Bezpieczeństwo zakupów

w polskich sklepach internetowych

Kupujesz w Internecie? Zobacz, czy to bezpieczne...

RAPORT
marzec
2011

PARTNERZY RAPORTU

//CertyfikatySSL.pl Domeny.pl polskihosting.pl

Euromonitor International

Wstęp

Polski rynek e-commerce rozwija się bardzo dynamicznie, zwiększając stale swoją wartość. Według analiz jego wartość szacowana jest na **17,6 mld** złotych, a w bieżącym roku Internauci dokonają zakupów za niemal **7,5 mld** złotych. To o **1 mld** więcej niż w roku ubiegłym. Klientem e-sklepów jest już co trzeci Polak.

Na wzrost deklarowanej liczby transakcji ma wpływ rosnąca liczba użytkowników Internetu oraz coraz większa świadomość wygody e-zakupów. Niewielka jest jednak wiedza internautów o zagrożeniach związanych z przesyłaniem danych on-line, możliwościach ich kradzieży oraz o ogólnej charakterystyce cyberprzestępczości.

Niestety, rozwój e-commerce wpływa również na rozwój działalności hakerów, którzy z każdym dniem mają więcej możliwości do przechwycenia danych teleadresowych, numerów kont bankowych, kart kredytowych, haseł zabezpieczających itp.

Walka z hakerami jest nierówna. Ich działalność bazuje na społecznej nieświadomości w zakresie e-bezpieczeństwa oraz na oszczędnych zabezpieczeniach danych, wprowadzanych przez właścicieli sklepów internetowych.

Przygotowany przez nas raport dotyczy poziomu bezpieczeństwa polskich sklepów internetowych. Wyniki przeprowadzonych badań pokazują, że mimo łatwego dostępu do narzędzi ochrony danych, korzysta z nich minimalny procent polskiego rynku e-commerce.

Domeny.pl była jedną z pierwszych firm hostingowych w Polsce. Dzisiaj to liczący się w kraju dostawca usług internetowych. Działalność rozpoczęła w 1997 roku od rejestracji domen i obsługi serwerów wirtualnych. Teraz oferuje wiele dodatkowych usług związanych m.in. z: bezpieczeństwem w Internecie (Certyfikaty SSL), monitoringiem pracy serwerów, e-reklamą oraz e-biznesem.

Domeny.pl

Spis treści

Domeny.pl

Metodologia

Bezpieczny e-sklep to taki, który **chroni swoich klientów** przed zagrożeniami w Internecie. Do głównych niebezpieczeństw w sieci należą kradzieże przesyłanych danych. Działalność sklepów internetowych opiera się na transmisji poufnych danych klientów, którzy ufają, że są one chronione. Bezpieczny e-sklep powinien szanować ich **zaufanie**. Szczególnie poprzez ochronę klienta i informacji o nim (osobowych, teleadresowych, haseł dostępu do kont, płatności itp.).

Sklepy zgłoszone do konkursu były oceniane według kilku kryteriów, określonych w regulaminie. Ochrona danych osobowych jest jednym z nich. Prezentowany przez nas raport skupia się natomiast głównie na ochronie prywatnych danych przesyłanych on-line.

Sprawdziliśmy, ile sklepów gwarantuje swoim klientom bezpieczeństwo przesyłania danych. Impulsem do badania stał się konkurs **„Bezpieczny eSklep”**, organizowany przez Instytut Logistyki i Magazynowania. Zgłoszenia przyjmowano do 4 lutego br. Warunkiem przystąpienia do konkursu było prowadzenie działalności od co najmniej 12 miesięcy przed datą zgłoszenia oraz wpis na listę. Stała się ona bazą wyjściową naszego badania.

Badanie „Bezpieczeństwo zakupów w polskich sklepach internetowych” zostało przeprowadzone w styczniu i lutym 2011 roku na **1428** sklepach internetowych. Tyle e-sklepów było wpisanych na listę uczestników powyższego konkursu. Bezpieczeństwo przesyłanych danych zostało sprawdzone poprzez weryfikację zainstalowanego certyfikatu SSL, który jest jednym z narzędzi ochrony informacji przesyłanych on-line. Jest to również powszechnie znany sposób szyfrowania danych stosowany przez banki, urzędy, instytucje rządowe i prywatne oraz największe serwisy e-commerce. Należy również wziąć pod uwagę, że certyfikaty SSL są dostępne dla wszystkich. Wystarczy być właścicielem domeny internetowej, aby móc go zainstalować.

Od 1 stycznia 2011 r. minimalna długość klucza to 2048-bitów. Więcej na: https://certyfikatyssl.pl

Bezpieczeństwo każdego e-sklepu zostało zweryfikowane na podstawie:

- posiadania zainstalowanego certyfikatu SSL, a zwłaszcza:
  - jego ważności,
  - zaufanego wystawcy (Urzędu Certyfikującego),
  - poprawnego klucza szyfrowania,
- automatycznej zmiany protokołu http:// na https:// w najbardziej newralgicznych punktach przesyłania danych, tj. na podstronach, gdzie następuje:
  - logowanie klienta,
  - rejestracja użytkownika,
  - złożenie zamówienia,
- używanych znaków bezpieczeństwa i informowania klientów o bezpieczeństwie na stronie,
- niezależnej oceny zabezpieczeń certyfikatu SSL przez zewnętrzne narzędzie SSL Labs.

SSL Labs jest niekomercyjnym narzędziem badawczym należącym do firmy Qualys.

Domeny.pl

Badanie przebiegało w dwóch etapach.

Data ważności i zaufanie do wystawcy to podstawowe czynniki, które wpływają na ocenę certyfikatu; jeśli nie są zadowalające, certyfikat automatycznie otrzymuje 0 punktów.

Etap I

Wszystkie adresy sklepów internetowych zostały przeskanowane wyszukiwarką SSL Labs. To niezależne narzędzie, które sprawdza konfigurację certyfikatów SSL na danym serwerze. Przyznaje również oceny A-F (wg punktacji od 0 do 100: F < 20, E >= 20, D >= 35, C >= 50, B >= 65 i A >= 80) oraz wyświetla uwagi.

Wyszukiwarka bierze pod uwagę:

- datę ważności certyfikatu,
- zaufanie do wystawcy,
- konfigurację serwera w trzech kategoriach:
  - obsługa protokołu SSL 30%,
  - obsługa wymiany kluczy 30%,
  - obsługa szyfrowania 40%.

Obsługa protokołu SSL

Każdy serwer może obsługiwać różne typy protokołów. Nie wszystkie są tak samo skuteczne. Znana jest np. słabość protokołu SSL 2.0. Z tego względu SSL Labs ocenia obsługę protokołu wg algorytmu:

- wynik najsilniejszego protokołu
- zsumowany z oceną najsłabszego protokołu
- podzielone przez 2.

