Raport TestArmy

Stan Cyberbezpieczeństwa Polskiej Branży E-commerce

TestArmy

www.testarmy.com

W TestArmy nie tylko dbamy o najwyższą jakość produktów IT w kraju i na świecie, ale także monitorujemy stan serwisów i aplikacji poszczególnych branż oraz świadomości przedsiębiorców na temat zagrożeń. Przeprowadziliśmy więc ankietę wśród właścicieli sklepów internetowych, aby dowiedzieć się co wiedzą o czyhających na nich zagrożeniach i jak się przed nimi zabezpieczają.

Z zebranych odpowiedzi powstał raport, który właśnie czytasz. Jego wyniki wydawać się mogą szokujące i prawdopodobnie tłumaczą skalę problemu. Miejmy nadzieję, że misja TestArmy się powiedzie i uda nam się zapobiec choćby części ataków na polskie sklepy online.

Ankieta składała się z 71 pytań poruszających najróżniejsze aspekty dotyczące zarówno samych firm, jak i tego jak dbają one o bezpieczeństwo swoje i swoich klientów. Skierowana była przede wszystkim do właścicieli przedsiębiorstw oraz osób decyzyjnych, które mają realny wpływ na poruszane w niej zagadnienia. Do omówienia wyników zaangażowaliśmy naszego eksperta od cyberbezpieczeństwa, Dawida Bałuta.

Dawid Bałut

Pentester i Bug Hunter z dużym doświadczeniem, który dołączył do defensywnej strony mocy i przez ponad pół dekady pracował jako Architekt Bezpieczeństwa dla korporacji z Doliny Krzemowej. Na co dzień buduje systemy zabezpieczeń, szkoli pracowników i automatyzuje wszelkie procesy bezpieczeństwa.

O TestArmy

TestArmy to dobrze zorganizowana grupa operacyjna testerów. Specjalizujemy się w testowaniu bezpieczeństwa, funkcjonalności i wydajności wszystkiego co się da: od aplikacji bankowych, po inteligentne szczoteczki do zębów. Od ponad 7 lat zapewniamy bezpieczeństwo i wysoką jakość produktów IT we współpracy z deweloperami z Polski i nie tylko, sukcesywnie zwiększając swój udział w globalnym rynku.

Skala firm e-commerce w Polsce

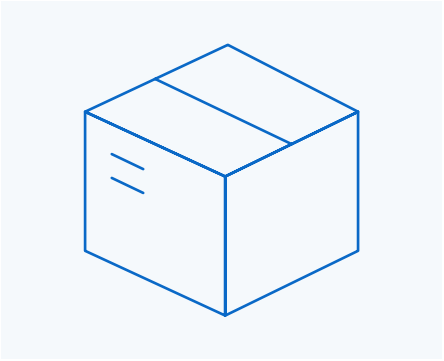
Dla wielu ankietowanych sprzedaż internetowa stanowi ponad 50% całości obrotów firmy, a w przypadku niektórych przedsiębiorców jest jedynym źródłem przychodów. Jest zatem czego bronić przed potencjalnymi agresorami. Na polskim rynku działają firmy o przychodach sięgających 10 milionów złotych i zatrudniają nawet po 50 osób.

Zdecydowana większość biznesów e-commerce w Polsce handluje fizycznym towarem. Tylko 10% sklepów prowadzi sprzedaż dóbr wirtualnych, takich jak muzyka w formatach cyfrowych, czy e-booki.

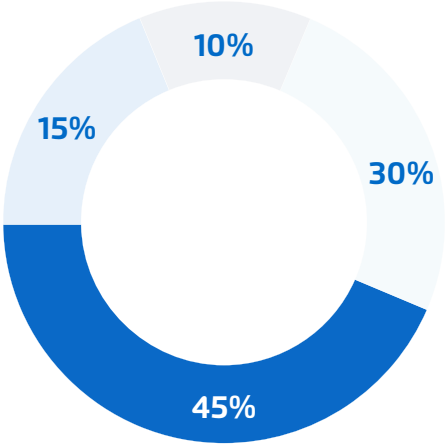
Obroty roczne większości sklepów zdecydowanie przekraczają milion złotych. Tylko 5% przedsiębiorców zdecydowało się nie ujawniać informacji o swoich przychodach w naszej całkowicie anonimowej ankiecie.

