TestArmy CyberForces

Zadbaj o bezpieczeństwo systemu e-commerce

czyli jak pomożemy Ci uchronić się przed atakami na najbardziej narażoną branżę świata

www.cyberforces.com

Jak przygotować się na atak cyberprzestępcy

Błędem, który często popełniają właściciele sklepów internetowych jest myślenie, że "Jestem za mały, żeby mnie zaatakować". To nieprawda. Absolutnie każdy może stać się ofiarą cyberataku. Małe firmy tak naprawdę są dużo łatwiejszym celem, ponieważ często nie mają odpowiednio rozbudowanych zabezpieczeń, a przecież przechowywane przez nie dane wciąż są wartościowe. Jak więc się zabezpieczyć?

01

Przygotuj się na najgorsze - musisz zrozumieć, że jeśli haker obierze Cię za cel, nie ukryjesz się przed nim. Gdy będzie chciał włamać się do Twoich systemów - zrobi to. To od Ciebie zależy czy będzie mu się to opłacało, a jeśli tak, to jaki wpływ na funkcjonowanie Twojego biznesu będzie miał taki incydent.

- Zabezpiecz sieci najlepiej jak to możliwe
- Nie bój się inwestować w systemy obronne i dąż do ich maksymalnej szczelności

02

Poznaj swój system bezpieczeństwa - wiedz jakie zabezpieczenia posiadasz i jak wygląda architektura sieci. Zastanów się czy dbasz o jakość bezpieczeństwa, podążasz za trendami i posiadasz najnowsze wersje oprogramowania

- Opracuj strategię bezpieczeństwa
- Przeprowadzaj regularne testy penetracyjne

03

Zabezpiecz krytyczne dane - nadaj priorytet przechowywanym przez ciebie informacjom. Te, które są niezbędne do prawidłowego funkcjonowania Twojego biznesu, muszą być szczególnie chronione.

- Używaj przynajmniej dwóch miejsc do przechowywania danych
- Zadbaj o ich odpowiednie szyfrowanie

04

Stale monitoruj sieć - wykrywaj usterki w jak najkrótszym czasie. W przypadku ataku taka kontrola może zapewnić szybkie wykrycie zmiany i umożliwić natychmiastowe podjęcie działania

- Automatyzuj bezpieczeństwo jak tylko się da
- Zainwestuj w narzędzie, które w określonych iteracjach bada sieć pod kątem usterek i podejrzanych ruchów

05

Zadbaj o świadomość bezpieczeństwa na poziomie organizacji - najsłabszym ogniwem zabezpieczeń jest człowiek, dlatego nawet podstawowa strategia bezpieczeństwa powinna uwzględniać pracowników

- zadbaj o uświadomienie i wyszkolenie pracowników pod kątem bezpieczeństwa.

06

Reaguj szybko i zdecydowanie - dzięki temu możesz ograniczyć do minimum straty wyrządzone przez cyberprzestępcę

Intro

TestArmy CyberForces to elitarna jednostka do spraw cyfrowego bezpieczeństwa, składająca się z jednych z najlepszych specjalistów w kraju. Nasze usługi pozwolą zadbać o bezpieczeństwo firmom, które dopiero zaczynają w nie inwestować, a dojrzałym organizacjom pomóc w opracowaniu i realizacji długofalowej strategii bezpieczeństwa.

Z rynkiem e-commerce mamy styczność praktycznie od początku istnienia. Współpracowaliśmy z największymi e-sklepami w Polsce i kilkoma globalnymi firmami, które mają tu swoje placówki. Doskonale znamy ich problemy i ryzyka biznesowe, na które są stale wystawieni. Jesteśmy świadomi, jak bolesna może być utrata reputacji, ponieważ byliśmy świadkami sytuacji w których brak odpowiednich zabezpieczeń okazał się katastrofalny w skutkach. W 2018 roku opracowaliśmy raport dotyczący stanu zabezpieczeń rynku e-commerce w Polsce, a jego wyniki pozostawiały wiele do życzenia. Dużo firm wciąż jest podatnych na łatwe do uniknięcia zagrożenia i chcemy pomóc im to zmienić.