Oceny procentowe protokołów:

SSL 2.0.....20%
SSL 3.0.....80%
TLS 1.0.....90%
TLS 1.1.....95%
TLS 1.2.....100%

Obsługa wymiany kluczy

Proces składa się z dwóch faz: uwierzytelnienia oraz weryfikacji bezpieczeństwa wygenerowanych kluczy (publicznego i prywatnego) wraz z ich wymianą.

Od 2011 roku najkrótszym uznawanym kluczem szyfrowania jest klucz 2048-bit. Im więcej bitów ma klucz prywatny, tym trudniej jest go złamać. Słaby klucz lub proces wymiany, który używa tylko części klucza, może wpływać na złamanie połączenia.

Oceny procentowe kluczy (dane z 2009 r.):

słaby klucz.....0%
brak klucza.....0%
krótszy niż 512-bitów.....20%
limit 512-bitów.....40%
krótszy niż 1024-bitów.....40%
krótszy od 2048-bitów.....80%
krótszy od 4096-bitów (np. 2048).....90%
dłuższy lub równy 4096-bitów.....100%

Obsługa szyfrowania

Mocniejszy algorytm szyfru zapewnia silniejsze szyfrowanie połączenia, a tym samym zmniejsza prawdopodobieństwo jego przerwania. Ponieważ serwer może obsługiwać różnego rodzaju szyfry, najmniej punktów przyznaje się najsłabszym. Obliczanie wyniku tej kategorii następuje wg wzoru:

- ocena najsilniejszego szyfru
- zsumowana z wynikiem najsłabszego szyfru
- podzielone przez 2.

Sposób procentowej oceny szyfrowania:

brak.....0%
poniżej 128-bitów (40, 56).....20%
128-256 (128, 168).....80%
256 lub więcej.....100%

Końcowy wynik SSL Labs jest kombinacją pozostałych komponentów konfiguracji serwera (m.in. zabezpieczenia domeny z lub bez przedrostka www), ale nie wszystkie mają tak istotny wpływ na ostateczną ocenę, jak trzy wymienione powyżej. Niektóre składowe konfiguracji certyfikatu na serwerze osłabiają ostateczny wynik. Nie są jednak w stanie zniżyć go do zera, jeśli powyższe punkty są spełnione na zadowalającym poziomie. Wyjątkiem jest niedopasowanie nazwy domeny do certyfikatu (tzw. **mismatch**).

Mismatch – sytuacja, gdy certyfikat SSL jest zainstalowany na serwerze, na którym znajduje się sprawdzana domena, jednak nie jest on dla niej wystawiony.

Domeny.pl

Sprawdziliśmy, jaki procent sklepów internetowych podaje swoim klientom nieprawdziwe informacje o zabezpieczeniach.

Etap II

W kolejnej fazie weryfikacji każda domena sklepu internetowego została wpisana do przeglądarki internetowej. W ten sposób sprawdzono, czy serwer automatycznie przekierowuje protokół http:// na https:// na podstronach:

- logowania,
- rejestracji
- i składania zamówienia.

Analizie poddane zostały także strony główne, na których sprawdzono obecność znaków bezpieczeństwa (np. kłódek i kluczy przy polach logowania lub w stopce). W ten sposób zweryfikowano, jaki procent sklepów internetowych podaje swoim klientom nieprawdziwe informacje dotyczące zabezpieczeń serwisu.

Te dwa etapy badań pozwoliły na zebranie obiektywnych danych dotyczących bezpieczeństwa e-sklepów w Polsce. Wszystkie przeanalizowane adresy sklepów internetowych zostały wpisane na listę konkursu „Bezpieczny eSklep" przez zarządzające nimi osoby. Powstała w ten sposób baza informacji o działalności 1428 sklepów, stanowiąca zarys polskiego rynku e-commerce.

Wszystkie zebrane dane zostały przedstawione z komentarzem w dalszej części raportu.

Bezpieczeństwo e-sklepu

O bezpieczeństwie sklepów internetowych decyduje kilka podstawowych czynników. Wszystkie z nich opierają się na narzędziach ogólnodostępnych na rynku.

Posiadanie ważnego certyfikatu SSL

Jednym ze sposobów wyświetlenia szczegółów certyfikatu jest kliknięcie ikony bezpieczeństwa (kłódki) w prawym dolnym rogu przeglądarki internetowej.

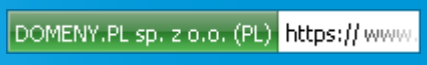
Certyfikaty SSL wydawane są na okres od 1 do 10 lat, w zależności od wystawcy. Ich ważność i pozostałe **kluczowe informacje są dostępne po wyświetleniu szczegółów certyfikatu**. Może się zdarzyć, że witryna zawiera treści niepodpisane certyfikatem (np. linki zewnętrzne). Wówczas na kłódce w prawym dolnym rogu pojawia się ostrzeżenie w postaci czerwonego wykrzyknika. Warto również zaznaczyć, że bezpieczne korzystanie ze strony umożliwia jedynie ważny certyfikat SSL. Samo zainstalowanie certyfikatu nie gwarantuje bezpieczeństwa.

Automatyczne przekierowanie na protokół https://

„s" w pasku adresu znaczy chroniony - od angielskiego słowa *secure.*

https:// to jeden ze znaków potwierdzających posiadanie zainstalowanego certyfikatu SSL. Litera „s" dodana do standardowego protokołu http:// jest gwarancją szyfrowania połączenia i bezpieczeństwa przesyłanych danych (jest to skrót od angielskiego słowa *secure* – bezpieczny, chroniony).

Za bezpieczne e-sklepy uznaje się takie serwisy, których strona logowania, rejestracji bądź realizacji zamówienia jest automatycznie przekierowana na protokół https://, bez konieczności wykonywania dodatkowych czynności przez użytkownika (takich, jak dodawanie wyjątków do przeglądarki, samodzielne wpisywanie **„s"** w pasku adresu).



Znaki bezpieczeństwa

Jest kilka podstawowych znaków graficznych, informujących użytkowników o bezpiecznych witrynach i szyfrowanych połączeniach. Część z nich to tzw. pieczęci bezpieczeństwa, instalowane razem z certyfikatem SSL (wydawane przez Urzędy Certyfikacji). Zawierają one dane dotyczące firmy i informują o szyfrowaniu połączenia. Drugą grupę stanowią symbole powszechnie kojarzone z bezpieczeństwem, czyli wszelkiego rodzaju kłódki, klucze etc. Kłódka pojawiająca się przy polu logowania czy rejestracji sugeruje użytkownikowi, że proces ten jest bezpieczny. Niestety, duży procent tych znaków to tylko elementy graficzne, które mogą wprowadzić potencjalnego klienta w błąd. **Sama kłódka nie jest gwarancją bezpieczeństwa.**

Domeny.pl

Więcej na:
https://certyfikatyssl.pl

Moc szyfrowania

Od **1 stycznia 2011** roku **jedynym gwarantem bezpieczeństwa** przesyłanych danych są certyfikaty SSL z kluczami o długości **2048-bitów**. Nowe normy bezpieczeństwa zostały ustalone przez Narodowy Instytut Standaryzacji i Technologii z USA (The National Institute of Standards and Technology) i obowiązują do odwołania.

