- nie otwierać podejrzanych załączników, bo cyberprzestępcy wykorzystują ciekawość ludzką. Większość z nas zetknęła się z robakami pocztowymi, które rozsyłane są jako załączniki zainfekowanych wiadomości. Aby robak mógł się dalej rozprzestrzeniać, trzeba go uaktywnić, otwierając załącznik. A ciekawość ludzka nie zna granic;
- nie odpowiadać na spam, bo spowoduje to potwierdzenie poprawności adresu mailowego użytkownika;
- unikać pobierania bezpłatnych programów użytkowych. Często zawierają one oprogramowanie typu „spyware". Coraz częściej trojany – programy z wbudowanymi, ukrytymi funkcjami, które pozwalają przejąć kontrolę nad komputerem i wykraść dane. Występują one w postaci darmowych, pozornie pożytecznych programów, które pracownicy sami pobierają z internetu i instalują na firmowym komputerze;
- nie podawać firmowego adresu do prywatnych celów. Naraża to szpital na zwiększenie ilości spamu i ułatwia przestępcom wytypowanie potencjalnych celów.

Samodzielne instalowanie oprogramowania

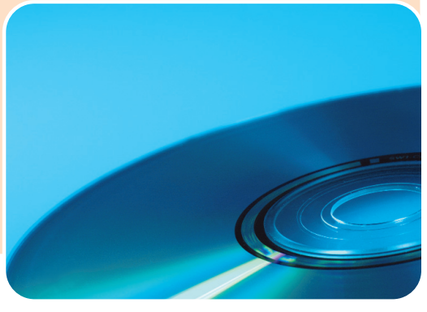
Aplikacje, takie jak Skype, MSN Messenger, ICQ czy Kazała są popularne i przydatne. Nie powinny być jednak zainstalowane w komputerze używanym w pracy, chyba że któraś z nich jest oficjalnie stosowana w firmowym systemie obsługi wiadomości. Takie programy narażone są na wystąpienie luk w zabezpieczeniach i ataki wirusów, co może ułatwić rozpowszechnianie się różnorodnych infekcji. Jest to szczególnie niebezpieczne, gdy pliki przesyłane za pośrednictwem tego oprogramowania nie są analizowane przez firmowy program antywirusowy. Niedozwolone jest nielegalne pobieranie plików muzycznych do komputera firmowego.

Licencje na oprogramowanie

Licencje dotyczą określonej liczby komputerów. Przeprowadzanie niekontrolowanych, niezgodnych z warunkami umowy instalacji jest niedopuszczalne. To pozornie niewinne zachowanie stanowi naruszenie przepisów dotyczących licencji na oprogramowanie. Zgodnie z zapisami ustawy o prawie autorskim i prawach pokrewnych, programy komputerowe podlegają takiej samej ochronie jak utwory literackie. Za nieprzestrzeganie tych przepisów grozi odpowiedzialność karna – kara grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. W szpitalu obowiązuje kategoryczny zakaz instalowania oprogramowania bez autoryzacji.

Uprawnienia dostępu

Z dniem rozwiązania umowy o pracę pracownik powinien mieć zablokowane konto. Będzie to możliwe, jeśli odpowiednie informacje dotrą na czas do administratora systemu, nadającego uprawnienia dostępu. W odniesieniu do mechanizmów uwierzytelniania użytkowników powinny być wskazane i opisane zarówno zagadnienia uwierzytelniania w systemach informatycznych, jak i dotyczące uwierzytelnienia przy wejściu (wyjściu) do określonych pomieszczeń oraz sposób rejestracji wejść/wyjść. Np. podpis elektroniczny autoryzuje każdy kolejny wpis na dokumencie. Jeden dokument może zawierać wpisy kilku osób. Niedozwolone jest dokonywanie wpisów przy użyciu cudzego podpisu elektronicznego. Pamiętajmy też o jeszcze jednej zasadzie – odpowiedzialności, którą za wszelkie szkody wynikające z niewłaściwego korzystania z firmowego konta ponosi jego użytkownik. Zatem nie możemy się tłumaczyć, iż na „chwilę" udostępniliśmy hasło czy pin koledze lub koleżance czy nawet przełożonemu. Wszystko, co zostało wykonane w systemie w ramach naszego konta, zawsze pójdzie na nasz rachunek.



