Poradnik bezpieczeństwa w Internecie

Raiffeisen POLBANK

Bankowość elektroniczna, internetowa, mobilna

Opracował: Janusz Nawrat

Dyrektor Departamentu Bezpieczeństwa Informacji
i Systemów Informatycznych Raiffeisen Polbank

Ponad 20 milionów Polaków między 15. a 64. rokiem życia ma dostęp do Internetu. Badania wykazują, że spędzają w sieci do sześciu godzin dziennie. Internetu i komputerów używają nie tylko do pracy, lecz także do zdobywania informacji, zabawy, surfowania po Internecie, czytania poczty, robienia zakupów, korzystania z komunikatorów i serwisów społecznościowych oraz obsługi bankowości internetowej. Zatem od bezpieczeństwa naszego komputera zależy w dużym stopniu bezpieczeństwo naszych danych osobistych i finansów. Uświadomienie sobie tego faktu jest bardzo ważne – na tyle, że dbałość o bezpieczeństwo komputera powinna na stałe wpisać się w nasze życie.

Zagrożenia występujące w Internecie

Internetowi oszuści wybierają coraz częściej najprostszą drogę do osiągnięcia swojego celu – atakują komputery poszczególnych użytkowników. Niestety są one zazwyczaj słabo zabezpieczone, często również działa na nich „dziurawe", od dawna nieaktualizowane standardowe oprogramowanie, które jest bardzo podatne na ataki oszustów. Oznacza to, że długo nieaktualizowane, a powszechnie wykorzystywane aplikacje – takie jak np. Microsoft Office, Adobe Reader czy Flash Player – mogą być wykorzystywane przez oszustów – hakerów – do zdalnego zaatakowania komputera i przejęcia nad nim kontroli.

Po udanym ataku oszust może zyskać pełną władzę nad naszym komputerem – oznacza to, że podobnie tak jak my ma do niego nieograniczony dostęp. Trzeba też pamiętać o tym, że najczęstszym sposobem rozprzestrzeniania się ataków jest szkodliwe oprogramowanie, czyli między innymi wirusy, robaki internetowe i oprogramowanie szpiegujące oraz tzw. wytrychy (exploits) służące do penetrowania dopiero co odkrytych luk w zabezpieczeniach oprogramowania.

Co nam grozi, jeśli nie zadbamy o bezpieczeństwo naszego komputera?

Przejęcie zdalnej kontroli nad komputerem – a tym samym dostęp oszustów do naszych danych – jest możliwe i bardzo prawdopodobne w sytuacji:

- **braku oprogramowania antywirusowego** lub braku jego regularnej aktualizacji,
- **zaniedbania** w przeprowadzaniu regularnych, pełnych **skanów antywirusowych** komputera,
- **braku lub niepoprawnej konfiguracji osobistej zapory sieciowej** (personal firewall) – czy to sprzętowej, w dzisiejszych czasach często spotykanej w routerach klasy Home Office, czy to programowej, instalowanej bezpośrednio na naszym komputerze,
- **używania starych**, nieaktualnych i pełnych błędów **przeglądarek internetowych**,
- **braku aktualizacji oprogramowania systemowego i aplikacji**, np. stare wersje Adobe Reader, Java, Flash Player itp.,
- **braku wiedzy po stronie użytkownika na temat istniejących zagrożeń**, z czym wiąże się narażenie na sprytne socjotechniki internetowych oszustów.

Z reguły atak na słabo zabezpieczony lub całkowicie niezabezpieczony komputer zaczyna się zainfekowaniem komputera poprzez szkodliwe oprogramowanie albo „uderzeniem" hakera poprzez lukę w bezpieczeństwie systemu. Wspomniana luka jest najczęściej pochodną błędów istniejących w kodzie lub konfiguracji oprogramowania. Przeprowadzając atak, oszust używa tzw. wytrychu, umożliwiającego „niewinne" podglądanie tego, co robi użytkownik komputera, które obejmuje:

- **podglądanie internauty** przy pomocy kamerki,
- **podsłuchiwanie** przez mikrofon,
- **rejestrowanie aktywności** klawiatury oraz myszki,
- **wykonywanie zrzutów ekranowych** lub rejestrowanie w formie filmu przebiegu pracy na komputerze.