Techniczne aspekty działania badanych sklepów

Większość przedsiębiorstw branży e-commerce korzysta z hostingu www, podczas gdy zaledwie kilkanaście procent ankietowanych odpowiedziało, że korzysta z chmury do prowadzenia swojego biznesu online. Jest to o tyle ciekawe zjawisko, że zagraniczne firmy e-commerce bardzo chętnie przenoszą się do chmury, dzięki czemu mogą powierzyć odpowiedzialność za bezpieczeństwo korporacjom, które są w stanie zagwarantować im bardzo wysokie standardy utrzymania infrastruktury.



Odpowiedź na pytanie:
Nasz sklep internetowy działa na (jedna odpowiedź):



Własne serwery we własnym centrum danych	0%
Serwery dzierżawione w jednym z polskich centrów danych	15%
Chmura polskiego dostawcy	30%
Chmura jednego ze światowych liderów usług chmurowych	0%
Hosting WWW	45%
Nie wiem	10%

Źródło: opracowanie własne TestArmy

Prawie połowa ankietowanych firm opiera swój sklep o oprogramowanie na licencji Open Source[1]. Reszta stawia na komercyjne rozwiązania, a co ciekawe - nigdzie nie miesza się ze sobą tych dwóch skrajnie różnych podejść.

Bezpieczeństwo polskich przedsiębiorstw e-commerce

Znaczna liczba ankietowanych nie jest w stanie stwierdzić, czy systemy bezpieczeństwa w ich firmach są na wystarczająco wysokim poziomie. Mimo, że ankietowani samodzielnie oceniają się neutralnie, to skłanialibyśmy się raczej w stronę stwierdzenia, że są nieprzygotowani do odparcia zagrożeń. Taki wniosek opieramy na fakcie, że bardzo wiele firm nie posiada nawet backup planu.

W firmach tych budżet na kwestie bezpieczeństwa nigdy się nie zmienia albo jest w ogóle

[1] Open Source (otwarte oprogramowanie) jest to oprogramowanie, którego licencja pozwala na legalne oraz nieodpłatne kopiowanie. Jednocześnie zapewnia swobodne rozwijanie, analizowane i rozbudowę danego przez użytkowników.

pomijany. Na szczęście ryzyko jest jakoś balansowane - większość z ankietowanych outsourcuje proces zarządzania bezpieczeństwem do firm hostingowych i nie próbuje nawet zarządzać serwerami na własną rękę. Przechowywanie serwerów we własnej infrastrukturze biurowej wiąże się z ogromnym ryzykiem operacyjnym, jak i ze względu na przepisy GDPR (RODO), które wymagają zastosowania odpowiednich, wyjątkowo kosztownych (szczególnie dla małych/średnich przedsiębiorstw) środków bezpieczeństwa.

Większe firmy zlecają hosting swoich serwisów specjalistycznym firmom IT, które posiadają swoje własne departamenty bezpieczeństwa, zajmujące się monitorowaniem ewentualnych ataków na sklepy internetowe klientów.

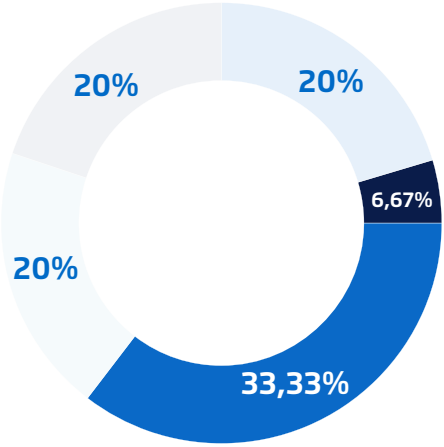
Polem do popisu, jeśli chodzi o bezpieczeństwo w e-commerce, jest usprawnienie procesów audytu i weryfikacji dostawców oprogramowania i infrastruktury sprzętowej: czy posiadają oni stosowne zabezpieczenia i ubezpieczenia obejmujące cyberataki? Kiedy powierzamy komuś opiekę nad elementami, bez których nasz biznes nie jest w stanie funkcjonować, musimy mieć pewność, że trafiają one w dobre ręce. Często trafiamy na przypadki firm hostingowych, które ogłaszają bankructwo po tym, jak padły ofiarą ataku hakerskiego.

