



GIEŁDA NA ZIELONO

Czyli jak polskie spółki giełdowe dbają o bezpieczeństwo danych swoich klientów w Internecie.

Patron medialny



Patron merytoryczny



Spis treści

Wstęp	4
1. O badaniach	5
2. Przedmiot badań	5
3. Wyniki badań	7
3.1 Posiadanie certyfikatów SSL	7
3.2 Jakie rodzaje certyfikatów są stosowane przez spółki giełdowe?	9
4. Podsumowanie	11
O realizatorze badania	14
O patronie medialnym	14

Wstęp

Zapewnianie bezpieczeństwa to nie tylko ochrona danych. To również świadome kształtowanie pozytywnego wizerunku i prestiżu w środowisku biznesowym. Choć zagrożenie w postaci ataków hakerskich i ustawowe wymogi ochrony danych osobowych przemawiają za wprowadzeniem skutecznej ochrony serwisów internetowych, dopiero potrzeba zwiększania zaufania i pielęgnowania relacji z potencjalnymi klientami i partnerami stanowi argument decydujący.



Otwarta komunikacja w internecie i gwarancja bezpiecznej wymiany danych to aspekty szczególnie ważne w kontekście spółek stawiających na przejrzystość i wiarygodność prowadzonego biznesu. Firmy notowane na giełdzie powinny być w tej kwestii wyznacznikiem jakości dla całości rynku. W związku z tym zdecydowaliśmy się sprawdzić, jak polskie spółki giełdowe dbają o bezpieczeństwo prowadzonych serwisów internetowych. Raport „Giełda na zielono” zawiera wyniki przeprowadzonych badań wraz z podsumowaniem kondycji witryn spółek giełdowych w odniesieniu do poziomu ich zabezpieczenia. Nazwa raportu nawiązuje do zielonego paska adresu, który wyświetlany jest przy zastosowaniu certyfikatu SSL typu EV, zapewniającego najwyższy poziom zabezpieczenia strony.

Tomasz Litarowicz

Dyrektor CERTUM Powszechnego Centrum Certyfikacji

1. O badaniach

Badania zostały przeprowadzone w sierpniu 2012 r. na grupie 440 serwisów internetowych podmiotów notowanych na Giełdzie Papierów Wartościowych w Warszawie [GPW]. **Spółki akcyjne badane były pod kątem zabezpieczania danych przesyłanych przy wypełnianiu formularza kontaktowego, logowaniu do systemu oraz przesyłaniu danych z prośbą o newsletter.** Za realizację badań odpowiada Unizeto Technologies – właściciel CERTUM, pierwszego polskiego centrum certyfikacji.