Wszystko to prowadzi ostatecznie do pełnego przejęcia kontroli nad zaatakowaną stacją, a nawet do wykorzystania zainfekowanego komputera do innych form przestępczego procederu, np. do wysyłania spamu, atakowania innych komputerów, udziału w praniu nieuczciwie zdobytych pieniędzy itd.

Jak może wyglądać atak oszusta internetowego na komputer użytkownika?

W praktyce scenariusze ataku hakera mogą wyglądać następująco:

Przykład 1

> Do potencjalnej ofiary wysyłane są e-maile z załącznikami w postaci np. faktur od legalnego dostawcy czy też kontrahenta w plikach PDF – które nie wzbudzają podejrzeń, ponieważ ich wygląd wydaje się potwierdzać ich autentyczność. Jednak do dokumentu sprytnie „doczepiony" jest kod tzw. wytrycha, który – wykorzystując błędy w programie Adobe Reader – uruchamia się automatycznie na komputerze użytkownika w momencie odczytu dokumentu. Czyni to przeważnie w bardzo dyskretny sposób, bez alarmów i jakichkolwiek komunikatów, nie wzbudzając tym samym żadnych podejrzeń użytkownika. Wspomniany kod albo sam „oprogramowuje" cały scenariusz ataku, albo też może być odpowiedzialny za późniejsze pobranie z sieci i zainstalowanie na zaatakowanym sprzęcie dodatkowego oprogramowania szkodliwego (malware), ułatwiającego przejęcie kontroli nad komputerem ofiary.

Przykład 2

> Ofiara zachęcana jest do odwiedzin na stronach internetowych, na których prezentowane są spreparowane, złośliwe treści, na przykład grafiki z doklejonym szkodliwym kodem. Treści te, wyświetlone w przeglądarce internetowej, która nie była aktualizowana, powodują efekt identyczny jak w przykładzie omawianym powyżej. W tym przypadku – oprócz odwiedzenia zainfekowanej strony – nie wymaga to nawet żadnej interakcji z użytkownikiem („klikania" na cokolwiek), więc atak jest jeszcze trudniejszy do uniknięcia.

W obu przykładach warunkami sukcesu ataku oszusta były niewystarczający poziom ochrony komputera i zaniedbanie jego bezpieczeństwa – polegające na niezaktualizowaniu oprogramowania używanego do codziennej pracy: w pierwszym przykładzie był to Adobe Reader, w drugim zaś „niewinna" przeglądarka internetowa.

W jaki sposób możemy się bronić przed oszustami w Internecie?

Najlepszym sposobem zapewnienia ochrony jest stosowanie na co dzień podstawowych zasad bezpieczeństwa:

- niepobieranie z Internetu oprogramowania z nieznanych lub niezaufanych źródeł,
- unikanie surfowania po podejrzanych stronach WWW,
- bieżące aktualizowanie (najlepiej automatyczne) systemu operacyjnego i oprogramowania użytkowego oraz instalowanie do nich odpowiednich „łatek",
- używanie dobrego oprogramowania antywirusowego, a najlepiej pakietu zintegrowanych narzędzi do ochrony komputera, zawierającego – obok skanera antywirusowego – dodatkowo osobistą zaporę sieciową (personal firewall), osobisty system przeciwdziałania włamaniom (host intrusion prevention system – HIPS) itp.,
- wykonywanie częstych skanów antywirusowych (pełny skan co najmniej raz na tydzień), nielekceważenie komunikatów i ostrzeżeń, podejmowanie natychmiastowych działań w odpowiedzi na istotne alerty z systemów ochrony komputera o próbie przełamania jego zabezpieczeń itp.

W razie wątpliwości co do tego, jakie działania należy podjąć w odpowiedzi na alert z systemów zabezpieczeń, zawsze warto skorzystać z wiedzy doświadczonego informatyka lub specjalisty od bezpieczeństwa.

W jaki sposób korzystać bezpiecznie z komputera i nie dać się zwariować?