Jeśli chodzi o ubezpieczenia od konsekwencji cyberataków, to jest to relatywnie nowy temat, który jednak powinien zainteresować każdą firmę opierającą się o działania on-line. Kilkoro ankietowanych potwierdziło wykupienie stosownej polisy chroniącej przed skutkami prawnymi oraz finansowymi cyberataku. Co piąty ankietowany nie wie nawet, czy jego firma posiada polisę, która mogłaby uratować go w przypadku cyberataku.

Nie ważne jednak, czy firma jest ubezpieczona, czy nie, jeśli nieodwracalnie utraci ona wszystkie dane znajdujące się na serwerach i zaufanie klientów. Finansowa

rekompensata może nie pozwolić uratować biznesu, który ucierpiał tak dotkliwie. Zapytaliśmy więc o kwestię back-upu danych.

Odpowiedzi na pytanie:
W przypadku incydentu prowadzącego do uszkodzenia danych w głównym centrum danych Państwa providera...



Nie obawiamy się utraty danych, gdyż mamy aktualną kopię danych w innej lokalizacji.	20%
Dane w sklepie internetowym pochodzą z innych systemów lub są do innych systemów często eksportowane i możemy je odtworzyć przy niedużym nakładzie pracy.	33,33%
Odtworzenie większości danych powinno być możliwe przy dużym nakładzie pracy.	6,67%
Sklepy internetowy w głównym centrum danych jest jedyny miejscem przechowywania aktualnych danych związanych z jego działalnością.	20%
Nie wiem	20%

Źródło: opracowanie własne TestArmy

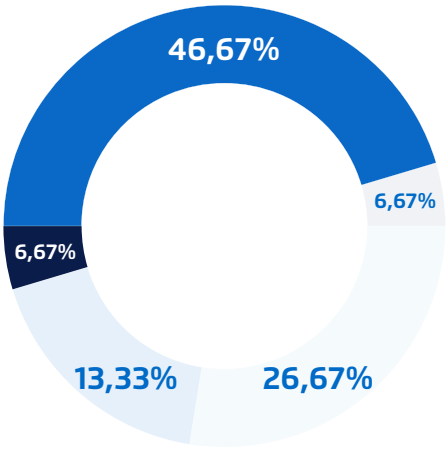
Wielu respondentów zdaje sobie sprawę z tego, że odpowiedzialność za bezpieczeństwo serwisów ciąży zarówno na ich użytkownikach, jak i właścicielach oraz pracownikach. Jedną z bardziej cennych informacji, jakie udało nam się zdobyć jest fakt, że wiele firm e-commerce potrafi zachować się dojrzale i w przypadku ataku wziąć na siebie część odpowiedzialności za straty, zamiast zrzucać całą winę na przestępców. Poczuwanie się do winy sprawia, że takie przedsiębiorstwa reagują na incydenty w rozsądniejszy sposób, co zdecydowanie pozytywnie wpływa na ich wizerunek w oczach klientów.

Połowa badanych przedsiębiorstw jest teoretycznie przygotowana na ewentualne incydenty związane z bezpieczeństwem, jednak równie wielu ankietowanych nie było w stanie stwierdzić, czy są na taką sytuację gotowi. Oznacza

to najczęściej, że takie osoby nie znają dokładnie anatomii swojego biznesu.

Większość ankietowanych przyznaje się, że nie przeprowadziło analizy ryzyka, która pozwoliłaby im ocenić rozmiar potencjalnych strat. Jeszcze więcej przedsiębiorców mówi wprost, że cyberbezpieczeństwo nie jest czymś, co w ogóle biorą pod uwagę przy planowaniu budżetu, a ryzyko przerwy w sprzedaży internetowej traktują jako coś, co po prostu "może się zdarzyć".