Dla przedsiębiorców, którzy chcą wyróżnić się z tłumu i zadbać o bezpieczeństwo swojej platformy przygotowaliśmy kilka rekomendacji, które zdecydowaliśmy się zawrzeć w tej ofercie.

Zapraszam do zapoznania się z dedykowaną sektorowi e-commerce ofertą TestArmy CyberForces.

Dawid Bałut
Chief Security Strategist & CEO TestArmy CyberForces

Spis treści

Bezpieczeństwo sektora e-commerce

Nowe realia handlowe to także nowe zagrożenia. Cyberprzestępcy są czujni, a ich działaniami kieruje chęć zysku. Jeśli jednak weźmiemy pod uwagę możliwe luki w naszych zabezpieczeniach i związane z nimi wektory ich ataku dochodzimy do prostego wniosku - bezpieczeństwo nie jest stanem.

Bezpieczeństwo to płynny proces, polegający na ciągłym rozwijaniu swojej infrastruktury i powtarzalnych czynnościach, których zadaniem jest sprawdzić jej obecny stan i wskazać luki, które należy załatać.

Każdą platformę e-commerce należy traktować jako funkcjonujący system, polegający na odpowiednim zarządzaniu danymi. W jego skład wchodzą rozmaite dane osobowe, informacje o firmach i produktach oraz transfery pieniężne. Z perspektywy hakera są one atrakcyjnym łupem, który łatwo może zostać zmonetyzowany, lub wykorzystany do zaplanowania kolejnego, bardziej wyrafinowanego ataku.

Kluczem do zapewnienia bezpieczeństwa swojej platformy jest ustalenie odpowiedniej polityki bezpieczeństwa, inwestycja w infrastrukturę bezpieczeństwa i regularne testowanie jej pod możliwie jak najszerszym kątem.

FUNKCJONOWANIE BEZPIECZNEGO SYSTEMU E-COMMERCE POWINNO OPIERAĆ SIĘ NA PIĘCIU WSKAŹNIKACH:

Poufność
odpowiednie dane, usługi i działania powinny być dostępne wyłącznie dla uprawnionych podmiotów. Każda nieścisłość na tym polu niesie ze sobą ryzyko utraty ważnych danych.

Integralność
nieuprawnione modyfikowanie informacji nie powinno być możliwe, a wszelkie próby muszą zostać odnotowane i zbadane.

Dostępność
określone informacje i usługi powinny być dostępne w każdych okolicznościach dopuszczonych przez politykę bezpieczeństwa.

Autentyczność
zapewnienie o prawdziwości wszystkich stron biorących udział w transakcji.

Niepodważalność
zapewnienie o niepodrabialności wszelkich operacji. Zadbanie o ten punkt pozwoli uniknąć ryzyka np. przetworzenia podrobionej karty płatniczej.

Niedostateczne zadbanie o bezpieczeństwo może wiązać się z poważnymi ryzykami, takimi jak straty finansowe i utrata reputacji. O ile to pierwsze nie musi oznaczać końca biznesu, o tyle drugie może mieć katastrofalne skutki dla firm, nawet jeśli zbudowały już silną globalną markę.

Nasza oferta

ORGANIZACJOM, KTÓRE ZACZYNAJĄ INWESTOWAĆ W BEZPIECZEŃSTWO, LUB CHCĄ SPRAWDZIĆ SWOJE SYSTEMY, ZAPEWNIAMY:

Testy penetracyjne

Audyt bezpieczeństwa

Testy wydajnościowe

Bezpieczne wytwarzanie oprogramowania

Testy socjotechniczne

Szkolenia dla pracowników

DOJRZAŁYM ORGANIZACJOM POMAGAMY OPRACOWAĆ:

Kompleksową strategię rozwijania infrastruktury bezpieczeństwa

Kompleksową strategię zachowania ciągłości biznesu (Business Continuity) **i odbudowania po katastrofie** (Disaster Recovery)

