygodzie / komforcie pracy nie jest w tym wypadku wystarczający.

Tam, gdzie bezwzględnie konieczne jest przesyłanie elektronicznych informacji zdrowotnych do lub z urządzenia mobilnego, eksperci ds. cyberbezpieczeństwa zalecają szyfrowanie danych. Nie należy używać urządzeń mobilnych, które nie obsługują wspomnianego szyfrowania.

Jeśli bezwzględnie konieczne jest wyniesienie laptopa zawierającego elektroniczne informacje zdrowotne z terenu placówki zdrowotnej, należy zabezpieczyć informacje na dysku twardym laptopa za pomocą szyfrowania.

Zasady określające okoliczności, w jakich urządzenia mogą zostać wyniesione z obiektu, są bardzo ważne i należy zachować szczególną ostrożność przy opracowywaniu i egzekwowaniu tych zasad. Podstawowym celem jest ochrona informacji pacjenta, więc względy wygody lub praktyki (np. praca w domu) muszą być brane pod uwagę w tym zakresie.

Praca zdalna, m.in. ze względu na pandemię COVID-19, stała się niezwykle popularna. Osoby odpowiedzialne za ochronę informacji o pacjentach muszą zdać sobie sprawę, że ich odpowiedzialność nie kończy się na drzwiach gabinetu. Zawsze należy przestrzegać dobrych praktyk dotyczących prywatności i bezpieczeństwa.

3. Utrzymuj dobre nawyki

Lekarz zna znaczenie zdrowych nawyków dla utrzymania dobrego stanu zdrowia i zmniejszenia ryzyka infekcji i chorób. To samo dotyczy systemów informatycznych. Aby działały one prawidłowo i niezawodnie, potrzebna jest odpowiednia profilaktyka. Jest to szczególnie istotne w sytuacji, gdy wspomniane systemy informatyczne przechowują dane wrażliwe dot. pacjentów. W tym zakresie możemy zaobserwować bardzo wyraźną analogię w stosunku do profilaktyki zdrowotnej – czasami bardzo drobne rzeczy mogą mieć kluczowe znaczenie.

Odpowiednie skonfigurowanie oprogramowania komputerowego

Nowe komputery i pakiety oprogramowania mają często oszałamiającą gamę możliwości. Jednocześnie jednak dostawcy sprzętu/oprogramowania bardzo często skąpią informacji, jak odpowiednio je skonfigurować, aby system był bezpieczny. W obliczu tej złożoności standardowy użytkownik może mieć trudności w podjęciu decyzji, na jakie opcje zezwolić, a które wyłączyć. Istnieje w tym zakresie jednak kilka stosunkowo uniwersalnych zasad:

- Odinstaluj wszelkie aplikacje, które nie są niezbędne do prowadzenia placówki zdrowotnej (np. gry, komunikatory internetowe, narzędzia do udostępniania zdjęć). Jeśli przeznaczenie aplikacji nie jest oczywiste, zajrzyj na stronę internetową producenta oprogramowania, aby dowiedzieć się więcej o celach i zastosowaniach danej aplikacji. Jeśli masz wątpliwości odnośnie znaczenia danej aplikacji, skontaktuj się z administratorem systemu.
- Podczas instalacji oprogramowania nie akceptuj ustawień domyślnych lub „standardowych”. Przejrzyj każdą opcję, zapoznaj się z możliwymi wyborami i w razie potrzeby skontaktuj się z pomocą techniczną.
- Dowiedz się, czy dostawca danej aplikacji do obsługi jednostki medycznej wymaga otwartego połączenia z zainstalowanym oprogramowaniem („back door”) w celu zapewnienia aktualizacji i wsparcia. Jeśli tak, zapewnij bezpieczne połączenie na zaporze („firewall”) i poproś o wyłączenie tego dostępu, gdy nie jest używany.
- Wyłącz zdalne udostępnianie plików i zdalne drukowanie w ramach konfiguracji systemu operacyjnego. Zezwolenie na to może spowodować przypadkowe udostępnienie lub wydrukowanie plików w miejscach, w których nieupoważnione osoby mogą uzyskać do nich dostęp.

Aktualizacja oprogramowania

Większość oprogramowania wymaga okresowej aktualizacji w celu zapewnienia bezpieczeństwa i wprowadzenia dodatkowych funkcji. Dostawcy mogą wysyłać aktualizacje na różne sposoby: pobieranie automatyczne lub pobieranie na żądanie użytkownika.