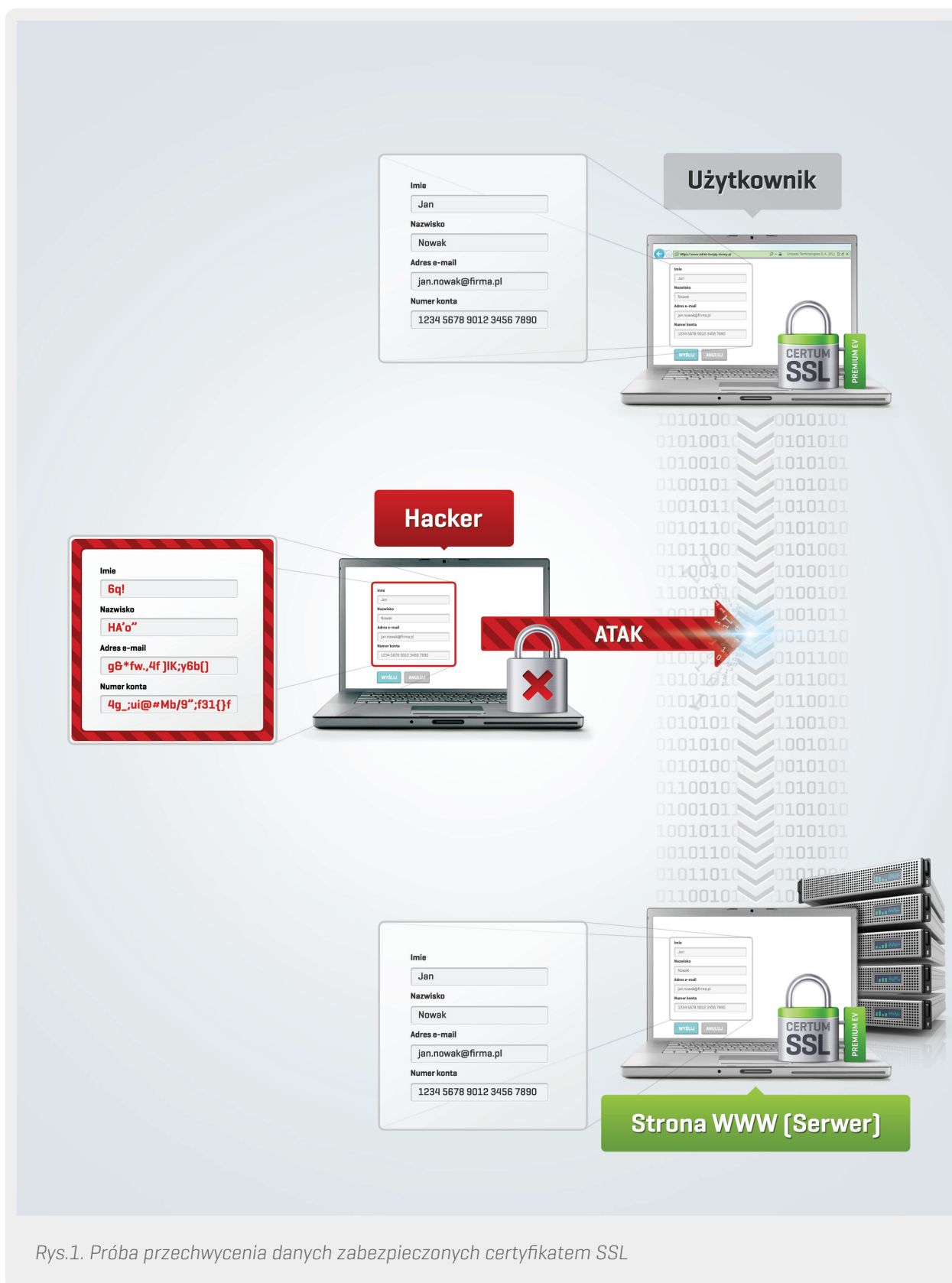
Celem badań było zweryfikowanie stanu zabezpieczeń stron internetowych polskich spółek giełdowych, które ze względu na osobowość prawną i specyficzny charakter zobligowane są do zapewnienia i właściwego koordynowania otwartej i aktywnej komunikacji z rynkiem. Wyniki analizy serwisów zostały zebrane i opracowane, a następnie opublikowane w postaci niniejszego raportu.

2. Przedmiot badań

Głównym przedmiotem przeprowadzonych badań były certyfikaty SSL, zainstalowane na stronach spółek giełdowych. Zostały one wybrane z uwagi na fakt, że jest to podstawowy, najprostszy i najpewniejszy sposób weryfikacji danej witryny. Zgodnie z Ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 r., administrator witryny internetowej, na której zbierane są dane osobowe, ma obowiązek zabezpieczenia ich przed nieuprawnionym dostępem. W wymóg ten idealnie wpisują się certyfikaty szyfrujące.

Z uwagi na wysoką wiarygodność i możliwość dostosowania rozwiązania do charakteru działalności, certyfikaty SSL stosowane są przez wszystkie podmioty dbające o bezpieczeństwo swych klientów – bez względu na wielkość firmy, bogactwo oferty czy liczbę dokonywanych przez nią transakcji.

Istotą działania certyfikatu SSL jest stosowanie szyfrowanego połączenia w komunikacji między komputerami. Łącząc się z witryną, użytkownik jest w stanie natychmiastowo zweryfikować jej bezpieczeństwo i podjąć decyzję dotyczącą wprowadzania danych w jej obszarze. Przy zainstalowanym certyfikacie SSL w pasku przeglądarki widoczny jest skrót HTTPS zamiast standardowego HTTP. Ponadto, w zależności od używanej przeglądarki oraz rodzaju certyfikatu – w pasku adresu strony pojawia się ikonka kłódki, a sam pasek może zmieniać kolor na zielony, żółty i niebieski.