TE OBSZARY PODDAJEMY TESTOM BEZPIECZEŃSTWA:

- **Infrastruktura systemu i jego komponenty**
- **Poziom bezpieczeństwa baz danych** (także kopie zapasowe i monitorowanie systemu)
- **Proces zakupowy**
- **Konfiguracja protokołu HTTPS**
- **Występowanie błędów logicznych**
- **Oprogramowanie CMS**
- **Integracja z bramkami zakupowymi**
- **Wydajność serwerów**
- **Weryfikacja i autoryzacja** (proces zakładania konta i logowania)
- **Raporty błędów**
- **Bezpieczeństwo chmury danych**

Podczas przeprowadzania kompleksowych testów bezpieczeństwa korzystamy z wewnętrznych systemów i platform umożliwiających szereg operacji, od znajdowania miejsc, do których standardowy użytkownik nie powinien mieć dostępu, po środowiska służące do symulacji zorganizowanych ataków hakerskich.

Zabezpieczenie serwisu WWW i aplikacji mobilnej

Sklepy internetowe w Polsce opierają się w większości na aplikacjach webowych i mobilnych. Ponieważ mówimy o e-handlu, strona i aplikacja sklepu pośredniczą we wszystkich operacjach, jakie dokonywane są w obrębie systemu, np. komunikacji z serwerem, transferze danych czy zarządzaniu płatnościami.

Jednym z podstawowych wektorów ataku na e-commerce, będzie więc atak na platformę zakupową za pośrednictwem aplikacji. Cyberprzestępcy znają wiele podatności, które mogą prześlizgnąć się niezauważenie przez proces tworzenia kodu. Odpowiednio wykorzystane, mogą pozwolić im np. na ingerencję w bazy danych, czy osadzenie w treści strony kodu, którego wykonanie może skutkować zainfekowaniem urządzenia kupującego.

Zadaniem CyberForces jest znalezienie i wskazanie takich podatności, a następnie przesłanie kompleksowego raportu oraz pomoc w ich naprawie.

Jak to robimy:

Audyt bezpieczeństwa

Przy użyciu testów manualnych i automatycznych sprawdzamy standardowe zagrożenia aplikacji WWW i najpopularniejsze podatności platform e-commerce, które mogą służyć za furtkę dla cyberprzestępców. Są to na przykład:

| SQL injection - umieszczenie zmodyfikowanego zapytania w formularzu na stronie, pozwalającego na ominięcie zabezpieczeń i swobodną ingerencję w bazę danych. Może posłużyć do kradzieży wrażliwych danych Twoich klientów.

| Cross-site scripting - podatność pozwalająca na wykonanie kodu JavaScript, który infekuje urządzenie po otwarciu strony lub kliknięciu w zawarty na niej link. Twój serwis staje się wtedy narzędziem ataku na jego użytkowników.

Testy penetracyjne

Kontrolowane i bezpieczne ataki hakerskie mające na celu odkrycie podatności, na które mógłby trafić prawdziwy cyberprzestępca. Przeprowadzane metodami:

| czarnej skrzynki - przeprowadzane z zewnątrz sieci, co oznacza, że tester wciela się w cyberprzestępcę, ale nie zna dokładnych specyfikacji systemu, który jest celem jego ataku.

| szarej skrzynki - testy z perspektywy zalogowanego użytkownika z nadanymi pewnymi przywilejami, pozwalające na bardziej skoncentrowany i wydajny atak. Tester zwykle ma dostęp do dokumentacji i zna architekturę systemu.

| białej skrzynki - przeprowadzane przez testera, który ma dostęp do pełnej dokumentacji i kodu źródłowego aplikacji, co pozwala na pasywne i aktywne przeanalizowanie jej pod kątem wewnętrznych i zewnętrznych podatności.

Testy wydajnościowe

Pozwolą uniknąć konsekwencji ataku typu DDoS (Distributed Denial of Service) czyli przeciążeniu serwera poprzez wysłanie dużej liczby zapytań z tysięcy adresów IP, co może doprowadzić do spowolnienia, a nawet wyłączenia serwisu.