Zastosowanie wymienionych wyznaczników jest gwarantem bezpiecznej transmisji danych i zaufania klientów.

Wyniki badania

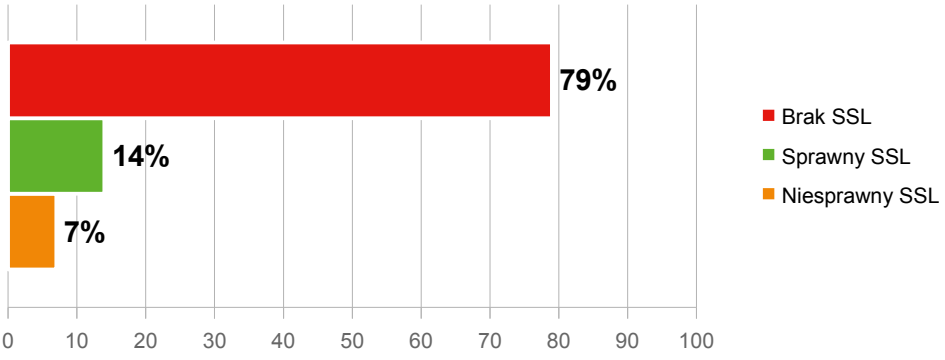
Wykryte certyfikaty SSL

Po analizie wszystkich **1428** domen e-sklepów w wyszukiwarce SSL Labs, a następnie manualnej weryfikacji adresów w celu sprawdzenia zainstalowanego certyfikatu SSL, okazało się, że jedynie **21%** z nich (**301**) posiada certyfikaty SSL. **17%** sklepów z certyfikatami SSL (**241**) zostało wskazanych przez SSL Labs, natomiast pozostałe **4%** (**60**) zweryfikowano poprzez sprawdzenie protokołów http:// oraz https:// na stronie internetowej. Zostały one wcześniej zakwalifikowane przez wyszukiwarkę SSL Labs jako „mismatch" lub „nie znaleziono połączenia z serwerem".

Sprawne certyfikaty SSL

Jedynie 14% z badanych e-sklepów posiada sprawny certyfikat SSL.

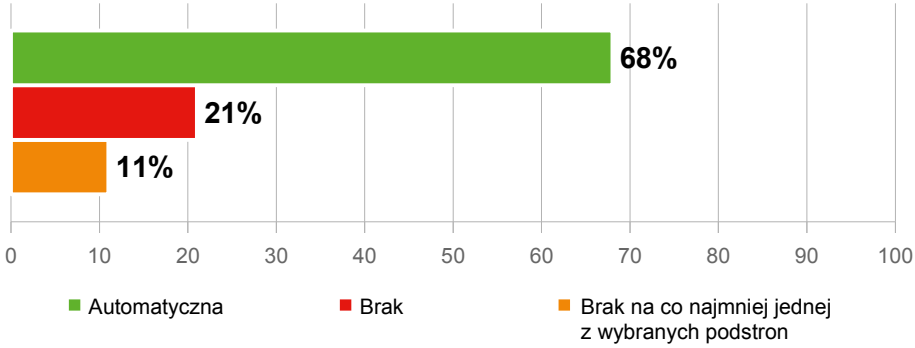
Dalsze badanie funkcjonowania certyfikatów SSL wykazało, że spośród **1428** e-sklepów jedynie **14%** automatycznie przekierowuje użytkowników na protokół https:// w najbardziej newralgicznych punktach internetowej transmisji danych. Zalicza się do nich zarówno stronę logowania, jak również rejestracji oraz składania zamówienia. Takie certyfikaty uznaje się za **w pełni sprawne**, ponieważ mechanicznie kierują klientów na szyfrowane połączenie internetowe. Pozostałe **7%** z zainstalowanych certyfikatów można uznać za niesprawne, ponieważ nie spełniają one swoich podstawowych funkcji.



Polskie e-sklepy i ich zabezpieczenia

SSL bez automatycznej zmiany protokołu na https://

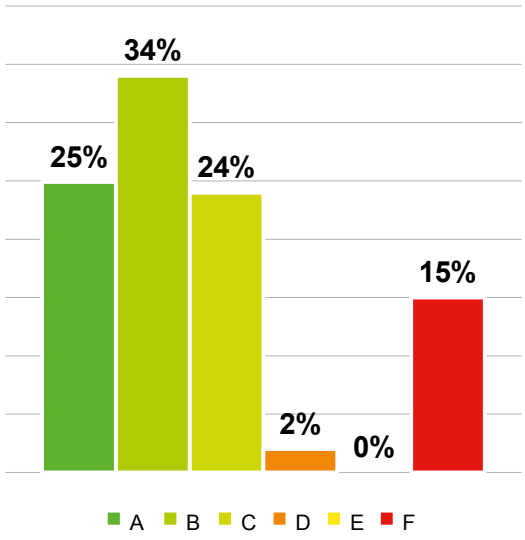
Aż **21%** e-sklepów z zainstalowanymi certyfikatami SSL (**62** z **301**) nie wprowadza automatycznego protokołu https:// na trzech najważniejszych stronach przesyłania danych: stronie logowania, rejestracji i składania zamówienia. Kolejne **11%** nie wprowadza go przynajmniej na jednej z tych stron. W sumie aż **32%** sklepów z certyfikatem SSL nie spełnia podstawowego założenia szyfrowania danych.



Zmiana protokołu http:// na https:// na stronach z zainstalowanym SSL

Ocena certyfikatów przez SSL Labs

Wszystkie certyfikaty SSL wskazane przez SSL Labs (**241**) zostały ocenione w skali od A do F. Zasady przyznawania punktów, według których system przyporządkowywał noty, zostały przedstawione w metodologii. Procentowy rozkład ocen przyznawanych przez SSL Labs przedstawia się następująco:



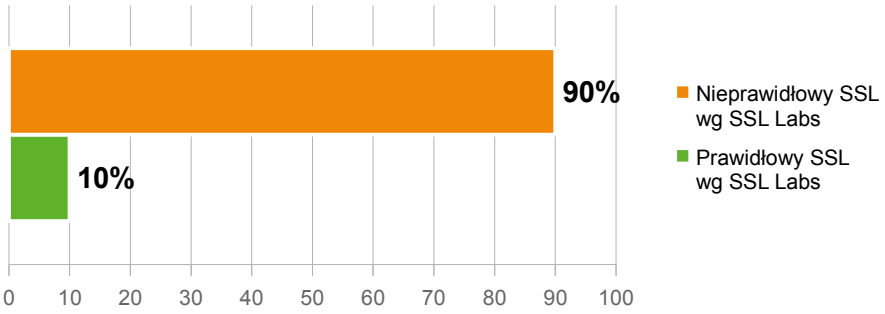
Oceny SSL Labs

Self-signed to nieuznawany certyfikat, którym firma sama stwierdza, że jest godna zaufania. Uznawane certyfikaty SSL wystawiają niezależne Urzędy Certyfikacji.