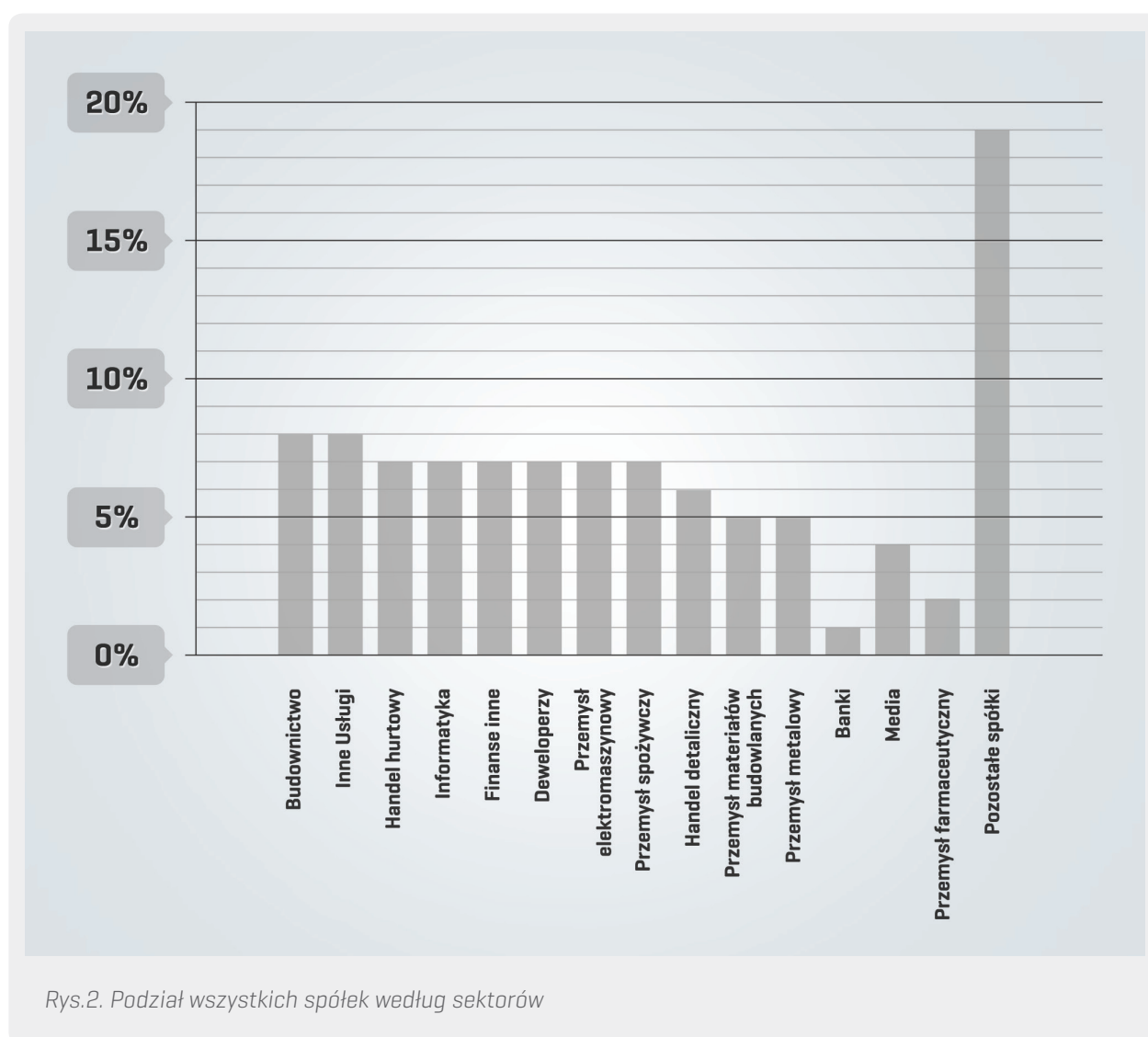


Rys.1. Próba przechwycenia danych zabezpieczonych certyfikatem SSL

3. Wyniki badań

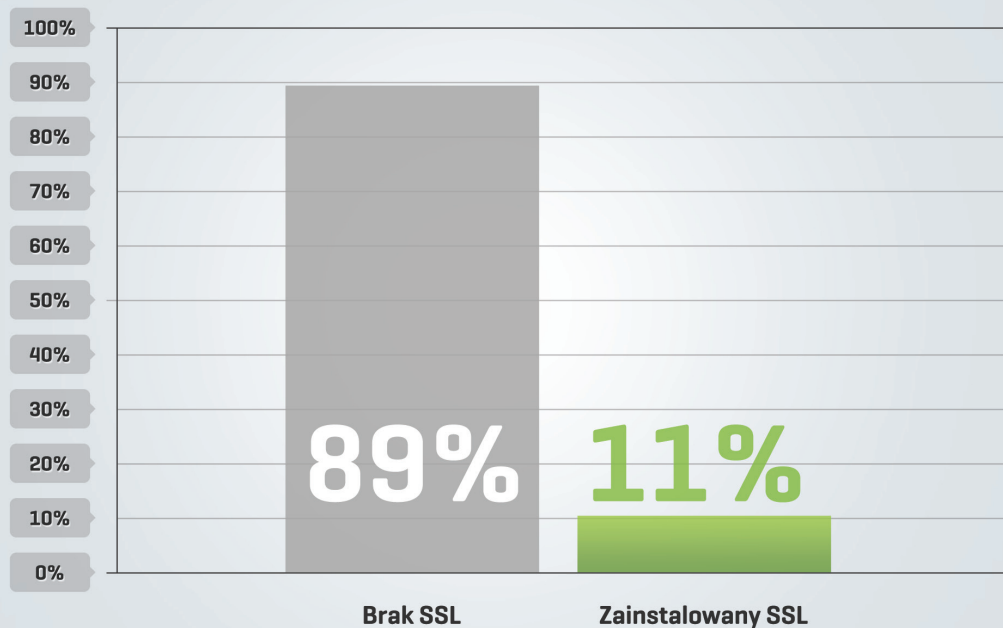
3.1 Posiadanie certyfikatów SSL

Na potrzeby niniejszego raportu została przeprowadzona manualna weryfikacja wybranych 440 serwisów internetowych spółek giełdowych. Największą reprezentację miały w badaniu sektory: budownictwa, handlowy, informatyczny oraz finansowy. Badanie miało na celu weryfikację zainstalowanego certyfikatu SSL, który broni przed nieuczciwymi próbami przejęcia informacji podawanych za pośrednictwem witryny przedsiębiorstwa.



Analizując zgromadzone dane okazało się, że jedynie co dziewiąta badana spółka giełdowa [28] posiada zainstalowany certyfikat SSL. Możemy zatem stwierdzić, iż jedynie 11% spółek giełdowych dba właściwie o bezpieczeństwo swoich użytkowników, wzmacnia wiarygodność strony WWW i świadomie buduje zaufanie otoczenia. Wśród tych 11% znajdują się głównie spółki z sektora finansowego, dla których kwestie bezpieczeństwa wpisane są w profil działania. Przedsiębiorcy pamiętać muszą, że niezależnie od tego, czy administrują stroną internetową dużej instytucji finansowej czy niewielkiej firmy ubezpieczeniowej, zobowiązani są oni realizować ustawowy obowiązek ochrony danych osobowych użytkowników [Dz. U. z 2002 Nr 101, poz 926, ze zm.]. Budowanie bezpiecznej marki jest procesem ciągłym, którego przebieg powinien być stale weryfikowany, a działania dostosowywane do coraz to nowych zagrożeń. Każdy, komu zależy na dobrych relacjach z odwiedzającymi, powinien przede wszystkim zadbać o to, by czuli się w jego witrynie bezpiecznie. Raz stracone zaufanie klienta jest później bardzo trudno odbudować.

Tylko **co dziewiąta** badana spółka giełdowa **dawała gwarancję bezpieczeństwa** przesyłania danych.



Rys.3. Próba przechwycenia danych zabezpieczonych certyfikatem SSL

3.2 Jakie rodzaje certyfikatów są stosowane przez spółki giełdowe?

W zależności od typu prowadzonej działalności, poziomu zabezpieczeń i stopnia weryfikacji wyróżnić możemy trzy rodzaje certyfikatów SSL, które różnią się następującymi danymi zawartymi w certyfikacie:

- ✓ nazwa domeny w certyfikacie [DV],
- ✓ nazwa domeny i organizacji w certyfikacie [OV],
- ✓ nazwa domeny i organizacji w certyfikacie + zielony pasek adresu + nazwa firmy oraz nazwa wystawcy certyfikatu [EV] w pasku adresu strony www.