Aby korzystanie z internetowych systemów transakcyjnych było bezstresowe i bezpieczne dla nas oraz naszego portfela, należy pamiętać o kilku elementarnych zasadach:

- **Komputer powinien być zabezpieczony odpowiednim, dobrej jakości oprogramowaniem chroniącym go przed wirusami i atakami z sieci.** Należy go wyposażyć w legalne oprogramowanie, bo tylko takie pochodzi z zaufanych źródeł i upoważnia nas do korzystania z aktualizacji oraz poprawek bezpieczeństwa. Wszystkie zalecane przez dostawców danego oprogramowania poprawki, aktualizacje czy „łatki" powinny być bezzwłocznie instalowane, ponieważ wiele z nich koryguje identyfikowane na bieżąco krytyczne podatności – będące dla hakerów niczym wrota do przeprowadzania ataków. Najlepiej jest włączyć automatyczne aktualizacje – wszędzie, gdzie tylko to możliwe. Jeśli jednak z jakichś powodów trzeba pobierać aktualizacje oprogramowania w sposób manualny, należy to czynić wyłącznie poprzez stronę producenta i – co bardzo ważne – tylko przez szyfrowane połączenie (protokół HTTPS, nie HTTP). Dzięki temu bowiem można zapobiec ingerencji hakerów w nieszyfrowany strumień ruchu sieciowego i podstawieniu szkodliwego oprogramowania w miejsce legalnych aktualizacji. Na komputerze musi działać osobista zapora sieciowa, w której należy ustawić blokadę wszystkich połączeń przychodzących do zabezpieczonego komputera. Nie utrudnia to korzystania ze sprzętu dopóty, dopóki nie udostępniasz na nim usług sieciowych (na przykład WWW) innym użytkownikom. Jeśli jednak tak jest, to z całą pewnością będziesz w stanie skonfigurować odpowiednią regułę na firewallu, która uprawni ruch na określony port udostępnianej usługi. Oprócz klasycznego antywirusa, w celu podniesienia bezpieczeństwa swojego komputera możesz zainstalować na nim dodatkowe narzędzia chroniące przed szkodliwym oprogramowaniem, takie jak: Bit9 (narzędzie do whitelistingu programów) czy EMET (unieszkodliwi wiele wytrychów, jeśli już dotrą do Twojego komputera).

- **Na co dzień nie należy korzystać na komputerze z kont z uprawnieniami administratora, a tzw. konta gościa i pomocy zdalnej w zasadzie powinny być zablokowane.** Do normalnej pracy z komputerem należy wykorzystywać konta nieuprzywilejowane, ponieważ w razie ataku (na przykład z użyciem szkodliwego oprogramowania) agresorzy będą mieli znacznie utrudnione lub wręcz uniemożliwione wykonanie czynności związanych z ewentualnym przejęciem zdalnej kontroli nad komputerem.

- **Nie możemy udostępniać swoich komputerów osobom postronnym.** Ponadto powinniśmy zadbać o zabezpieczenie swojego sprzętu przed kradzieżą, zagubieniem, uszkodzeniem, zniszczeniem i nieuprawnionym użyciem. W szczególności należy zapewnić ochronę komputera pozostawianego bez osobistego nadzoru. Szczególna dbałość o fizyczne bezpieczeństwo sprzętu oznacza między innymi: niepozostawianie urządzeń w samochodzie i w pokojach hotelowych oraz ciągły nadzór nad komputerem w podróży. Podczas korzystania z publicznych środków transportu (autokar, samolot) należy zawsze przewozić laptopa czy tablet w taki sposób, by mieć je stale na oku – czyli jako bagaż podręczny. W razie kradzieży komputera staje się on dla złodzieja wielką kopalnią tzw. danych wrażliwych. Podstawowym sposobem zabezpieczenia tych informacji jest zaszyfrowanie całego dysku twardego. Praktycznie dla wszystkich systemów istnieją odpowiednie do tego celu narzędzia (BitLocker dla Windows, FileVault 2 dla Mac OS czy dm-crypt dla Linux). W przypadku zastosowania szyfrowania dysku należy zadbać o przygotowanie i zabezpieczenie na zewnętrznym nośniku (na przykład na dysku USB) niezaszyfrowanej kopii zapasowej danych, ponieważ awaria zaszyfrowanego dysku na ogół wiąże się z nieodwracalną utratą tych danych. Komputer powinien mieć założone hasło na dostęp do BIOS-u (lub tzw. startup password w komputerach Mac). Samo w sobie nie stanowi to zabezpieczenia niemożliwego do obejścia, ale w połączeniu z szyfrowanym dyskiem uniemożliwia odczytanie danych wrażliwych z komputera.