SSL Labs uznaje za prawidłowo skonfigurowane certyfikaty tylko te, które otrzymały oceny A lub B. Wynika z tego, że z certyfikatów wyszukanych przez SSL Labs **59%** (**142**) ma zainstalowany ważny i zaufany certyfikaty SSL. To jedynie **10%** w stosunku do wszystkich analizowanych sklepów. Natomiast aż **15%** certyfikatów uzyskało najgorszą ocenę F. Wlicza się w nie certyfikaty nieważne i self-signed.

Według SSL Labs z 1428 tylko 142 sklepy są bezpieczne. To jedynie 10% całości.

Zestawienie wskazań sprawnych certyfikatów SSL (z oceną A lub B) przy liczbie wszystkich przebadanych adresów wygląda następująco:



Badanie SSL Labs w liczbach

Według wyszukiwarki, jedynie **142** sklepy (z **1428**) otrzymały ocenę A lub B. Pozostałe domeny, które posiadały zainstalowany certyfikat (**99**) uzyskały niższe noty.
Aż **37** certyfikatów SSL otrzymało 0 punktów, **75** opierało szyfrowanie danych na 1024-bitowym kluczu szyfrowania (nieważnym po 31 grudnia 2010 roku), **17** straciło ważność, a **9** nie było podpisanych przez Urząd Certyfikacji.

Klucze szyfrowania

Na rynku można już spotkać certyfikaty z 4096-bitowymi kluczami szyfrowania.

W większości certyfikatów SSL wykrytych w analizowanych e-sklepach klucz szyfrowania wynosi **2048-bitów**. Co czwarty certyfikat SSL posiada **1024-bitowy** klucz szyfrowania, który z początkiem tego roku przestał być uznawany za gwarancję bezpieczeństwa. Spora liczba takich certyfikatów może wynikać z tego, że zarządzające nimi osoby nie dowiedziały się o wprowadzeniu zmian w normach bezpieczeństwa lub zakupiły wcześniej certyfikaty na dłuższy okres.
Na liście pojawiły się także certyfikaty z **4096-bitowym** kluczem szyfrowania. Jest to śladowa ilość (**1%**), jednak zadowalający jest fakt, że można już spotkać zabezpieczenia na poziomie wyższym niż obowiązujący standard 2048-bit.

Domeny.pl

Nie można samodzielnie wystawić ważnego certyfikatu SSL. Mogą to zrobić jedynie niezależne Urzędy Certyfikacji.

Informacje o firmach, ich produktach, udziale w rynku można znaleźć na https://certyfikatyssl.pl

Zaufanie do wystawcy

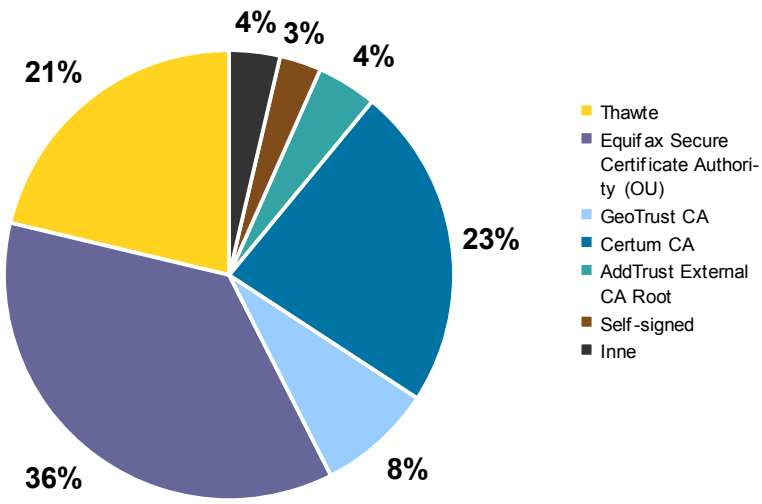
Urzędy Certyfikacji

Każdy certyfikat zawiera informację, przez jaki Urząd Certyfikacji został wystawiony.

Godne zaufania Urzędy to takie, które na podstawie wymaganych dokumentów, niezależnie potwierdzają tożsamość danej firmy lub organizacji. Wszystkie certyfikaty, które zostały wystawione subiektywnie są traktowane jako niezaufane i niezgodne z normami bezpieczeństwa. Jest to tzw. podpis self-signed, czyli przypadek, gdy organizacja lub firma sama instaluje własny certyfikat SSL. Ma on gwarantować, że firma jest godna zaufania, jednak w rzeczywistości nie jest on uznawany.

Za najczęściej wybierane i najbardziej rozpoznawane uznaje się urzędy wystawiające certyfikaty takich marek jak: VeriSign, Comodo, GeoTrust, Thawte i GlobalSign. Jednak nie tylko one mogą zapewniać bezpieczeństwo danych przysyłanych on-line.

Które Urzędy Certyfikacji wybierały badane e-sklepy?



Najpopularniejsi wystawcy SSL

Z powyższych danych wynika, że wśród przebadanych sklepów najwięcej korzysta z certyfikatów wystawionych przez Equifax Secure Certificate Authority (OU) – jest to **36%** całości. Na drugim miejscu znalazło się Powszechne Centrum Autoryzacji CERTUM z Polski (**23%**), na trzecim - Thawte z RPA (**21%**). **3%** stanowiły nieważne certyfikaty self-signed.

Domeny.pl

Znaki bezpieczeństwa

Wiarygodność znaków bezpieczeństwa umieszczonych na stronach sklepów

6% badanych e-sklepów posiada znaki bezpieczeństwa, mimo braku jakichkolwiek zabezpieczeń przesyłania danych.

Zapewnienie bezpieczeństwa przesyłanych danych to nie tylko szansa uniknięcia ich kradzieży oraz wysokich kosztów z nią związanych, ale także budowanie długotrwałych, opartych na zaufaniu, relacji z klientami.