Aktualizowanie oprogramowania ma kluczowe znaczenie dla zachowania bezpieczeństwa systemu, ponieważ wiele z tych aktualizacji usuwa nowo wykryte luki w zabezpieczeniach produktu. W większych przedsiębiorstwach takie „łatanie” może stanowić regularne, codzienne zadanie (jeśli używamy wielu aplikacji, może się okazać że praktycznie codziennie których z dostawców przygotował nową aktualizację). W jednostce możemy nie mieć wystarczających zasobów, by stale monitorować nowe aktualizacje i instalować je w odpowiednim momencie. Warto w związku z tym ustawić wszędzie gdzie to jest możliwe aktualizacje automatyczne (np. Użyj automatycznej aktualizacji systemu Microsoft Windows). Niezależnie od tego przynajmniej jeden pracownik powinien na bieżąco monitorować informacje dostarczane przez kluczowych producentów oprogramowania, z którego korzysta placówka (zwłaszcza dotyczy to aplikacji do zarządzania danymi pacjentów). W momencie, gdy pojawią się jakiegokolwiek poprawki krytyczne, należy zadbać o to by były one jak najszybciej zainstalowane.

Konserwacja systemu operacyjnego (OS)

System operacyjny ma tendencję do gromadzenia przestarzałych informacji i ustawień, chyba że przeprowadzana jest jego regularna konserwacja. Tym samym należy regularnie monitorować wszystkie komputery, i jeśli to możliwe, regularnie formatować dyski twarde i instalować system operacyjny od nowa.

Powinniśmy regularnie sprawdzać m.in.:

- Czy konta byłych pracowników są odpowiednio i terminowo wyłączane. W przypadku zwolnienia pracownika z inicjatywy pracodawcy należy zablokować dostęp do konta przed doręczeniem wypowiedzenia.
- Komputery i wszelkie inne urządzenia, takie jak kserokopiarki, na których przechowywane są dane, są odpowiednio czyszczone przed utylizacją. Nawet jeśli wszystkie dane na dysku twardym zostały usunięte, nadal można je odzyskać za pomocą powszechnie dostępnych narzędzi.

- Stare bazy danych i pliki z danymi osobowymi są archiwizowane w odpowiednich warunkach lub całkowicie usuwane z systemu, jeśli nie są już potrzebne, zgodnie z obowiązującymi wymogami dotyczącymi przetwarzania danych.
- Oprogramowanie, które nie jest już potrzebne, jest w pełni odinstalowane (w tym oprogramowanie testowe oraz stare wersje bieżącego oprogramowania).

Skąd wiesz, czy członkowie personelu pobrali programy, których nie powinni?

Istnieje wiele komercyjnych aplikacji i usług, które można skonfigurować w celu zgłaszania lub nawet zatrzymywania pobierania nieautoryzowanego oprogramowania. Możemy także skorzystać z aplikacji do przeprowadzenia analizy podatności i konfiguracji, a niektóre aplikacje/usługi mogą również przeprowadzać ogólne audyty bezpieczeństwa.

4. Użyj zapory sieciowej (firewall)

Każda placówka służby zdrowia, która korzysta z internetu (czyli w obecnej chwili KAŻDA placówka) powinna mieć odpowiednio skonfigurowaną zaporę sieciową. Zapora ta chroni sieć lokalną (LAN) przed włamaniami i zagrożeniami ze źródeł zewnętrznych. Podczas gdy oprogramowanie antywirusowe pomoże znaleźć i zniszczyć złośliwe oprogramowanie, które już się pojawiło, zadaniem zapory jest przede wszystkim zapobieganie przedostawaniu się intruzów. Krótko mówiąc, program antywirusowy można traktować jako kontrolę infekcji, podczas gdy zapora ma za zadanie zapobiegać chorobom.

Zapora (Firewall) może mieć charakter zarówno odpowiedniej aplikacji zainstalowanej na komputerze serwerowym, jak i dedykowanego urządzenia podłączanego przy routerze / access poście. W obu przypadkach jej zadaniem jest sprawdzenie wszystkich danych przychodzących do systemu z zewnątrz (z Internetu lub sieci lokalnej) i podjęcie decyzji, zgodnie z wcześniej określonymi kryteriami, czy dane te powinny zostać przepuszczone.