CASE STUDY

DDoS to nie jedyna przyczyna wyłączenia serwisu. Często w okresach wzmożonego ruchu np. w podczas Black Friday czy w okresie przedświątecznym, sklepy, które nie są na to przygotowane, mogą odczuć przykre konsekwencje przeciążenia serwerów. Taka sytuacja miała miejsce w 2018 roku, kiedy Allegro wystawiło ponad sto sztuk telefonu przecenionego z ok. 850 zł na 1 zł. Niestety nie spodziewali się aż takiego zainteresowania i wygenerowane w ten sposób obciążenie spowodowało brak dostępu do serwisu, który poniósł spore straty finansowe.

Może się zdarzyć, że atak DDoS zostanie zlecony przez konkurencję, dla której Twoja strata jest przecież zyskiem. Takie ryzyko, choć niewielkie, istnieje. Możliwość rozładowania sztucznie generowanego ruchu powinno więc być wpisane w strategię bezpieczeństwa e-sklepu. Każdy e-commerce powinien też znać ograniczenia swoich serwerów.

CyberForces posiada platformę testową, która jest w stanie zweryfikować dostępność Twojego serwisu na różnych stopniach obciążenia. Zweryfikujemy ich wydajność, wesprzemy Twoją firmę w okresach wzmożonego zainteresowania i błyskawicznie zareagujemy, jeśli padniesz ofiarą ataku DDoS.

Bezpieczeństwo baz danych

Bazy danych to najbardziej wartościowe zasoby sklepów internetowych. Zawierają bogate informacje o klientach, ich dane osobowe, historię zakupów, dane płatnicze i metadane dotyczące np. urządzeń jakimi się posługują podczas przeglądania strony sklepu. Takie informacje są wartościowe same w sobie, ponieważ łatwo można je sprzedać, ale co sprytniejsi hakerzy wykorzystują je do przeprowadzenia bardziej wyrafinowanych ataków. Mogą stać się wypadową kradzieży tożsamości, albo zaawansowanej strategii phishingowej wymierzonej w konkretnego użytkownika.

Bezpieczeństwo danych klientów powinno stać się priorytetem ze względu na obowiązujące akty prawne:

RODO/GDPR

Rozporządzenie unijne z 27.04.2016. Zgodnie z jego postanowieniami, każda firma posiadająca bazy danych klientów jest zobowiązana m. in. do zabezpieczenia swoich systemów informatycznych i ochrony danych klientów.

CCPA

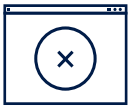
Rozporządzenie prawne obowiązujące w Kalifornii, bazowane na GDPR. Za niedostosowanie się do jej postanowień może wiązać się z dotkliwymi karami finansowymi (tym wyższymi w przypadku braku lub niewłaściwej komunikacji do klientów).

ISO 27001

Międzynarodowa norma standaryzująca systemy zarządzania bezpieczeństwem informacji.

Bardzo wiele sklepów internetowych powstaje na platformach dostarczonych przez firmy trzecie w chmurze lub jako SaaS. Takie rozwiązanie niesie ze sobą **model współdzielonej odpowiedzialności**, ale to **nie oznacza, że bezpieczeństwo leży po stronie dostawcy**. Tak naprawdę, wymaga to dodatkowego przeszkolenia ze strony właściciela sklepu. Należy również pamiętać, że w przypadku ewentualnego ataku, jest on odpowiedzialny za minimalizację ryzyka i odpowiednią komunikację do klientów.