Sklepy internetowe nie mają prawnego obowiązku instalowania zabezpieczeń szyfrowania danych. Powinny jednak na swojej stronie poinformować klienta, jeżeli przesyłane przez niego **dane nie są chronione szyfrowanym** połączeniem. W praktyce nikt nie umieszcza takich informacji. Zdarzają się także sytuacje, gdy na stronach głównych znajdują się symbole bezpiecznych połączeń internetowych, mimo że strona nie obsługuje tego typu zabezpieczeń.

Jedynie sprawny certyfikat SSL i automatyczna zmiana protokołu na https:// gwarantuje bezpieczny transfer danych.

Wśród analizowanych sklepów **6%** (92 z 1428) **posiada znaki bezpieczeństwa na swoich stronach głównych, pomimo braku jakichkolwiek zabezpieczeń przesyłania danych**. Stosowanie najprostszego symbolu kłódki przy polach do logowania lub rejestracji wyraźnie sugeruje, że procedury te są bezpieczne, a jednocześnie **jawnie wprowadza w błąd**. Dane przesyłane na takiej witrynie nie są szyfrowane i mogą wpaść w niepowołane ręce.

Ponad **62%** (187 z 301) sklepów z zainstalowanym certyfikatem SSL nie posiada znaków bezpieczeństwa na swoich stronach. Umieszczenie takiego znaku byłoby sygnałem dla klientów, że ich dane są całkowicie bezpieczne i mogą spokojnie dokonywać zakupów.

W analizie tego czynnika nie były brane pod uwagę systemy płatności, często wykorzystywane przez serwisy e-commerce. Takie systemy szyfrują jedynie moment płatności, a nie wszystkie przesyłane dane, w związku z tym nie stanowiły w badaniu miernika poziomu bezpieczeństwa.

Domeny.pl

Obraz polskiego e-commerce

Tylko mały procent przebadanych sklepów posiada zainstalowany certyfikat SSL, który poprawnie chroni przesyłane dane.

Polski rynek e-commerce wciąż się rozwija, zyskując nowych konsumentów i oferując im coraz szerszy wachlarz produktów. Równocześnie pojawia się więcej cyberataków. Ich efektem są liczne kradzieże danych, co wymaga od przedsiębiorców prowadzących działalność w Internecie stosowania kolejnych, mocniejszych zabezpieczeń. Nie jest to jeszcze normą w tym rozwijającym się sektorze polskiego rynku. **Przedstawione w raporcie dane są niepokojące - tylko mały procent przebadanych sklepów posiada zainstalowany certyfikat SSL, który poprawnie chroni przesyłane dane.**

E-sklepy - branże i bezpieczeństwo

Wszystkie sklepy biorące udział w badaniu podzieliliśmy według branż, aby sprawdzić, czy poziom e-bezpieczeństwa może wynikać z profilu działalności.

Sport, turystyka, rekreacja sprzęt fitness, wyposażenie siłowni, podstawowe akcesoria sportowe, biura podróży, bazy noclegowe	**Elektronika i AGD** RTV i AGD, komputery, fotografia	**Kultura i rozrywka** literatura, film, muzyka, multimedia
Dom i ogród meble, wnętrza, drewno, ogród	**Zdrowie i uroda** kosmetyki, perfumy, leki	**Moda** odzież, obuwie, biżuteria
Hobby filatelistyka, instrumenty muzyczne, izoteryka, astronomia, gotowanie itp.	**Zoologia** akcesoria, bezpieczeństwo, higiena, zdrowie zwierząt	**Inne** artykuły i usługi niestandardowe (tatuaże, winiarnie, dekoracyjne wyroby artystyczne itp.)
Art. dziecięce meble, odzież, higiena, bezpieczeństwo, zabawki dla dzieci	**Motoryzacja** części zamienne, akcesoria samochodowe, usługi, serwis	**Sklepy wielobranżowe** mieszany asortyment, supermarkety internetowe
Sklepy specjalistyczne maszyny, wyposażenie specjalistyczne, materiały budowlane, zabezpieczenia, materiały chłodnicze, grzewcze i sanitarne, chemia przemysłowa, oświetlenie		

Podział poszczególnych kategorii

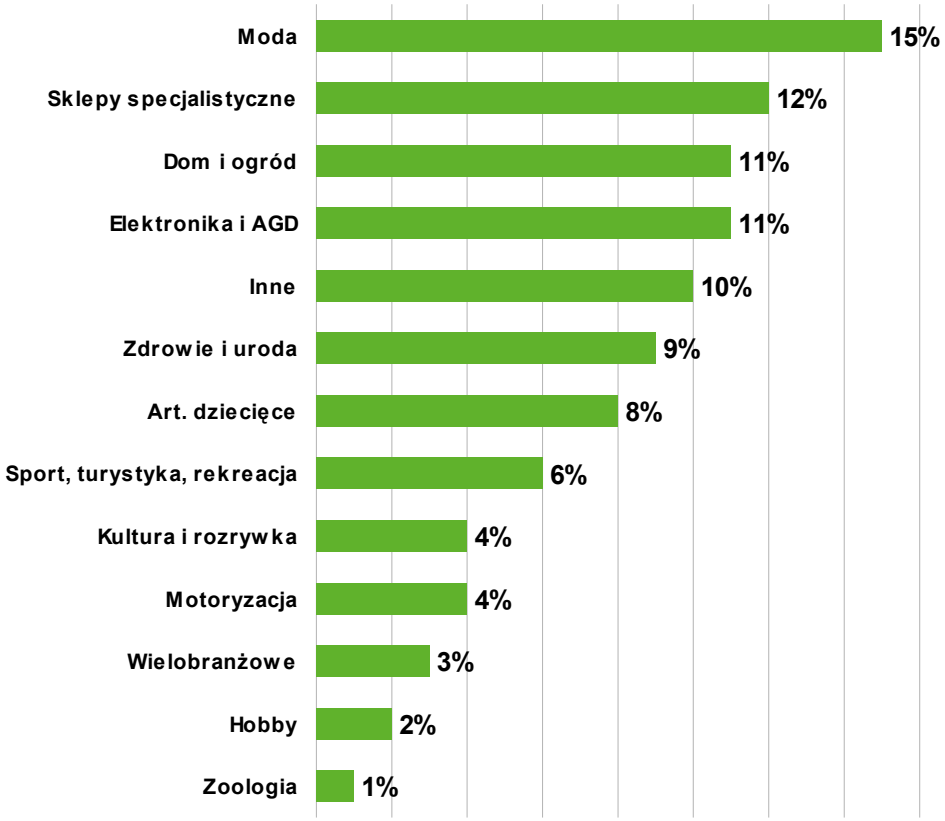
Domeny.pl

Najwięcej polskich sklepów internetowych oferuje produkty związane z modą.