nr 15 kwiecień 2008

BIULETYN

biuletyn Szpitala Wolskiego

do użytku wewnętrznego

co gdzie kiedy

Na spotkanie wielkanocne, które mieliśmy 19 marca, przybyli nasi przyjaciele z Rady Społecznej: dr Marcin Hoffman – przewodniczący oraz radni – pani Anna Podłucka i pan Przemysław Gołębski. Swoją obecnością zaszczycił nas również prof. Maciej Borkowski, który zawsze jest z nami na święta. Pan dyrektor Adam Doliwa złożył wszystkim pracownikom i gościom życzenia słonecznej i radosnej Wielkanocy, także od posła Marka Balickiego, któremu obowiązki w sejmie nie pozwoliły uczestniczyć w tym spotkaniu. Poczęstunek przygotowała firma „Bar Bistro", która wkrótce otworzy bufet w pawilonie 7, a uroczystość uwieczniał na zdjęciach kolega Piotr Paczewski.

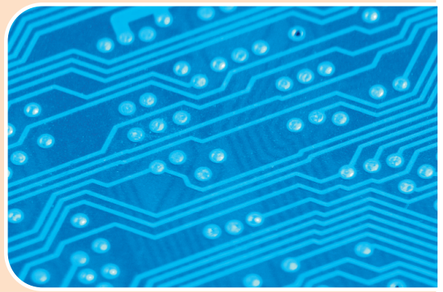
1 nasz szpital

Chroń dane osobowe

Czy znasz swoją rolę i znaczenie w ochronie informacji, które są w posiadaniu szpitala? Czy wiesz, iż zgodnie z przepisami prawa zarówno ty, jak i pacjenci mają prawo do ochrony danych osobowych? Czy chciałbyś, żeby miał do nich dostęp ktoś nieupoważniony? Czy szpital bez twojej pomocy zapewni właściwą ochronę danych osobowych pracowników i pacjentów? Na te pytania musimy sobie odpowiedzieć. By to ułatwić, przedstawimy pokrótce podstawowe zasady bezpieczeństwa informacji.

W żadnej firmie bezpieczeństwo informacji nie może być pozostawione przypadkowi. W wielu wdrażane są różne rozwiązania programowe i sprzętowe z zakresu informatyki, obsługiwane przez specjalistów.

Podstawowe zasady korzystania z sieci informatycznej zamieszczone są na wewnętrznej stronie internetowej szpitala. I zawsze należy o nich pamiętać. Istotną rolę pełnią również zabezpieczenia fizyczne, które chronią sprzęt oraz dokumentację w wersji papierowej. Mimo tego kierownictwo takiej organizacji jak szpital nie jest w stanie w pełni kontrolować niezwykle ważnego elementu: zachowań pracowników, w tym użytkowników komputerów, czyli czynnika ludzkiego. Statystycznie biorąc, błąd człowieka jest najczęstszą przyczyną strat czasu i pieniędzy w firmach. Popełnianie błędów leży w ludzkiej naturze i wynika nie ze złej woli, lecz z nieostrożności, przemęczenia, stresu, braku doświadczenia, niedostatecznej wiedzy i innych, trudnych do przewidzenia czynników.



Zgodnie z przepisami, dbałość o bezpieczeństwo danych osobowych i innych informacji wrażliwych w miejscu pracy jest obowiązkiem każdego pracownika, a nie tylko kierownictwa. Bez współpracy wszystkich nie zapewni się bezpieczeństwa danych przetwarzanych w szpitalu.

Kradzież i ujawnienie danych wrażliwych

Nieodpowiedzialne zachowania użytkownika komputera mogą doprowadzić do ujawnienia bądź utraty danych pacjentów, a także danych osobowych z systemów informatycznych obsługujących kadry i finanse. Problem ten pojawia się w wyniku zaniedbań użytkowników, luk w oprogramowaniu lub świadomego sabotażu.