Zainstalowanie i odpowiednie ustawienie parametrów zapory może być skomplikowane technicznie, a zapory sprzętowe powinny być konfigurowane przez przeszkolony personel techniczny. z drugiej strony zapory programowe są często wstępnie skonfigurowane z typowymi ustawieniami, które sprawdzają się w wielu standardowych sytuacjach. Zapory programowe są dołączone do niektórych popularnych systemów operacyjnych, zapewniając ochronę na etapie instalacji (taką podstawową zaporę posiada np. system MS Windows). Alternatywnie, oddzielne oprogramowanie typu Firewall jest szeroko dostępne u dostawców zabezpieczeń komputerowych, w tym u większości dostawców oprogramowania

antywirusowego. Dostawcy ci zwykle zapewniają pomoc techniczną i wskazówki dotyczące instalacji zapory, tak by mogły sobie z tym poradzić także osoby nie posiadające bardziej zaawansowanej wiedzy technicznej.

Kiedy należy używać zapory sprzętowej?

W dużych firmach korzystających z sieci lokalnej (LAN) należy rozważyć zaporę sprzętową. Zapora sprzętowa znajduje się między siecią LAN a Internetem, zapewniając scentralizowane zarządzanie ustawieniami zapory. Zwiększa to bezpieczeństwo sieci LAN, ponieważ gwarantuje, że ustawienia zapory są identyczne dla wszystkich użytkowników sieci lokalnej.

Trzeba jednak pamiętać, że jeśli zapora sprzętowa ma spełniać swoją rolę, to powinna być konfigurowana oraz regularnie monitorowana i konserwowana przez specjalistę w tej dziedzinie.

5. Zainstaluj i aktualizuj oprogramowanie antywirusowe

Podstawowym narzędziem ataku na systemy informatyczne (zwłaszcza w małym biurze) są wirusy komputerowe, który wykorzystują luki w zabezpieczeniach komputera. Te luki są wszechobecne ze względu na charakter środowiska komputerowego. Nawet komputer, który ma wszystkie najnowsze aktualizacje zabezpieczeń systemu operacyjnego i aplikacji, może nadal być zagrożony z powodu niewykrytych wcześniej błędów. Komputery mogą zostać zainfekowane przez pozornie niewinne źródła zewnętrzne, takie jak płyty CD, poczta e-mail, pendrive czy pliki pobrane z sieci. Dlatego ważne jest, aby używać produktu, który zapewnia stale aktualizowaną ochronę. Oprogramowanie antywirusowe jest powszechnie dostępne, dobrze przetestowane pod kątem niezawodności i kosztuje stosunkowo niewiele.

Kluczowe jest, aby oprogramowanie antywirusowe było aktualne. Produkty antywirusowe wymagają regularnych aktualizacji od dostawcy w celu ochrony przed najnowszymi wirusami komputerowymi i złośliwym oprogramowaniem. Większość programów antywirusowych automatycznie generuje przypomnienia o tych aktualizacjach, a wiele z nich można skonfigurować tak, aby umożliwić automatyczną aktualizację.

Bez oprogramowania antywirusowego dane mogą zostać skradzione, zmodyfikowane lub zniszczone, a osoby atakujące mogą przejąć kontrolę nad komputerem.

Jak użytkownicy mogą rozpoznać infekcję wirusem komputerowym?

Niektóre typowe objawy zainfekowanego komputera to:

- System nie uruchamia się normalnie (np. „niebieski ekran śmierci”)
- System wielokrotnie się zawiesza bez wyraźnego powodu
- Przeglądarka internetowa otwiera niechciane strony internetowe
- Oprogramowanie antywirusowe nie działa
- Wiele niechcianych reklam pojawia się na ekranie
- Użytkownik nie może kontrolować myszy/wskaźnika

6. Spodziewaj się niespodziewanego

Prędzej czy później wydarzy się coś nieoczekiwanego. Stwierdzenie to na pierwszy rzut oka wydaje się banałem, ale jest niestety prawdziwe. Pożar, powódź, huragan, trzęsienie ziemi i inne klęski żywiołowe lub katastrofy spowodowane przez człowieka mogą uderzyć w dowolnym momencie. Ważne akta medyczne i inne kluczowe aktywa muszą być chronione przed utratą w wyniku tych zdarzeń. Musimy w związku z tym zadbać o dwie kluczowe rzeczy: regularne tworzenia kopii zapasowych danych oraz dobrze przemyślany plan backupu czyli odzyskiwania utraconych danych.

