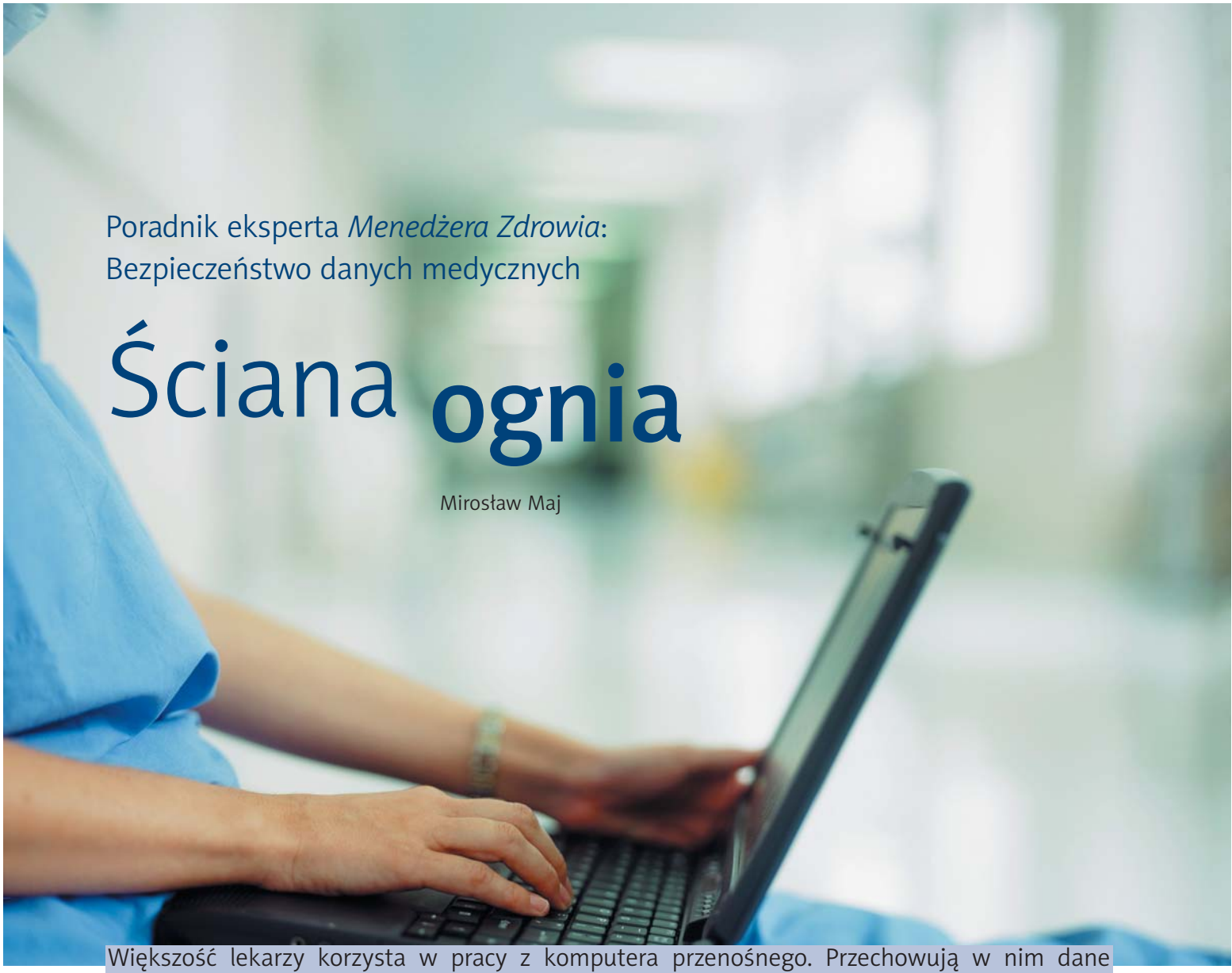
Poradnik eksperta *Menedżera Zdrowia*:
Bezpieczeństwo danych medycznych

Ściana ognia

Mirosław Maj



fot. ER Productions/Corbis

Większość lekarzy korzysta w pracy z komputera przenośnego. Przechowują w nim dane administracyjne i specjalistyczne, często takie, bez których trudno sobie wyobrazić dalsze prowadzenie terapii pacjentów. Równocześnie jednak laptopy częściej niż komputery stacjonarne padają łupem złodziei. Mogliśmy się przekonać przy okazji głośnej sprawy kradzieży komputera neurochirurgowi z Centrum Zdrowia Dziecka.