W przebadanych spółkach giełdowych aż 58% certyfikatów SSL to rozwiązania klasy EV. Są to certyfikaty SSL o najwyższym poziomie zabezpieczeń, przy których tożsamość nabywcy sprawdzana jest podczas kilkietapowej weryfikacji. Spółka giełdowa posiadająca taki certyfikat przeszła pozytywnie skrupulatną kontrolę adresu e-mail, dostępu do domeny, tożsamości, umowy i wniosku. Dzięki temu firma stała się posiadaczem prestiżowego „zielonego paska adresowego”, który według badań Tec-Ed Survey jest zauważany przez 100% użytkowników. Nasze badanie potwierdziło ogólnie przyjęte założenie, iż certyfikaty tej klasy są wybierane głównie przez instytucje finansowe.

75% posiadaczy certyfikatów typu EV, czyli o najwyższym poziomie zabezpieczeń, to banki. Do pozostałej części badanych należą firmy z branży ubezpieczeniowej, handlowej i telekomunikacyjnej. Klienci tych spółek mogą być całkowicie pewni najwyższego poziomu ochrony i bezpieczeństwa ich danych.

Zalety certyfikatów SSL EV:

- ✓ spełnienie ustawowego obowiązku ochrony danych osobowych,
- ✓ najwyższy poziom ochrony przesyłanych danych,
- ✓ zaufanie ze strony klientów, które przekłada się na transakcje,
- ✓ prestiż i wizerunek zaufanej witryny.

Na równoważnym drugim miejscu znalazły się certyfikaty typu OV oraz DV [po 21%].

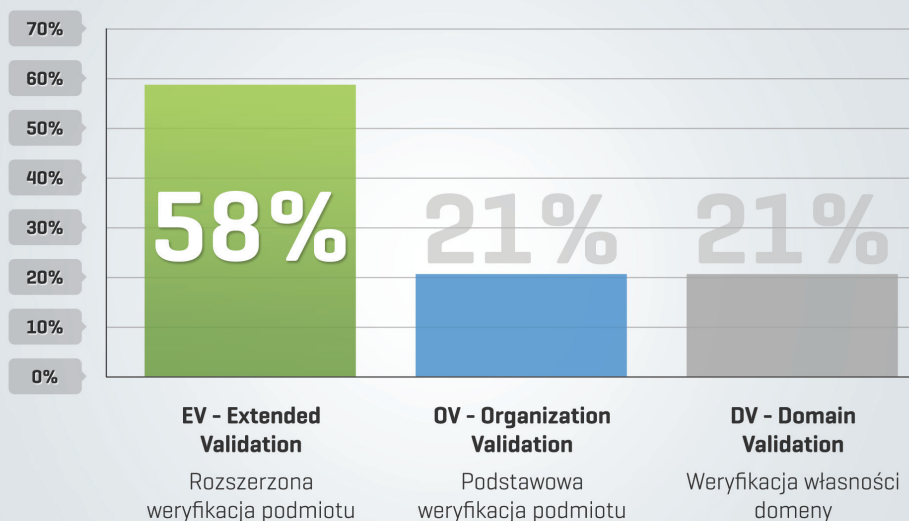
Spółka posiadająca certyfikat typu OV zapewnia wysoki poziom zabezpieczeń swoim użytkownikom. W celu otrzymania tego certyfikatu musiała przejść zarówno weryfikację swojej tożsamości, jak i dostępu do domeny. Według naszego badania certyfikaty typu OV wybrały branże: ubezpieczeniowa, budowlana, telekomunikacyjna oraz multimedialna.

Certyfikat typu DV, zapewniający podstawowy poziom zabezpieczeń, posiadają branże: deweloperska, informatyczna, handlowa oraz energetyczna. Spółki te w celu wydania certyfikatu DV potwierdziły jedynie prawo własności do danej domeny lub adresu IP. Oznacza to, że klienci tych spółek nie widzą w wyświetlanym certyfikacie takich danych, jak nazwa organizacji czy firmy.

Najlepiej zabezpieczoną spółką giełdową okazał się jeden z banków, który chroni dane najwyższym certyfikatem SSL typu EV na wszystkich stronach.