W świecie biznesu tworzenie kopii zapasowej jest stałą praktyką. Jednak w praktyce może się zdarzyć, że członkowie personelu znają tylko domowe środowisko komputerowe, w którym tworzenie kopii zapasowych jest rzadko brane pod uwagę, przynajmniej dopóki nie nastąpi awaria (i wtedy bardzo często jest już za późno na stosowanie jakichkolwiek środków zaradczych). W środowisku zawodowym należy regularnie i rzetelnie tworzyć kopie zapasowe. Niezawodna kopia zapasowa to taka, na którą można liczyć w sytuacji awaryjnej, dlatego ważne jest nie tylko prawidłowe zapisywanie wszystkich danych, ale także ich szybkie i dokładne przywrócenie. Nośniki kopii zapasowych należy regularnie testować pod kątem ich zdolności do prawidłowego przywracania.

Niezależnie od nośnika używanego do tworzenia kopii zapasowej, musi być on bezpiecznie przechowywany, aby dane nie mogły zostać uszkodzone przez tę samą awarię, która przytrafiła się systemowi głównemu. Dobrym rozwiązaniem jest tworzenie kopii zapasowej na serwerach zdalnych. Rozwiązaniem może być także wykorzystanie chmury danych do tworzenia kopii bezpieczeństwa. Takie rozwiązanie jest tańsze niż fizyczna infrastruktura, ale trzeba z dużą ostrożnością wybrać operatora tego typu rozwiązania.

Pliki krytyczne można ręcznie skopiować na nośniki kopii zapasowych, chociaż jest to rozwiązanie żmudne i potencjalnie podatne na błędy. Jeśli to możliwe, należy zastosować zautomatyzowaną metodę tworzenia kopii zapasowych.

Niektóre rodzaje nośników kopii zapasowych, takie jak taśma magnetyczna czy wymienne dyski twarde, mają charakter wielokrotnego użytku. Trzeba pamiętać, że mogą one z czasem ulec zużyciu, dlatego trzeba regularnie monitorować ich stan.

Przywracanie danych z kopii zapasowej powinno opierać się na jasnej i przygotowanej wcześniej procedurze. Jest to o tyle istotne, że w przypadku wystąpienia jakiegokolwiek katastrofy dane medyczne pacjentów powinny zostać jak najszybciej odtworzone.

Ognioodporny, zainstalowany na stałe sejf domowy, którego kombinację zna tylko pracownik służby zdrowia, może być dla wielu małych ośrodków zdrowia najlepszym wyborem do przechowywania nośników kopii zapasowych. Nie umieszcza to kopii zapasowej poza strefą zagrożenia katastrofą powszechną (trzęsienie ziemi, huragan, broń nuklearna), ale zapewnia przynajmniej pewne zabezpieczenie przed lokalnymi sytuacjami kryzysowymi, takimi jak pożar i powódź. Ognioodporne przenośne pudełka lub sejfy są rozwiązaniem w żadnym wypadku niewystarczającym.

7. Kontroluj dostęp do wrażliwych danych

Kluczowym elementem budowania systemu informatycznego odpornego na cyber ataki jest regularna higiena haseł (wskazana w pkt 8). Hasło to jednak tylko połowa tego, co składa się na dane uwierzytelniające użytkownika. Druga połowa to login lub nazwa użytkownika. W większości systemów komputerowych te poświadczenia (login i hasło) są używane jako część systemu kontroli dostępu, w którym użytkownikom przypisuje się określone prawa dostępu do danych. Ten system kontroli dostępu może być częścią systemu operacyjnego (np. Windows) lub wbudowany w konkretną aplikację (np. moduł e-recept). Administrator systemu informatycznego powinien tak ograniczać dostęp danych, by każdy użytkownik uzyskiwał jedynie te informacje, które są mu/jej niezbędne w pracy – nie wszyscy muszą wiedzieć wszystko!

W małych jednostkach ograniczenie dostępu do plików/baz danych można wykonać ręcznie, korzystając z listy kontroli dostępu. Może to zrobić tylko ktoś z administracyjnymi uprawnieniami do systemu. Przed ustawieniem tych uprawnień ważne jest, aby określić, które pliki powinny być dostępne dla których członków personelu.