Lekarz utracił niezwykle ważne dane obserwacje medyczne pacjentów, zdjęcia, dawkowanie leków, listy oczekujących na zabieg oraz setki danych korespondencyjnych. Ich odtworzenie to żmudna praca, zajmująca dużo bezcennego – w wypadku wybitnego specjalisty czasu. Zresztą, przyznajmy szczerze – stuprocentowe odtworzenie tego, co zostało utracone, jest po prostu niemożliwe. Co robić, aby do takich sytuacji nie dochodziło? Warto przede wszystkim zwrócić uwagę na dwie sprawy – bezpieczeństwo fizyczne laptopa oraz dostępność kopii danych.

Bezpieczeństwo fizyczne laptopa

Zabezpieczenie fizyczne komputera nie jest łatwym zadaniem. Nie we wszystkich miejscach, w których przebywamy (np. w hotelach), są w pokojach sejfy, a zostawianie sprzętu w recepcji utrudnia życie – jest na tyle niewygodne, że w praktyce niestosowane. Warto więc wykazać odrobinę kreatywności i znaleźć takie miejsce w pokoju, które choć trochę utrudni *pracę* złodziejowi. Zazwyczaj dość łatwo o lepszą kryjówkę niż szuflada w biurku (nie wspominając o pozostawianiu komputera na biurku). Kolejnym, wcale nie kosztownym, rozwiązaniem jest zaopatrzenie się w stalową linkę zamykaną na kluczyk lub zamek szyfrowy. Na rynku jest dostępnych wiele zabezpieczeń zarówno prostych (www.google.pl – laptop linka stalowa), jak i bardziej zaawansowanych (np. alarm dźwiękowy). Praktycznie każdy laptop jest dostosowany do takich zabezpieczeń. Oczywiście, nie zapewnia to stuprocento-

wego bezpieczeństwa, ale może się okazać istotnym elementem, który sprawi, że sprzęt ocaleje.

Kopie zapasowe

Innym sposobem ochrony komputera jest tworzenie zapasowych dokumentów. Kopia to nie tylko zabezpieczenie na wypadek kradzieży danych, ale również niezamierzonej modyfikacji, wykasowania czy po prostu awarii dysku. Mimo rozwiniętych technik odtwarzania skasowanych lub zniszczonych danych, nie można liczyć, że taka operacja za każdym razem skończy się sukcesem. Warto zaznaczyć, że związane są z tym spore koszty. Dlatego zdecydowanie tańsze jest systematyczne archiwizowanie danych. Najprostszym sposobem jest kopiowanie co jakiś czas (np. raz na tydzień) danych na dodatkowy dysk lub płyty CD lub DVD (oczywiście w wypadku archiwizacji danych w sieci komputerowej szpitala w grę wchodzą bardziej zaawansowane techniki archiwizacji, do których często wykorzystywane jest specjalistyczne oprogramowanie. Jest to zadanie, które należy zlecić administratorowi sieci komputerowej).

Innym prostym rozwiązaniem – jeśli laptop często podłączamy do lokalnej sieci komputerowej szpitala – jest umieszczanie tych danych na dysku sieciowym i systematyczne, automatyczne ich kopiowanie na dysk lokalny (odbywa się to poprzez stałą synchronizację danych między dyskiem sieciowym a dyskiem laptopa). W wypadku utraty danych zawsze będziemy mogli je odzyskać z dysku sieciowego.

Szyfrowanie danych

Na koniec rozważań o bezpieczeństwie laptopa warto wspomnieć o szyfrowaniu danych. Jest to możliwe za pośrednictwem prostego oprogramowania, szyfrującego zasoby dysku lub cały dysk. Takie oprogramowanie powinno się stać standardem dla komputerów przenośnych. Warto pamiętać, że kradzież laptopa to również kradzież danych, a ich użycie może przynieść szkody osobom, których te dane dotyczą. Nie łudźmy się, że proste hasło jest znaczącym zabezpieczeniem przed zdeterminowanym złodziejem. Zaszyfrowanie informacji zgodnie z obwiązującymi standardami, opartymi na algorytmie szyfrującym, to zdecydowanie lepsze rozwiązanie.