Na podstawie badań zauważono, iż spółki akcyjne zabezpieczają głównie strony logowania, nie zwracając uwagi na dane przesyłane przez swoich klientów w formularzach kontaktowych. **Oznacza to, iż informacje przesyłane przez klienta, takie jak imię, nazwisko czy adres email, są łatwym łupem do przechwycenia.**

Aż 58% certyfikatów SSL zainstalowanych w serwisach internetowych spółek giełdowych **to certyfikaty najwyższej klasy EV**, wyświetlające zielony pasek adresu w przeglądarce.



Rys.4. Procentowy udział poszczególnych certyfikatów SSL wg. sposobu weryfikacji w przebadanych spółkach giełdowych

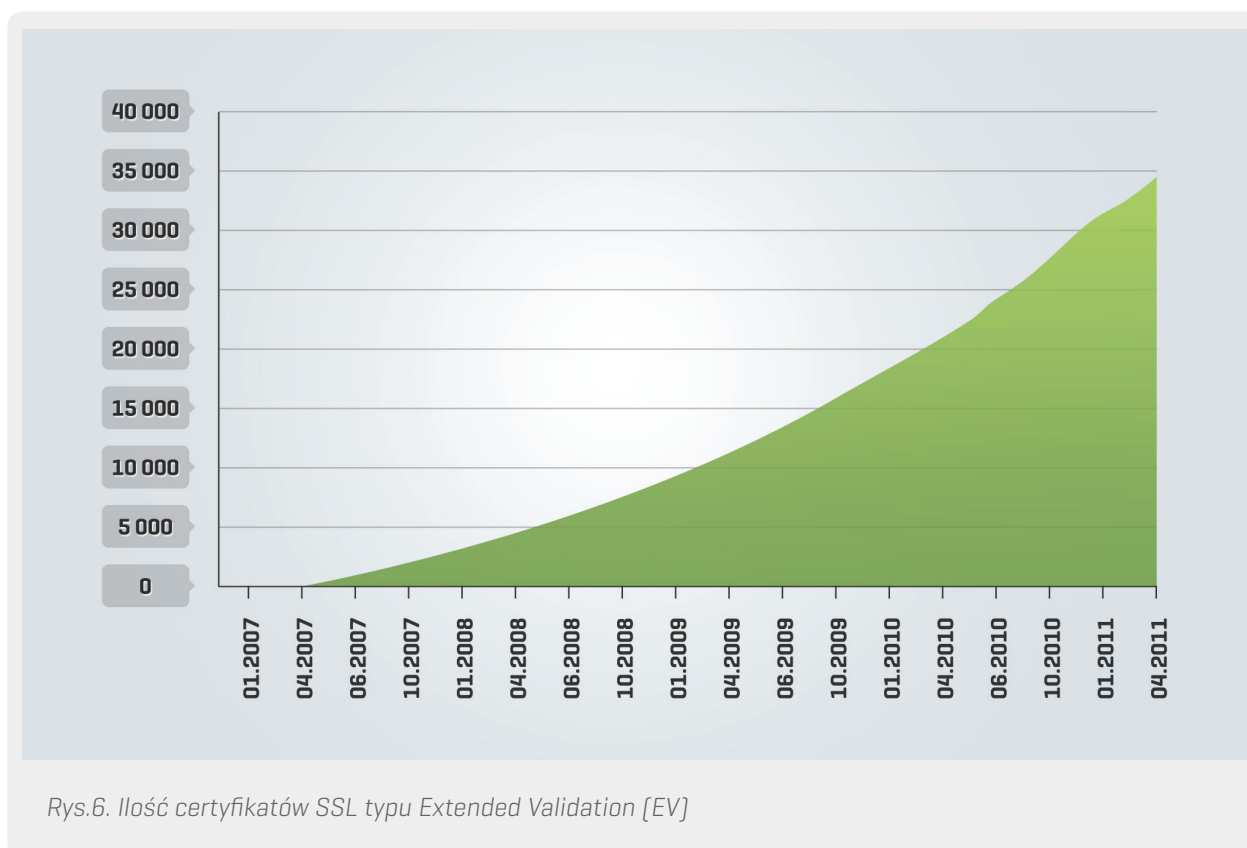
Podsumowanie

Przeprowadzone badania uwypukliły wciąż niską świadomość zagrożeń związanych z przesyłaniem danych w Internecie. Jedynie 11% polskich spółek giełdowych, które powinny chronić przetwarzane dane osobowe, posiada zainstalowany certyfikat SSL. Świadczy to o zbyt niskim przywiązaniu do kwestii ochrony danych swoich i klientów oraz o znikomej świadomości co do wymiaru wizerunkowego stosowania narzędzi zabezpieczających.