Dodatkowe kontrole dostępu, które można skonfigurować, obejmują kontrolę dostępu opartą na rolach, w której rola członka personelu w przychodni (np. lekarz, pielęgniarka, specjalista ds. rozliczeń) określa, do jakich informacji można uzyskać dostęp. W takim przypadku należy zadbać o przypisanie personelu do odpowiednich ról, a następnie o prawidłowe ustawienie uprawnień dostępu dla każdej roli z uwzględnieniem potrzeb danego stanowiska.

Co się stanie, jeżeli ktoś bez uprawnień uzyskał dostęp do elektronicznych informacji zdrowotnych?

W pewnych okolicznościach taki incydent jest uważany za naruszenie, które należy zgłosić do Prezesa Urzędu Ochrony Danych Osobowych. Posiadanie dobrych kontroli dostępu i wiedza o tym, kto przeglądał lub używał informacji (tzw. access log) może pomóc w zapobieganiu lub wykrywaniu takich naruszeń.

8. Używaj silnych haseł i zmieniaj je regularnie

Hasła są pierwszą linią obrony w zapobieganiu nieautoryzowanemu dostępowi do dowolnego komputera. Bez względu na typ lub system operacyjny, do zalogowania powinno być wymagane hasło. Chociaż silne hasło nie powstrzyma atakujących przed próbą uzyskania dostępu, może je spowolnić i zniechęcić. Ponadto silne hasła w połączeniu ze skuteczną kontrolą dostępu pomagają zapobiegać przypadkowym nadużyciom (np. mogą pohamować osobistą ciekawość pracowników w sprawie, co do której nie powinni mieć pełnych informacji).

Silne hasła to przede wszystkim takie, które jest trudno odgadnąć. Osoby atakujące mogą używać tzw. Łamaczy słownikowych, które będą po kolei sprawdzały kombinacje najczęściej pojawiających się fraz w oparciu o przygotowane słowniki.

Silne hasła nie powinny zawierać:

- Słów znalezionych w słowniku, nawet jeśli są nieco zmienione (np. zastąpienie litery cyfrą)
- Danych osobowych, takich jak np. data urodzenia, imiona (własne lub członków rodziny lub zwierząt domowych), numerów PESEL. Pamiętaj: Jeśli jakaś informacja o Tobie znajduje się w serwisie społecznościowym, nigdy nie powinna być używana w hasle.

Poniżej znajduje się kilka przykładów cech silnych haseł:

- Długość co najmniej ośmiu znaków (im dłużej, tym lepiej)
- Kombinacja wielkich i małych liter, jednej cyfry i co najmniej jednego znaku specjalnego, takiego jak znak interpunkcyjny

Wreszcie, systemy powinny być tak skonfigurowane, aby hasła były regularnie zmieniane. Chociaż może to być niewygodne dla użytkowników, zmniejsza również ryzyko łatwego włamania do systemu przy użyciu skradzionego hasła.

Hasła i silne uwierzytelnianie

Silne lub wieloskładnikowe uwierzytelnianie łączy w sobie wiele różnych metod uwierzytelniania, co zapewnia bardzo dużą ochronę. Oprócz nazwy użytkownika i hasła używana jest inna metoda uwierzytelniania (np. karta inteligentna, brelok, odcisk palca lub skan tęczówki oka).

A co z zapomnianymi hasłami?

Każdy może zapomnieć hasło, zwłaszcza jeśli jest ono długie. Aby zniechęcić ludzi do zapisywania haseł i pozostawiania ich w niezabezpieczonych lokalizacjach, stwórz możliwość do stosunkowo prostego resetowania haseł.

Przykładowe rozwiązania:

- Autoryzowanie dwóch różnych członków personelu do resetowania haseł
- Stworzenie/udostępnienie w ramach systemu informatycznego funkcji resetowania haseł

9. Ogranicz dostęp do sieci

Ze względu na łatwość użycia i elastyczność współczesne narzędzia sieciowe są bardzo atrakcyjne. Technologie Web 2.0, takie jak udostępnianie plików peer-to-peer i wiadomości błyskawiczne, są popularne i szeroko stosowane. Routing bezprzewodowy to szybki i łatwy sposób na skonfigurowanie połączenia szerokopasmowego w domu lub biurze. Jednak ze względu na poufność informacji dotyczących opieki zdrowotnej oraz fakt, że są one chronione przez prawo, narzędzia, które mogą umożliwić osobom postronnym uzyskanie dostępu do sieci placówki zdrowotnej, muszą być stosowane ze szczególną ostrożnością.