Bardzo popularnym rodzajem ataków, który niesie za sobą olbrzymie ryzyko strat finansowych jest **ransomware**. To atak wymierzony w bazę danych, który skutkuje jej zablokowaniem np. poprzez szyfrowanie. Brak dostępu do danych oznacza:



problemy z funkcjonowaniem serwisu

zablokowanie procesu zakupowego

brak możliwości przetwarzania transakcji

konieczność zapłaty za odszyfrowanie danych (nigdy tego nie rób, przestępcy będą wysyłali żądanie w nieskończoność)

Bezpieczna transmisja danych

Wszelkie dane transmitowane przez serwis e-commerce muszą być odpowiednio zabezpieczone. Aby upewnić się, że tak jest należy dokładnie sprawdzić dwa obszary:

| **Protokół HTTPS** - dane klienta i połączenie z systemem płatności muszą posługiwać się protokołem HTTPS. Oznacza to, że połączenie między danymi klienta, e-sklepem i systemem płatności jest bezpiecznie zaszyfrowane

| **Bezpieczeństwo backupów baz danych** - zaszyfrowane kopie zapasowe muszą znajdować się w innej lokalizacji, niż reszta serwisu

Zadbanie o takie praktyki oznacza jedno - nikt nie może podszyć się pod połączenie lub klienta, ani przechwycić płatności.

CASE STUDY

Szanujemy prywatność naszych klientów i dbamy o ich bezpieczeństwo, dlatego nie podajemy szczegółowych danych.

Właściciel jednej z większych platform e-commerce zwrócił się do CyberForces w celu wykonania serii testów penetracyjnych zorientowanych na kradzież bazy danych użytkowników.

Wyzwanie:

Namierzenie i analiza podatności na ataki na poziomie platformy zakupowej i zintegrowanej z nią aplikacji mobilnej.

Podatności w kontekście architektury platformy zakupowej:

| **SQL injection (SQLi)** - ingerencja w bazę danych umożliwiająca odczytywanie, aktualizowanie, modyfikowanie i usuwanie danych, realizowana za pomocą zmodyfikowanego zapytania umieszczanego w formularzach na stronie

| **Cross-site scripting (XSS)** - osadzenie w treści strony kodu, który wyświetlony użytkownikom może doprowadzić do wykonania niepożądanych akcji

| **Zdalna egzekucja kodu (RCE)** - pozwala na wysyłanie niestandardowych żądań do serwera zmieniających sposób jego działania

| **Podniesienie przywilejów** - zdalne połączenie się z bazą danych z konta użytkownika, dysponując uprawnieniami administratora

Podatności na ataki na poziomie aplikacji mobilnej:

| XSS, RCE, SQLi

| Niewystarczające zabezpieczenie danych w warstwie transportowej - umożliwia podsłuch danych przesyłanych do serwera

| Zabezpieczenia przechowywania danych na urządzeniu

Rezultaty:

Po zakończeniu testów przygotowaliśmy szczegółowy raport zawierający zalecenia pozwalające na załatanie istniejących podatności i sugerujący działania prewencyjne, między innymi:

- Implementacja automatycznych skanów sprawdzających stronę i aplikację pod kątem podatności na Cross-site scripting
- Ograniczenie przywilejów zapytań do operacyjnego minimum i wyposażenie strony w IPS (system wykrywania i zapobiegania włamaniom), co pozwoli uniknąć ataków związanych z podniesieniem uprawnień
- Wprowadzenie kompleksowego szyfrowania w celu zapewnienia bezpieczeństwa wszystkim danym zarządzanym i przesyłanym przez aplikację webową i mobilną

Ustalono termin retestów po upływie kwartału od zakończenia właściwych testów bezpieczeństwa.

Wysokiej jakości aplikacja e-sklepu

Sklepy internetowe, które nie chcą polegać na dostawcach SaaS decydują się na dedykowane aplikacje. Możliwość całkowitego dostosowania aplikacji do swoich usług to niewątpliwy plus, jednak tworzenie jej od początku wiąże się z koniecznością samodzielnego zadbania o wszystkie jej aspekty - w tym bezpieczeństwo.

TestArmy CyberForces pomaga zadbać o bezpieczeństwo aplikacji e-sklepu służąc wsparciem podczas całego procesu produkcji, począwszy od poziomu planowania, przez proces wytwarzania i dalej po wydaniu gotowego produktu.