- **Podnieś bezpieczeństwo swojej przeglądarki internetowej.** Wyłącz niepotrzebne wtyczki, takie jak na przykład Java. Włącz funkcję click2play dla wtyczek, dzięki czemu takie treści jak filmy, animacje i pliki multimedialne, do których najczęściej „doczepiane" są złośliwe kody, nie będą automatycznie odtwarzane w przeglądarce. Odtworzenie ich oczywiście będzie możliwe, lecz dopiero po kliknięciu w nie – czyli w sposób intencjonalny i świadomy. Zainstaluj przydatne rozszerzenia przeglądarki, na przykład NoScript (blokada JavaScript dla Firefox), NoScripts (blokada JavaScript dla Chrome), HTTPS Everywhere (wymusza szyfrowane połączenia, jeśli tylko są możliwe).

- **Nie umieszczaj w sieci danych wrażliwych.** Nie wysyłaj e-mailem niezaszyfrowanych informacji poufnych. Ogólnie rzecz biorąc, uważaj na wszystko, co wysyłasz w sieci.

- **Hasła powinny być traktowane przez każdego z nas tak, jak traktuje się klucz do skarbca.** Wiadomo, że utrata tego klucza oznacza kłopoty i ma przeważnie bardzo poważne konsekwencje. Podobnie jak z kluczem do skarbca czy do domu, rzecz ma się z hasłami. Ich ujawnienie wiąże się bowiem z niebezpieczeństwem uzyskania przez agresorów nieuprawnionego dostępu do systemów; występują oni wówczas w naszym imieniu, ze wszystkimi tego – nieraz bardzo bolesnymi – konsekwencjami. Warto więc pamiętać o podstawowych zasadach bezpieczeństwa: (1) tworzenie haseł, (2) posługiwania się nimi oraz (3) zarządzania nimi (zmiana, przechowywanie).

- **Należy zabezpieczyć dodatkowe urządzenia, służące do uwierzytelniania dostępu do systemów i do autoryzacji transakcji.** Mowa o tokenach i telefonach, na które wysyłane są kody jednorazowe do autoryzowania transakcji oraz komunikaty o zdarzeniach związanych z korzystaniem z internetowych systemów transakcyjnych (logowaniach, operacjach itp.). Tokeny z kluczami kryptograficznymi do podpisywania transakcji powinny być podłączane do komputera wyłącznie na czas korzystania z systemu transakcyjnego. Innymi słowy, nie mogą pozostawać podłączone do niego na stałe.
- **Powinniśmy unikać uruchamiania wykonywalnych plików (na ogół z rozszerzeniami nazw: .exe, .com, .bat, .dll, .cmd, .vbs, .vbe lub .pif), otrzymanych w załącznikach do e-maili.** To samo odnosi się do pobierania i uruchamiania wykonywalnych plików ze stron WWW oraz kopiowania danych z niesprawdzonych nośników.

W jaki sposób tworzyć hasła do systemów bankowości internetowej?