Oto przykład z życia wzięty. Zazwyczaj wychodząc z domu wyłączamy żelazko, telewizor i zamykamy drzwi na klucz. Więc dlaczego wychodząc z pokoju w pracy, zostawiamy zalogowany komputer, dokumentację na biurku, otwarte drzwi lub przyklejone na ekranie hasło dostępu do systemu? Czy nie zdajemy sobie sprawy, że może to prowadzić do nieumyślnego skasowania czy zafałszowania danych przez osobę postronną lub współpracownika, który niechcący naciśnie jakiś klawisz? A złośliwość koleżanki, która nas nie lubi? Czyż nie stwarzamy jej okazji do zaszkodzenia nam przez skorzystanie z naszej poczty mailowej w celach nieetycznych lub „poprawienie" naszych zapisów. Przecież to taka sama sytuacja jak pozostawienie klucza do mieszkania w zamku od zewnętrznej strony drzwi.

Miejmy świadomość, iż za dane osobowe i tzw. informacje wrażliwe zainteresowani skłonni są dużo zapłacić. Niewłaściwa ich ochrona lub przypadkowe ujawnienie, np. przez wyrzucenie wydruków archiwalnych na śmietnik lub utylizację komputerów bez zniszczenia twardych dysków, niosą za sobą poważne konsekwencje, począwszy od narażenia na szwank reputacji szpitala, a na konsekwencjach prawnych – cywilnych i karnych, i wkrótce finansowych skończywszy.

Dokumentacja medyczna

Pamiętajmy, że szpital może udostępnić dokumentację medyczną tylko podmiotom określonym w ustawie i że dokumentację prowadzoną w postaci elektronicznej udostępnia się z zachowaniem jej integralności oraz ochrony danych osobowych.

2 nasz szpital

A gdy konieczne jest dołączenie do niej materiałów w postaci fizycznej, to trzeba je oznaczyć w sposób zapewniający powiązanie z dokumentacją prowadzoną elektronicznie.

Dokumentację prowadzoną elektronicznie uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:

- dostęp do dokumentacji mają wyłącznie osoby uprawnione;
- jest ona chroniona przed przypadkowym lub nieuprawnionym zniszczeniem;
- zastosowane są takie metody i środki ochrony dokumentacji, których skuteczność jest uznawana powszechnie.

Niedopuszczalne jest, aby w obecności Pana x, który pyta o swoje dane, na ekranie komputera wyświetlone zostały dane innych osób, chyba że ekran jest tak ustawiony, iż osoby postronne nie mają do niego wglądu. Inne rozwiązanie dopuszcza się tylko wtedy, gdy wyniki wyszukiwania są dostępne wyłącznie dla osób upoważnionych do dostępu i przetwarzania danych osobowych.

Zafałszowanie informacji

Niefrasobliwość użytkowników może doprowadzić do zafałszowania informacji. Wszak każda podejmowana decyzja opiera się na przeświadczeniu o poprawności i prawdziwości zgromadzonych informacji. Wyobraźmy sobie, że ktoś świadomie i złośliwie zmienia w systemie dane o naszym wynagrodzeniu, przepracowanych godzinach, wykorzystaniu urlopu. Po jakim czasie zorientujemy się, że coś jest nie tak? Zafałszowanie informacji jest szczególnie szkodliwe, ponieważ decyzje podjęte na podstawie fałszywych danych mogą być błędne i w konsekwencji narazić szpital na straty. Dlatego prawidłowe wprowadzanie danych i ich autoryzacja są niezwykle istotnymi elementami systemu.