Z drugiej strony, uwidacznia się pozytywny trend wśród spółek, które zainwestowały odpowiednie zabezpieczenia. Większość z nich zdecydowała się na najwyższy poziom ochrony, jaki zapewniają certyfikaty SSL typu EV. Jest to nie tylko sposób na zapewnienie bezpieczeństwa i wywiązanie się z ustawowego obowiązku ochrony danych osobowych, ale też pomysł na wyróżnienie się na tle konkurencji i sposób zdobycia zaufania wśród klientów. Zielony pasek adresu, na jaki pozwalają wyłącznie certyfikaty SSL typu EV, jest jasnym i zrozumiałym znakiem, że dane są odpowiednio zabezpieczone, a użytkownik ma do czynienia z firmą stawiającą bezpieczeństwo wśród swoich priorytetów.



Popularność certyfikatów SSL EV wśród polskich spółek zabezpieczających strony WWW szyfrowanym połączeniem jest zgodna ze światowymi trendami. Obecnie prawie 1/3 certyfikatów SSL wybieranych przez największe serwisy internetowe na świecie [TOP 1 000 stron] to zabezpieczenia typu EV. Oznacza to, że najwyższy poziom wiarygodności istotny jest również tam, gdzie przetwarzana jest duża ilość danych i narażenie ich w jakikolwiek sposób mogłoby doprowadzić administratora do ogromnych strat wizerunkowych, a co za tym idzie – finansowych. Przedsiębiorstwa, działające lokalnie, ale myślące globalnie, poddać powinny się ogólnoświatowym tendencjom, wymuszającym najwyższą dbałość o bezpieczeństwo, także w kontekście komunikacji z otoczeniem, odbywającej się za pośrednictwem firmowej witryny.





Michał Smereczyński

redaktor naczelny
WebSecurity.pl

Raport, poza podkreśleniem oczywistej konieczności dochowania dbałości o bezpieczeństwo transmisji danych między serwisami spółek giełdowych, a ich klientami, zwraca uwagę na dość niepokojące kwestie. Przede wszystkim jest to fakt, że 89% serwisów nie jest w ogóle zabezpieczonych, a co za tym idzie, wszystkie one podatne są nie tylko na przechwycenie informacji, ale także na podmianę treści, co w przypadku spółek notowanych na giełdzie może mieć tragiczne skutki.

Poważna instytucja, która chce dbać o dobro własne oraz dobro swoich klientów, powinna postępować według schematu zapewniającego bezpieczeństwo w komunikacji on-line. Na schemat ten składa się kilka dobrych praktyk, które można opisać krótko w 5. punktach.

1. Zabezpieczać serwis internetowy certyfikatem SSL o najwyższym poziomie uwierzytelnienia.
2. Zabezpieczać wszystkie elementy serwisu, które tego wymagają – nie tylko stronę logowania, ale także formularze kontaktowe i strony z dokumentami do pobrania.
3. Zabezpieczać nie tylko serwisy internetowe, ale także korespondencję elektroniczną – źle zabezpieczona usługa poczty elektronicznej jest podatna na podszywanie się pod nadawcę [tzw. spoofing].
4. Rejestrować zbiory danych osobowych w GIODO – niezależnie od tego, czy serwis gromadzi podstawowe, czy wrażliwe dane swoich klientów, wymagane jest zgłoszenie takiego zbioru do Generalnego Inspektora Ochrony Danych Osobowych.
5. Zadbać o to, aby w zespole utrzymującym i rozwijającym serwis on-line, była osoba kompetentna w kwestiach bezpieczeństwa, na której spocznie odpowiedzialność za ten aspekt działania serwisu. Praktyka pokazuje, że oszczędności na polityce bezpieczeństwa owocują stratami na poziomie



Michał Kisiel

analityk Bankier.pl

W dzisiejszych czasach witryna internetowa to coś więcej niż tylko zbiór opublikowanych w sieci informacji. Jej wygląd, funkcjonalność i zawartość budują wizerunek firmy. Korzystanie z najlepszych dostępnych rozwiązań zapewniających bezpieczeństwo komunikacji to element dbałości o relacje z rynkiem.