Najpopularniejsze branże

Wśród **1428** przebadanych serwisów e-commerce najwięcej sklepów oferuje produkty związane z modą - **15%**. Sklepy specjalistyczne stanowią prawie **12%** całości. Niewiele mniej sklepów zajmuje się sprzedażą elektroniki i AGD – **11%.**

Najrzadziej występują sklepy prowadzące sprzedaż artykułów zoologicznych i hobbystycznych.



Najpopularniejsze branże

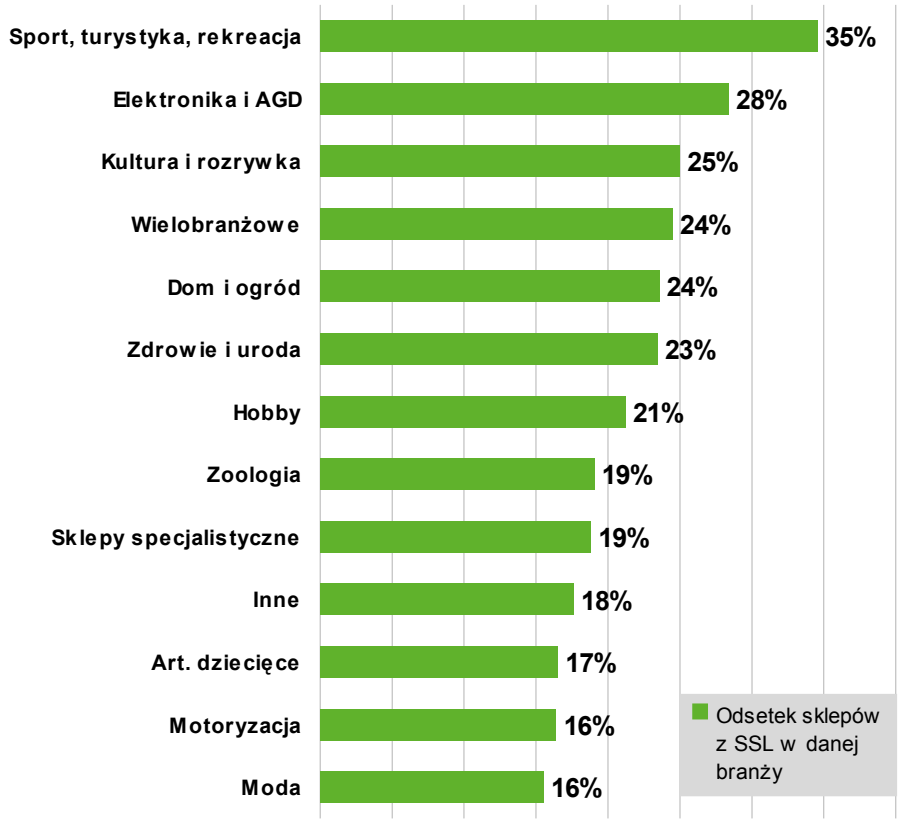
Najwyższym poziomem bezpieczeństwa odznacza się branża Sport, turystyka, rekreacja.

Okazało się, że sklepy z modą są najrzadziej chronione.

Najbezpieczniejsze branże

Aby wskazać najbezpieczniejsze branże, należało wziąć pod uwagę ile serwisów z danej kategorii posiada certyfikat SSL w stosunku do wszystkich sklepów danego profilu.

Najwyższym poziomem bezpieczeństwa odznacza się branża Sport, turystyka, rekreacja. **35%** sklepów z tej kategorii posiada zainstalowany certyfikat SSL. Na drugim miejscu znajduje się Elektronika i AGD (**28%**). Trzecie miejsce zajmuje Kultura i rozrywka. Co czwarty sklep o tej specjalizacji zapewnia szyfrowanie przesyłanych danych.



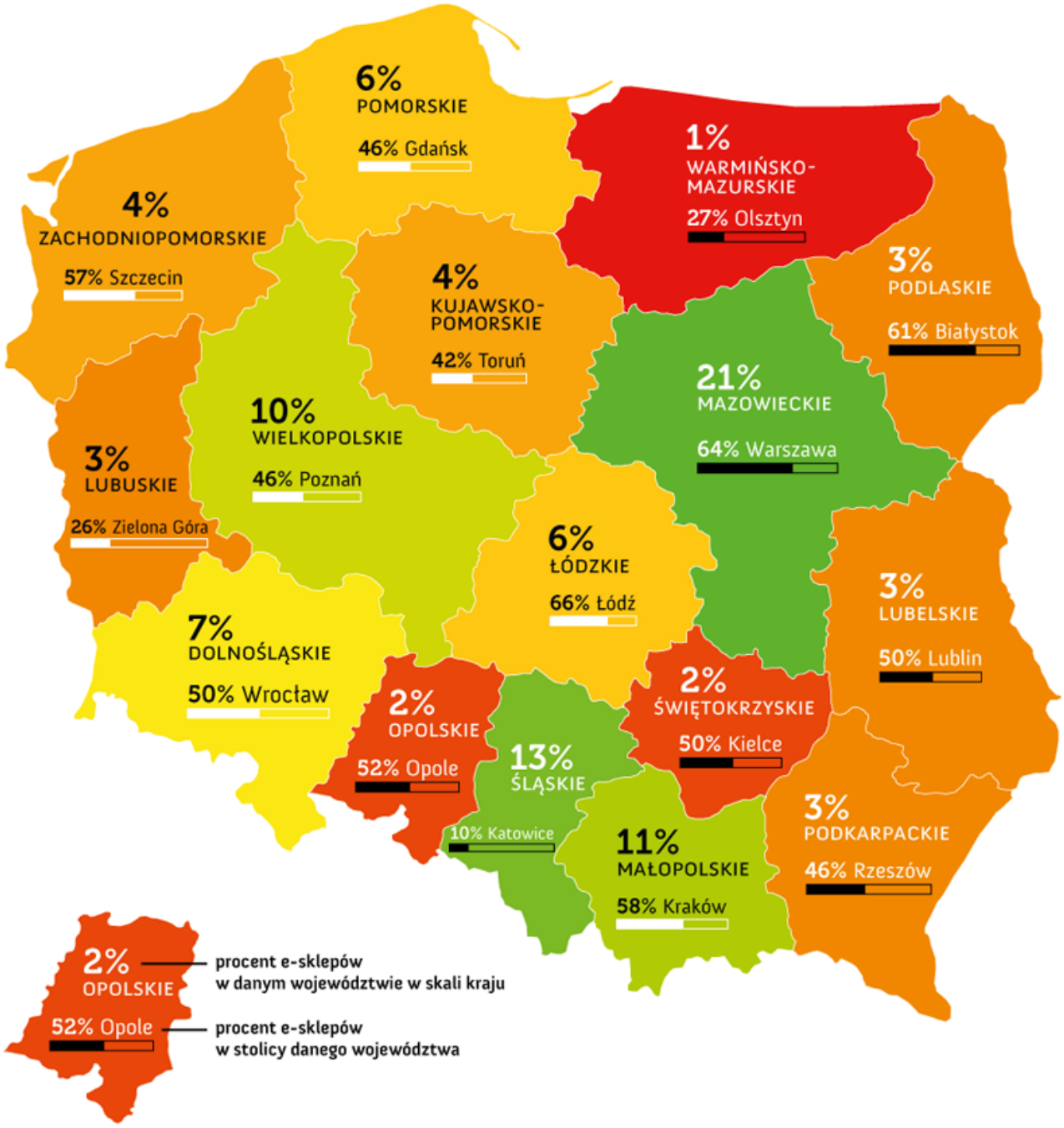
Najbezpieczniejsze branże

Najmniej bezpieczne okazały się e-sklepy oferujące produkty związane z modą, motoryzacją oraz artykułami dziecięcymi. Jedynie **16-17%** w każdej z tych grup ma zainstalowany certyfikat SSL.