Rubież ochronna

Komputery, z których korzystają lekarze i administracja szpitala, powinny być wyposażone w podstawowe zabezpieczenia przed zagrożeniami z sieci internetowej. Komputery pracujące w sieci szpitalnej najłatwiej ochronić poprzez prawidłową konfigurację tzw. styku z siecią komputerową, czyli zabezpieczenie miejsca, gdzie Internet *wchodzi* do naszej sieci i gdzie my sami z niej *wychodzimy*. To tam najłatwiej zorganizować *rubież ochronną* przed niepowołanym ruchem oraz robakami sieciowymi i wirusami. Wielu producentów oferuje oprogramowanie do kontroli tego, co dostaje się do naszej sieci (w tym zawartości poczty elektronicznej). Jest to zazwyczaj centralne oprogramowanie antywirusowe, które podejrzaną zawartość może odrzucić lub do czasu wyjaśnienia pochodzenia przesyłki skierować do kwarantanny. Ważne jest, aby po instalacji takiego rozwiązania nie zapomnieć o stałej, przeprowadzanej również automatycznie, aktualizacji wzorców wirusów. Bez tego oprogramowanie stanie się bardzo szybko bezużyteczne, gdyż w Internecie pojawiają się cały czas nowe wirusy.

Bezpieczny **laptop**

Sposoby zabezpieczenia:
- ochrona fizyczna – np. stalowa linka mocująca,
- kopia zapasowa danych znajdujących się na laptopie,
- zestaw podstawowych funkcji bezpieczeństwa – np. firewall osobisty, automatyczna aktualizacja, ochrona antywirusowa,
- szyfrowanie danych przechowywanych na dysku laptopa.

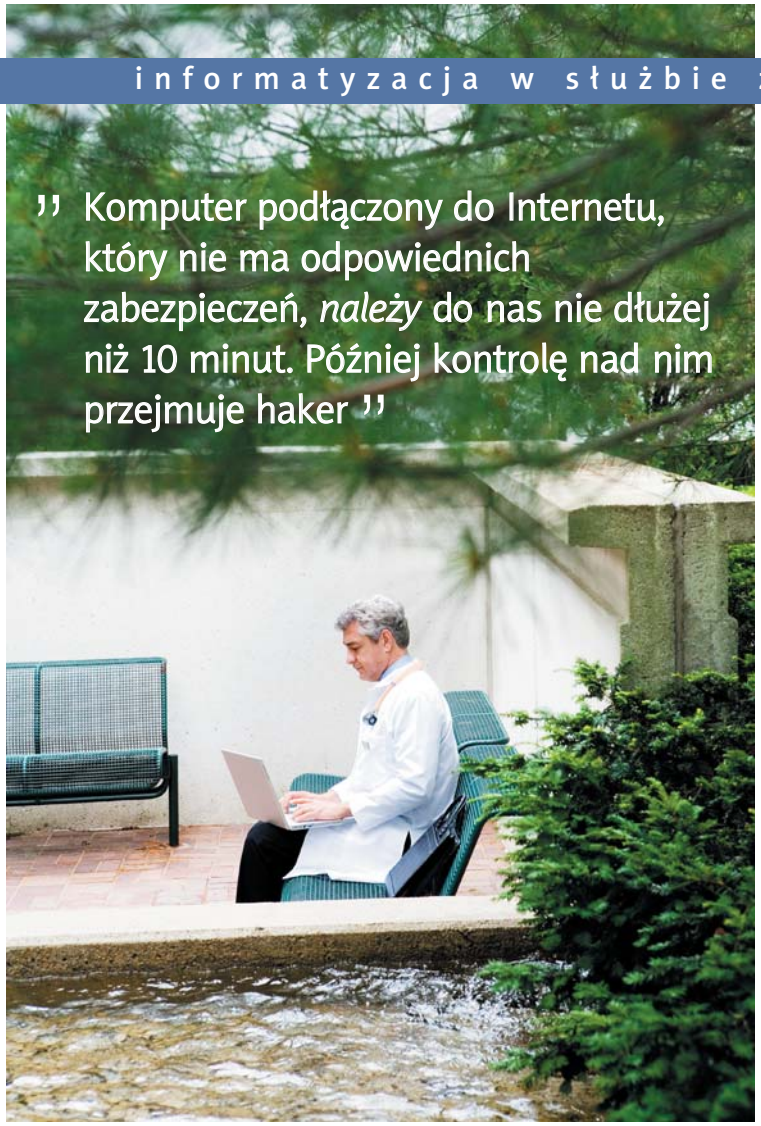
fot. Ned Frisk Photography/Brand X/Corbic

Firewall

Drugim podstawowym narzędziem ochrony styku z globalną siecią jest tzw. *firewall*, czyli zapora, która nie wpuszcza do naszej sieci ruchu innego niż uprawniony, odpowiadający używanym przez nas aplikacjom. Podstawowa zasada, jaką powinniśmy się kierować przy konfiguracji tego urządzenia, jest następująca: *na początku zablokować wszystko, a następnie dopuścić tylko ruch konieczny* (więcej na temat tego, jak skonfigurować *firewall* osobisty, można znaleźć w publikacji CERT Polska pod adresem: http://www.cert.pl/PDF/konf_pers_fw.pdf).