Klienci, partnerzy biznesowi, inwestorzy oczekują, że spółki notowane na giełdzie będą narzucać najwyższe standardy również w tej dziedzinie. Certyfikaty SSL EV pozwalają nie tylko odpowiednio zabezpieczyć cenne dane, ale stanowią także czytelny, wizualny sygnał wiarygodności. Zaufanie to podstawa każdego biznesu, a w anonimowym świecie internetu warto dbać o nie szczególnie.

0 realizatorze badania



Unizeto Technologies S.A. jest właścicielem marki CERTUM. Jako firma z branży IT działa nieprzerwanie od 1965 roku. Oferta Unizeto obejmuje produkty, usługi i rozwiązania dedykowane dla rynku administracji publicznej, ubezpieczeń społecznych, służby zdrowia, sektora biznesowego oraz klienta indywidualnego.



CERTUM - jako jedyny polski urząd certyfikacji, znajduje się nieprzerwanie od 2002 r. na liście światowych zaufanych centrów certyfikacji [CA] i posiada pieczęcie WebTrustSM/TM dla wszystkich swoich usług związanych z podpisem elektronicznym:

- ✓ pieczęć WebTrustSM/TM dla usług i certyfikatów kwalifikowanych,
- ✓ pieczęć WebTrustSM/TM dla usług i certyfikatów zwykłych [niekwalifikowanych],
- ✓ pieczęć WebTrustSM/TM Extended Validation dla certyfikatów EV SSL.

0 patronie medialnym



Bankier.pl to czołowy serwis finansowy w Polsce. Jego misją jest wskazywanie właściwej drogi w świecie finansów. Tworząc wiarygodne informacje, eksperckie analizy oraz profesjonalne narzędzia porównawcze, pomaga podjąć użytkownikom najkorzystniejsze decyzje finansowe. W portalu znaleźć można najnowsze informacje o finansach, gospodarce i biznesie, z kilkudziesięciu źródeł, a także wiele analiz i raportów przygotowanych przez ekspertów z działów Finanse osobiste, Firma i Inwestowanie.



WebSecurity.pl to największy w Polsce portal o bezpieczeństwie sieciowym. Misją WebSecurity.pl jest dzielenie się wiedzą [know-how] i umiejętnościami [how-to], publikując pomocne wskazówki, porady, kursy i tutoriale. W portalu można znaleźć także prezentacje sprzętu oraz recenzje oprogramowania. WebSecurity.pl to również baza najciekawszych i najważniejszych wydarzeń branżowych w Polsce i na świecie. WebSecurity.pl tworzą doświadczeni redaktorzy, a także specjaliści z zakresu bezpieczeństwa w sieci i blogerzy, którzy są ekspertami w takich dziedzinach, jak m.in. administrowanie systemami, aplikacje webowe czy analiza zagrożeń.

Unizeto Technologies SA

ul. Królowej Korony Polskiej 21
70-486 Szczecin

tel. +48 91 4801 201

fax +48 91 4801 220

info@unizeto.pl

Centrum Usług

ul. Bajeczna 13
71-838 Szczecin

szczecin@unizeto.pl



- Punkty Rejestracji
- Punkty Partnerskie

Warszawa

ul. Krzywickiego 34
02-078 Warszawa

tel. +48 22 5258 601

fax +48 22 5258 620

warszawa@unizeto.pl

Katowice

ul. Modelarska 12
40-142 Katowice

tel. +48 32 6069 801

fax +48 32 6069 820

katowice@unizeto.pl

Lublin

ul. Kowalska 5
20-115 Lublin

tel. +48 81 5366 901

fax +48 81 5366 920

lublin@unizeto.pl

Koszalin

ul. Morska 35
75-212 Koszalin

tel. +48 94 3419 701

fax +48 94 3419 720

koszalin@unizeto.pl



SYSTEM OBSŁUGI E-FAKTUR to:

- możliwość integracji z systemami księgowymi klienta
- cashflow - faktura trafia do klienta w dniu wystawienia (mail, SMS)
- pełna archiwizacja - konserwacja wartości dowodowej
- odpowiednik daty pewnej w wersji papierowej
- dokumenty zgodne z rozporządzeniem Ministra Finansów
- gwarantowane utrzymywanie dokumentu w formie elektronicznej przez 6 lat

WYGODA · BEZPIECZEŃSTWO · INNOWACYJNOŚĆ

Bezpłatne konsultacje: 801 540 340