Mapa polskiego e-commerce

Działalność polskich sklepów internetowych jest rozproszona po całym kraju. Poza województwem mazowieckim, w którym funkcjonuje co piąty e-sklep, ciężko jest wskazać regiony z silnie rozwiniętym rynkiem e-commerce. Świadczy to o tym, że proces regionalizacji w tym segmencie polskiego rynku jest słaby. W województwie śląskim, które zajmuje drugą pozycję, działa **13%** sklepów, w małopolskim **11%**, a w wielkopolskim **10%**. Różnice pomiędzy nimi nie są duże, co przy braku bliskości przestrzennej potwierdza fakt znikomej regionalizacji.

Z prezentacji danych na poniższej mapie wynika, że e-commerce jest słabiej rozwinięty w województwach sąsiadujących z granicami kraju na wschodzie, północy i zachodzie. Najmniej sklepów występuje w województwach: warmińsko-mazurskim, świętokrzyskim i opolskim.

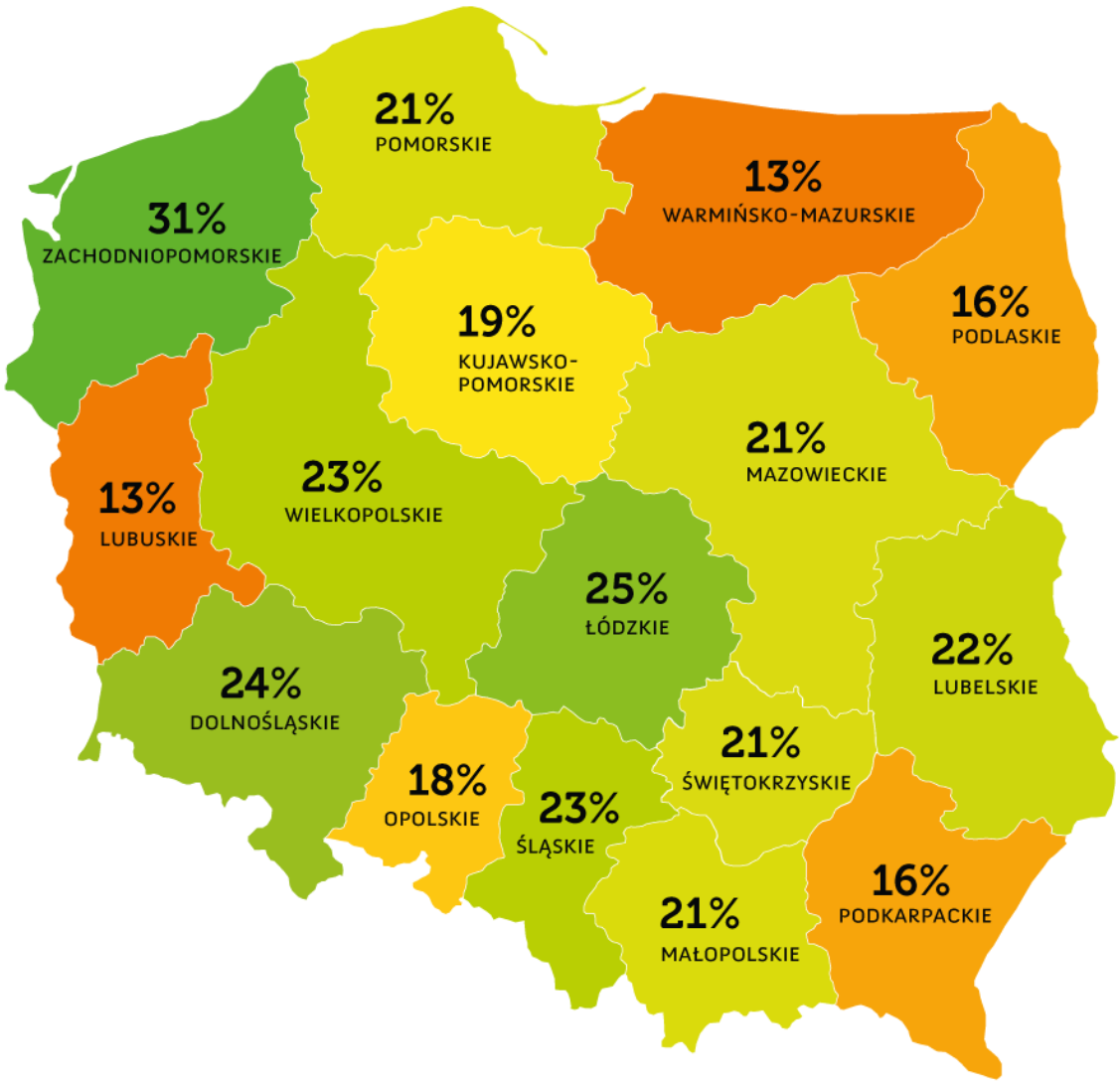


Sklepy internetowe w województwach i ich stolicach

Działalność e-commerce nie jest skupiona wyłącznie w dużych miastach. Tylko w sześciu województwach ponad połowa sklepów internetowych funkcjonuje w ich stolicy. W pozostałych województwach liczba ta jest mniejsza. Coraz łatwiejszy dostęp do Internetu wpływa na powstawanie nowych serwisów e-commerce, zwłaszcza w niewielkich miejscowościach, w których możliwości zatrudnienia są ograniczone.

Zebrane dane pozwoliły także na zbadanie poziomu bezpieczeństwa sklepów internetowych w województwach. Wyniki uzyskano na podstawie stosunku e-sklepów z SSL z danego województwa do wszystkich e-sklepów w tym regionie.

Najbezpieczniejszym województwem jest zachodniopomorskie, w którym prawie 31% sklepów posiada zainstalowany certyfikat SSL. Kolejne pozycje zajmują łódzkie i dolnośląskie.