Bezpieczne wytwarzanie oprogramowania

We współpracy z klientem i firmą wytwarzającą oprogramowanie opracowujemy najważniejsze punkty wdrażanej od początku strategii bezpieczeństwa na poziomie aplikacji i całej infrastruktury. Zależy nam na dogłębnym zrozumieniu działania aplikacji i celów biznesowych klienta, dzięki czemu określimy:

- możliwe podatności
- obszary wymagające testów i retestów
- ryzyko biznesowe i wynikające z niego priorytety
- cele biznesowe i plan rozwoju biznesowego klienta oraz wynikającą z nich długoterminową strategię bezpieczeństwa

Dzięki takim działaniom klient będzie miał pewność, że dobrze zna swoją aplikację i jest ona bezpieczna.

Audyt bezpieczeństwa

Możemy także przeprowadzić niezależny audyt aplikacji i dostarczyć raport wyłącznie klientowi, aby upewnił się, że wszystko zostało wykonane zgodnie z jego zaleceniami i najwyższymi standardami bezpieczeństwa.

Praktycznie każde oprogramowanie e-sklepu korzysta z wtyczek firm trzecich. Wchodzą one w skład serwisu i dla jego bezpieczeństwa powinne zostać odpowiednio przetestowane. Pozwoli to klientowi zweryfikować i zoptymalizować łańcuch dostaw.

Przykładowa ścieżka współpracy

Aby oferować usługi najwyższej jakości, zawsze patrzymy na problem z wielu perspektyw. Dużą wagę przywiązujemy do aspektu biznesowego, który pozwoli nam oszacować krytyczne punkty infrastruktury bezpieczeństwa i nadać odpowiedni priorytet znalezionym lukom w zabezpieczeniach, na podstawie wynikającego z nich ryzyka biznesowego.

01

Zaczynamy od **podpisania NDA** (umowy poufności) **i odbieramy dane dostępowe do systemów klienta**

02

Przeprowadzamy **wstępną analizę systemów,** i na podstawie wiadomości dotyczących ich architektury weryfikujemy zakres testów oraz wyceniamy projekt

03

Dobieramy **zespół testerów,** który dzięki specjalizacji w zakresie branży i systemów klienta dostarczy usługę najwyższej jakości

04

Przedstawiamy ofertę i dostarczamy klientowi wszelkie niezbędne informacje (np. adresy IP z których będą przeprowadzane testy penetracyjne)

05

Przygotowujemy testy, upewniamy się, że klient wie kiedy i w jaki sposób będą one przeprowadzane. Wspólnie ustalamy ich termin tak, aby w żaden sposób nie zakłócić ciągłości biznesu

06

Przeprowadzamy testy, podczas których natychmiast zgłaszamy wszelkie krytyczne podatności

07

Przygotowujemy **kompleksowy raport** zawierający podsumowanie w dwóch wersjach - pierwszej przeznaczonej dla zarządu, drugiej dla działu technicznego. **Wyszczególniamy** wszelkie znalezione podatności, **opisujemy** je, **pokazujemy** w jaki sposób je odtworzyć i **sugerujemy** w jaki sposób można je naprawić.

08

Przeprowadzamy szkolenia i wykłady pozwalające zespołom klienta przygotować się na zagrożenia i uniknąć podobnych sytuacji w przyszłości.

09

Wspólnie z klientem **ustalamy dogodny termin retestów** w celu weryfikacji szczelności systemu.

TestArmy
CyberForces

- QA consulting
- Testy funkcjonalne
- Automatyzacja
- Szkolenia i warsztaty

Cyberbezpieczeństwo

- Pentesting
- Programy Cybersecurity
- Wytwarzanie bezpiecznego oprogramowania
- Zapewnienie cyberbezpieczeństwa dla VIP-ów

Customer Experience

- Dostępność
- Wydajność
- User Experience
- Skalowalność

Kontakt

Gabriel Kamiński
Digital Assurance Strategist

TestArmy Group S.A.
t: +48 664 029 754
@: gabriel.kaminski@testarmy.com

Szymon Chruścicki
Poland New Business Director

TestArmy Group S.A.
t: +48 505 372 810
@: szymon.chruscicki@testarmy.com