To, że zabezpieczyliśmy styk z Internetem, nie oznacza, że możemy zapomnieć o ochronie komputerów funkcjonujących w sieci za tym stykiem. Pracują-

> ” Dane można archiwizować, umieszczając je na dysku sieciowym i systematycznie, automatycznie kopiując na lokalny dysk laptopa ”



ce w tej strefie urządzenia możemy podzielić na dwie kategorie komputery stacjonarne oraz przenośne. Pierwsze z nich warto dodatkowo chronić, drugie trzeba. Dodatkowa ochrona komputerów stacjonarnych jest po prostu drugą linią obrony przed potencjalnym atakiem (dlatego warto rozważyć użycie innego oprogramowania niż to, które jest na styku z Internetem, aby w wypadku skutecznego ataku na jedno z rozwiązań, drugie stało się skuteczną linią oporu).

Warto przy tej okazji wspomnieć, że laptopy muszą być chronione dodatkowo. Dlaczego? Ponieważ jest rzeczą oczywistą, iż za pomocą komputera przenośnego wielokrotnie łączymy się z Internetem poza siecią szpitalną. Jak pokazują proste doświadczenia, podłączony do Internetu komputer, który nie ma odpowiednich zabezpieczeń, *należy* do nas nie dłużej niż 10 minut. Po tym czasie jego rzeczywistym właścicielem jest już ktoś inny, kto być może już zainstalował na nim skaner klawiatury, wirusa, ukradł dane albo dołączył go do swojej armii komputerów, która zaatakuje jeszcze inne komputery w sieci.

" Laptop można zabezpieczyć stalową linką zamykaną na kluczyk lub zamek szyfrowy. Można też zastosować alarm dźwiękowy "

Jak zatem zdefiniować *odpowiednie zabezpieczenia*? Jest kilka filarów bezpieczeństwa komputerów osobistych:

- bezpieczna instalacja – daje szanse na to, że nasz komputer nie zostanie skutecznie zaatakowany, nim rozpoczniemy na nim pracę,
- stała aktualizacja oprogramowania – by komputer był ciągle *łatany* i dzięki temu odporny na stale pojawiające się ataki,
- korzystanie z alternatywnych, bezpieczniejszych programów – nie zawsze programy dostarczone wraz z systemem przez producenta zapewniają najlepszą ochronę. Alternatywne programy (np. pocztowe lub przeglądarki internetowe), które zazwyczaj są bezpłatne, oferują lepsze możliwości,
- ochrona przed spamem – spam jest nie tylko źródłem niezamawianej korespondencji, będącej ofertą handlową. Bardzo często wykorzystywany jest przez przestępców jako medium do rozprzestrzeniania wirusów i innego rodzaju złośliwego oprogramowania (np. zbierającego dane o naszym zachowaniu w sieci i przesyłającego go na zewnątrz bez naszej wiedzy).

Szczegółowe informacje o tym, jak zabezpieczyć komputer, można znaleźć w publikacji wydanej przez działający przy Naukowej i Akademickiej Sieci Komputerowej zespół CERT Polska (Przemysław Jaroszewski, Rafał Tarłowski NASK/CERT Polska, *Podstawy bezpiecznego korzystania z Internetu* http://www.cert.pl/PDF/bezp_komp_internet.pdf)

Naruszanie bezpieczeństwa

Warto wspomnieć, że zgłaszanie wypadków naruszenia bezpieczeństwa teleinformatycznego jest integralnym elementem dbałości o bezpieczeństwo w sieci. Wszystkich, którym takie nieszczęście się przytrafiło, zachęcamy, by powiadomili o tym wspomniany zespół CERT Polska. Na stronach CERT Polska dostępny jest formularz do zgłaszania takich przypadków (https://www.cert.pl/formularz/formularz.php). Informując o incydencie, możemy liczyć na bezpłatną pomoc w postaci podstawowych wskazówek dotyczących dalszego zachowania, w tym zabezpieczenia technicznego. Warto też pamiętać, że to, co nam się przytrafiło, jest zazwyczaj jedynie elementem większej całości i zgłoszenie może pomóc innym w ochronie ich komputerów.

Autor jest szefem polskiego zespołu ds. reagowania na naruszenia bezpieczeństwa w Internecie (NASK/CERT).
Publikacja jest kontynuacją artykułu dotyczącego bezpieczeństwa danych medycznych (Informacje cenne jak złoto, Menedżer Zdrowia nr 7/2007).