Najbezpieczniejsze województwa

Najmniejsze prawdopodobieństwo zakupów w sklepie z zainstalowanym certyfikatem SSL występuje w województwach lubuskim i warmińsko-mazurskim. To właśnie tam odnotowano **najniższy poziom bezpieczeństwa**, ponieważ serwisy szyfrujące przesyłane dane stanowią jedynie po **13%** wszystkich sklepów internetowych w tych województwach.

Domeny.pl

Podsumowanie

Polski rynek e-commerce rozwija się w szybkim tempie. Wzrasta liczba sklepów internetowych, pojawiają się nowe formy sprzedaży, a sprzedawcy oferują szerszy asortyment i często lepsze ceny niż w tradycyjnych sklepach. Popularność e-zakupów wynika także z ich wygody – można porównać oferty kilkudziesięciu różnych sklepów bez wychodzenia z domu.

Polscy internauci wydają on-line coraz więcej i deklarują, że kwoty te wzrosną w 2011 roku. **Rosnąca liczba użytkowników korzystających z e-sklepów oraz realizowanych transakcji czyni ten sektor rynku idealnym celem dla cyberprzestępców.**

Wraz z rozwojem polskiego rynku e-commerce wzrasta liczba kradzieży danych on-line.

Z wielu badań przeprowadzonych w ostatnich latach wynika, że internauci nie czują się bezpiecznie w Internecie i obawiają się kradzieży swoich danych. Zeszłoroczne ataki cyberprzestępców na największe światowe koncerny wywołały liczne **dyskusje na temat bezpieczeństwa internetowego**. W ówczesnej debacie publicznej została poruszona także tematyka bezpieczeństwa **zwykłych** użytkowników Internetu. Przy tej okazji pojawiły się publikacje i poradniki, które zapewne zwróciły uwagę wielu internautów i zachęciły ich do podjęcia prostych działań - np. aktualizacji systemu i oprogramowania antywirusowego, rozsądnego korzystania z sieciowych zasobów czy przeglądania tylko zaufanych stron. Są to ogólnie przyjęte zasady bezpiecznego użytkowania Internetu.

Tylko od nas zależy czy będziemy chronić swoje dane i na jakiej stronie je udostępnimy.

Jednak w przypadku sklepów internetowych, klient nie jest w stanie samodzielnie zapewnić sobie bezpieczeństwa. Głównie odpowiada za nie **właściciel**. To na nim spoczywa obowiązek dostarczenia narzędzi służących ochronie danych użytkowników. Odpowiednie zabezpieczenia nie tylko pozwalają uniknąć coraz częstszych i kosztownych w skutkach ataków działań hakerów, ale także wpływają na wzrost zaufania klientów do danego sklepu internetowego.

Przeprowadzone przez nas badanie pokazuje, że znaczna cześć polskich sklepów internetowych nie chroni danych swoich klientów. Wśród **1428** sklepów jedynie **301** szyfrowało transmisję danych certyfikatami SSL. To zaledwie **21%**.

Niewielkie zainteresowanie bezpieczeństwem e-biznesu może tłumaczyć klika podstawowych czynników

Jako jedną z głównych przyczyn należy wymienić niską świadomość zagrożeń w Internecie. Wielu właścicieli e-sklepów posiada podstawową wiedzę na temat narzędzi internetowych. Pozwala im to na sprawne

poruszanie się w wirtualnym świecie, jednak nie daje wyobrażenia o skali potencjalnych zagrożeń. Ponadto, wielu z nich jest zdania, że nie dotyczą ich negatywne wydarzenia, o których dowiadują się z mediów. W ten sposób nieświadomie **pozostają bierni na czynniki zewnętrzne** i nie oddziałują na rozwój swojej działalności. Sklepy, które nie padły ofiarą cyberprzestępców, traktują inwestycje w bezpieczeństwo jako dodatkowy element prowadzenia swojego biznesu. Często odwlekają zakup zabezpieczeń na ostatnią chwilę. To błędne założenie powoduje, że straty poniesione w wyniku działań hakerów mogą być znacznie większe – np. bezpowrotne zniszczenie reputacji sklepu.

Najbardziej narażone na cyberataki są serwisy z przesyłaniem danych osobowych oraz z dokonywaniem transakcji finansowych.

Oczywiście brak świadomości zagrożeń nie leży po jednej stronie – dzielą ją klienci i właściciele serwisów. Korzystanie z niezabezpieczonych e-sklepów jest częściowym przyzwoleniem na ich dalsze funkcjonowanie i nie prowadzi do wdrażania ulepszeń. Należy pamiętać, że to właściciele są odpowiedzialni za **poziom standardów działalności on-line**. Nie można zrównać nieumyślnego narażania użytkowników strony www na utratę danych ze świadomym oszczędzaniem na bezpieczeństwie. Jednak brak odpowiedniej wiedzy nie jest wystarczającym usprawiedliwieniem. Sprzeciw klientów wobec braku ochrony danych może przybrać formę dokonywania zakupów jedynie w bezpiecznych serwisach.

Zorientowany użytkownik ma świadomość, że sam **program antywirusowy zainstalowany na komputerze nie zapewni 100% ochrony podczas e-zakupów**. Dlatego ważne jest, aby właściciele serwisów wiedzieli i pamiętali o ochronie swoich sklepów. Ma to szczególne znaczenie w serwisach z przesyłaniem danych osobowych oraz dokonywaniem transakcji finansowych. Te informacje są najbardziej pożądane przez cyberprzestępców. Za ich bezpieczeństwo odpowiada właściciel. Jednak, jak pokazuje raport, niewielu z nich wywiązuje się z tej powinności.

Narzędzia do ochrony przesyłania danych on-line są łatwo dostępne i nie wymagają dużych nakładów finansowych. Dodatkowo są przyjazne dla internautów, ponieważ każdy może szybko sprawdzić czy dana strona www jest bezpieczna.

Na niewielkie zainteresowanie e-bezpieczeństwem wpływ ma również niski poziom wiedzy o technologiach oraz narzędziach do ochrony serwisów internetowych i przesyłanych danych. Nie każdy wie, że są ogólnodostępne i nie wymagają nakładu dużych środków finansowych.

Rozwój cyberprzestępczości powinien motywować odpowiednie instytucje, media, a także firmy oferujące produkty związane z bezpieczeństwem on-line do edukowania internautów (a zwłaszcza przedsiębiorców) w tym zakresie.

Mamy nadzieję, że konkursy, badania i analizy o tematyce e-bezpieczeństwa będą dla właścicieli sklepów internetowych źródłem wiedzy o prowadzeniu działalności, a dla użytkowników - przewodnikiem po rozsądnym korzystaniu z Internetu.

COPYRIGHT © 2011 CertyfikatySSL.pl, serwis należy do firmy Domeny.pl sp. z o.o.