Uwaga na hasła

W polityce bezpieczeństwa szpitala ważne są dobrze zdefiniowane i zabezpieczone hasła. Polskie przepisy prawne dotyczące ochrony danych osobowych dość szczegółowo regulują zasady zabezpieczenia hasłami. Konieczne jest przestrzeganie kilku zasad podstawowych:

- hasła powinny być zmieniane co jakiś czas, najlepiej nie rzadziej niż co 30 dni;
- hasła nie powinny być trywialne: jednoznakowe, jednoliterowe czy takie jak „abcdefgh". Niedopuszczalne są hasła słownikowe – „drzewo", „kwiatek", imiona czy daty urodzin bliskich. Dla osoby zainteresowanej poufnymi albo nie przeznaczonymi dla niej danymi nie zawsze opłacalne jest włamywanie się do systemu. Znacznie prostsze może być uzyskanie dostępu do hasła przez wyłudzenie, odgadnięcie lub złamanie „brutalną siłą" poprzez wypróbowanie różnych kombinacji;
- hasło powinno zawierać przynajmniej jedną dużą i małą literę, jedną cyfrę i jeden znak specjalny – pytajnik, wykrzyknik. W sumie powinno mieć co najmniej 8 znaków. Nie wolno go zapisywać. Jednak nie trzeba przesadzać z dodatkowymi restrykcjami nakładanymi na hasła, bo prowadzi to do nieprzestrzegania ww. zasad. Wyobraźmy sobie, że administrator wymaga od użytkowników, aby ich hasła były trudne do odgadnięcia, a przez to lepsze z punktu widzenia bezpieczeństwa. W teorii wygląda to ładnie, jednak takie „bezpieczne" hasła zapisywane są często na kartce papieru i pozostawiane na biurku użytkownika lub przyklejone do monitora;
- dobrym rozwiązaniem jest używanie zamiast haseł kart dostępu, tj. kluczy kryptograficznych, pod warunkiem, iż są właściwie zabezpieczone, a nie pozostawione w dostępnym miejscu;
- niedozwolone jest udostępnianie komukolwiek hasła czy pinu do podpisu elektronicznego. Grozi to zachwianiem tzw. zasady rozliczności, rozumianej jako możliwość jednoznacznego wskazania osoby, która określone dane do systemu wprowadziła lub zmieniła.

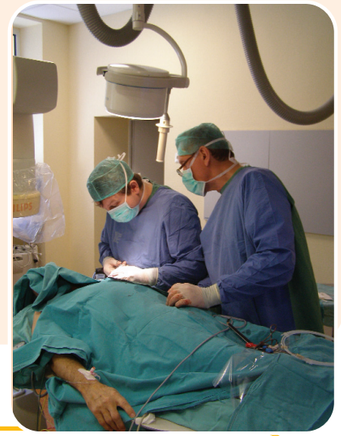
Korzystanie z poczty elektronicznej

Przez firmową skrzynkę pocztową dociera do nas większość szkodliwych programów. Przeto, używając poczty, należy być bardzo ostrożnym i:

forum

Jak w Teksasie

Nie tak dawno media relacjonowały kolejną wizytę prezydenta Lecha Wałęsy w Stanach Zjednoczonych. Tym razem nie była to podróż noblisty ani polityka, lecz wyjazd zdrowotny, spowodowany niewydolnością serca. Lech Wałęsa pojechał do kliniki Methodist DeBakey Heart and Vascular Center w Houston w stanie Teksas, gdzie przeszedł operację wszczepienia resynchronizującego rozrusznika serca.



W związku z tym warto wiedzieć, że od dwóch lat takie same zabiegi wykonywane są w naszym Ośrodku Elektroterapii Serca. Ostatni przeprowadzony został na początku marca. Rocznie koledzy kardiolodzy przeprowadzają około 30 takich operacji, a mogliby więcej. Niestety, ogranicza nas kontrakt z NFZ.

Wiosenne porządki w naszym ogrodzie

Biuletyn Szpitala Wolskiego Pr 14767

Redaguje zespół Edyta Kuklińska, Barbara Lis-Udrycka, Iwona Nowowiejska, Piotr Paczewski
e-mail redakcja@szpital.wolski, redakcja@wolski.med.pl
tel. 022 38 94 814, 0-601 31 51 01
Projekt graficzny Lena Maminajszwili/masz
Przygotowanie do druku i druk studio reklamy i wydawnictw masz

Redakcja zastrzega sobie prawo redagowania i skracania tekstów