Przy tworzeniu hasła powinniśmy pamiętać o następujących zasadach:

- **hasła nie powinny być frazami słownikowymi** (polskimi i obcojęzycznymi),
- hasło powinno zawierać **co najmniej 8 znaków**,
- **hasło nie powinno bazować na znanych danych osobowych** użytkownika lub być znaną powszechnie nazwą czy identyfikatorem, jak na przykład imieniem (własnym, przyjaciela, członka rodziny itp.), nazwiskiem, nazwą (na przykład systemów, poleceń, programów, procesów itp.), nazwą organizacji lub jej struktur, datą (datą urodzin, datą dobrze znanych wydarzeń historycznych itp.), adresem, numerem telefonu oraz kombinacjami wymienionych fraz,
- **hasło nie może być kombinacją powtarzających się znaków** (na przykład aaabbbccc), łatwo przewidywalną sekwencją znaków (na przykład 12345, qwerty itp.) lub ich odwrotną transpozycją (np. 54321),
- **hasło nie może być prostą kombinacją jednej ze wspomnianych fraz** wraz z cyfrą na początku lub na końcu (na przykład secret1 czy 1secret),
- **silne hasło musi zawierać kombinację zarówno małych, jak i wielkich liter oraz znaków specjalnych** (na przykład takich jak: !@#$%^&*()_+|~-=\`{}[]:";'<>?,./),
- **zalecanym sposobem tworzenia silnych haseł są tzw. pass-frazy**, tworzone zgodnie z następującym schematem: (1) należy opracować zdanie bazowe do pass-frazy, na przykład: „Czy można stworzyć bezpieczne hasło?", (2) należy wyróżnić w zdaniu bazowym charakterystyczne elementy pass-frazy, (3) należy dokonać mapowania wyróżnionych elementów pass-frazy na przyjęte, łatwe do zapamiętania reprezentujące je symbole i przeprowadzić ewentualną podmianę znaków (zmiana wielkości, znaki specjalne): Czy → 3; m → M; s → s; b → B; has → # (od „hasz"), ło? → 1o?, w wyniku czego powstaje silna pass-fraza, na przykład: 3MsBez#1o?.

Posługując się hasłami, powinniśmy pamiętać o tym, aby:

- **nie używać takich samych haseł do uwierzytelnień we wszystkich systemach**, do których się logujemy – na przykład do logowania się do systemu bankowości internetowej nie powinniśmy stosować hasła identycznego jak to, którego używamy w systemach pocztowych czy portalach społecznościowych (z portali społecznościowych czy z publicznych systemów pocztowych coraz częściej wyciekają różne informacje, zatem trzeba dbać o to, aby wyciek danych nie oznaczał jednocześnie ujawnienia naszego hasła do bankowości internetowej),
- **nie współdzielić hasła z innymi użytkownikami** (nawet członkami rodziny),
- **nie ujawniać haseł innym osobom** (w bezpośredniej rozmowie, przez telefon, w SMS-ach, w wiadomościach poczty).

W jaki sposób bezpiecznie zarządzać hasłami do bankowości internetowej?

W celu zapewnienia maksymalnej ochrony haseł należy:

- **nie zapamiętywać haseł w systemach i aplikacjach**, chyba że zapisujemy je w specjalnie do tego celu przeznaczonej aplikacji (tzw. Password Manager), przechowującej hasła w szyfrowanych bazach (polecam oprogramowanie KeePass dostępne dla każdego systemu operacyjnego, łącznie z systemami na urządzenia mobilne),
- **nie zapisywać haseł w postaci jawnej**, możliwej do odczytania przez niepowołane osoby,
- **zmieniać hasła regularnie**, przynajmniej raz na dwa miesiące – a ponadto należy je zmieniać natychmiast, w sytuacji gdy zachodzi podejrzenie ich ujawnienia niepowołanym osobom.

Internet może i powinien być bezpiecznym miejscem dla osób przestrzegających opisanych w niniejszym poradniku zasad postępowania. Trzeba jednak pamiętać o tym, że bezpieczeństwo jest wypadkową zarówno zastosowanych rozwiązań technicznych, jak i zachowań użytkownika. Zawsze też decyduje tu najsłabszy element. Na nic zda się nam nawet najdoskonalszy system zabezpieczeń, jeśli będziemy lekceważyć wszelkie jego ostrzeżenia o zagrożeniach oraz zaniedbywać podstawowe zasady bezpiecznego korzystania z komputera.

Strefa Obsługi Biznesu
22 548 99 00
raiffeisenpolbank.com

* Koszt połączenia według taryfy operatora.