Routery bezprzewodowe są w tym momencie powszechnie stosowane, zarówno przez małe jak i większe podmioty. Jeśli się wi-fi w routerze bezprzewodowym nie jest zabezpieczona, jego sygnał może być odbierany z pewnej odległości, w tym na przykład z parkingu budynku, innych biur w tym samym budynku, a nawet pobliskich domów. Ponieważ elektroniczne informacje zdrowotne przesyłane przez sieć bezprzewodową muszą być chronione przez prawo, ważne jest zabezpieczenie sygnału bezprzewodowego, aby tylko ci, którzy mają dostęp do informacji, mogli go odebrać. Routery bezprzewodowe muszą być skonfigurowane do działania tylko w trybie szyfrowanym.

Urządzenia mobilne pacjentów nie powinny mieć możliwości autometrycznego łączenia się z siecią wifi bez podania hasła. Skonfigurowanie sieci w celu bezpiecznego dostępu gości jest kosztowne i czasochłonne, więc najlepszą obroną jest zabronienie przypadkowego dostępu. Gdy skonfigurowana jest sieć bezprzewodowa, każde firmowe urządzenie powinno zostać zidentyfikowane na routerze i dopiero wtedy powinien być gwarantowany dla niego dostęp do sieci.

Aplikacje wykorzystujące model peer-to-peer (m.in. do udostępniania plików i wiadomości błyskawicznych) mogą narażać podłączone urządzenia w tym zezwalać na nieautoryzowany dostęp do urządzeń, na których są zainstalowane. Sprawdź, czy aplikacje peer-to-peer nie zostały zainstalowane bez autoryzacji. Nie wystarczy po prostu wyłączyć te programy lub je odinstalować. Maszyna zawierająca aplikacje peer-to-peer może zawierać fragmenty kodu, które można wykorzystać nawet po usunięciu programów.

Dobłą zasadą jest zabronienie personelowi instalowania oprogramowania bez uprzedniej zgody.

10. Kontroluj dostęp fizyczny

Nie tylko zasoby, takie jak pliki i dane, muszą być zabezpieczone. Same urządzenia składające się na system informatyczny również muszą być odpowiednio zabezpieczone przed nieuprawnionym dostępem. Najczęstszym sposobem, w jaki elektroniczne informacje zdrowotne są zagrożone, jest utrata urządzeń, niezależnie od tego, czy dzieje się to przypadkowo, czy w wyniku kradzieży. Incydenty zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych pokazują, że ponad połowa przypadków utraty danych związana jest ze zgubionymi urządzeniami, zwłaszcza przenośnymi (np. pendrive'y, tablety, laptopy). Zdarzają się jednak także kradzieże komputerów stacjonarnych, ale nawet czasami same dyski twarde są wrywane z maszyn.

W przypadku zniknięcia urządzenia do przechowywania danych (bez względu na to, jak dobrze instytucja zadbała o odpowiednie hasła, kontrolę dostępu i uprawnienia do plików) istnieje możliwość, że określona osoba uzyska dostęp do znajdujących się na nim danych. Dlatego ważne jest, aby ograniczyć ryzyko zgubienia lub kradzieży urządzeń.

Fizyczne zabezpieczanie urządzeń i danych powinno skupiać się na ograniczeniach dostępu fizycznego, np. zabezpieczenie urządzeń w zamkniętych pomieszczeniach / szafach pancernych, zarządzanie dostępem do kluczy fizycznych lub ograniczenie możliwości wnoszenia urządzeń z bezpiecznego obszaru.

Gdzie powinienem umieścić serwer, który przechowuje elektroniczne informacje zdrowotne?

Rozważając lokalizację serwera zawierającego elektroniczne informacje zdrowotne należy wziąć pod uwagę dwa główne czynniki: ochronę fizyczną i ochronę środowiskową. Ochrona fizyczna powinna koncentrować się na uniemożliwieniu dostępu do serwera osobom niepowołanym (np. przechowywanie serwera w zamkniętym pomieszczeniu dostępnym tylko dla personelu). Ochrona środowiskowa powinna skupiać się na ochronie serwera przed ogniem, wodą i innymi czynnikami szkodliwymi (np. nie twórz serwerowni w pomieszczeniu znajdującym się tuż pod toaletą, w miarę możliwości serwer nie powinien znajdować się w pomieszczeniu z oknami, powinna też zostać zapewniona odpowiednia temperatura i cyrkulacja powietrza).