Odpowiedzi na pytanie:
W przypadku przerwy w działaniu sklepu w głównym centrum danych...



...nie spodziewamy się wpływu awarii na sprzedaż, gdyż funkcje automatycznie przejmą serwery z innej lokalizacji.	26,67%
...mamy gotowy plan ręcznego uruchomienia sklepu w innej lokalizacji.	6,67%
...mamy wkalkulowane w biznes ryzyko wystąpienia przerwy w sprzedaży internetowej.	6,67%
...jeszcze nie mamy aktualnego planu działania.	46,67%
Nie wiem	13,33%

Źródło: opracowanie własne TestArmy

Okazało się, że kilka firm w ogóle nie ma żadnego planu działania na wypadek wystąpienia cyberataku, co jest skrajnie niebezpiecznym podejściem.

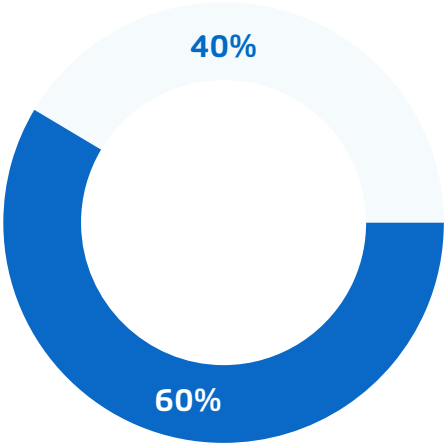
Skoro firmy nie rozważały takiej sytuacji nawet teoretycznie, to najprawdopodobniej nie

przeprowadziły też jakichkolwiek działań prewencyjnych od strony technicznej, aby zwiększyć swoją odporność na ataki, na przykład typu ransomware. Nasze podejrzenia znajdują potwierdzenie w odpowiedziach jakie otrzymaliśmy na pytanie dotyczące testów penetracyjnych. Okazuje się, że polscy przedsiębiorcy traktują tę kwestię po macoszemu i bardzo często w ogóle nie interesuje ich zlecenie audytu bezpieczeństwa niezależnym ekspertom. Nie mają oni więc kompletnie pojęcia jak łatwo jest włamać się do ich systemów i wyrządzić szkody.

Zrzucanie całej odpowiedzialności na providera hostingu to nie wymówka, bo na końcu najwięcej traci i tak sklep oraz jego klienci.

Najgorszy jest fakt, że przedsiębiorcy zdają sobie sprawę z tego, że ich firmy nigdy nie były badane pod tym kątem, a nic z tym faktem nie robią!

Odpowiedzi na pytanie:
Czy w Państwa firmie był przeprowadzony audyt bezpieczeństwa strony internetowej sklepu (test penetracyjny)?



Tak, przy okazji uruchomienia sklepu.	0%
Tak, przeprowadzane są regularnie.	0%
Tak, przeprowadzany jest nieregularnie.	40%
Nie był przeprowadzany.	60%
Nie wiem	0%

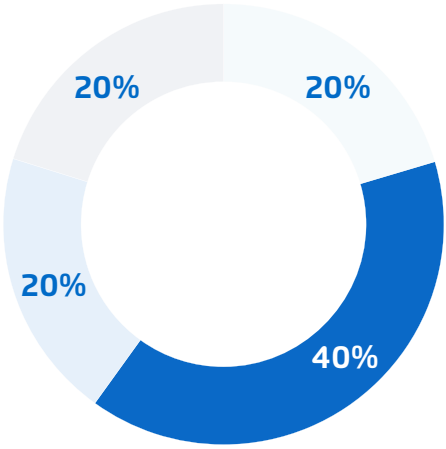
Źródło: opracowanie własne TestArmy

Statystycznie rzecz biorąc, firmy nie stosują dostatecznie dużej liczby zabezpieczeń, a wiele urządzeń wykorzystywanych przez

pracowników jest w ogóle nie kontrolowana - pracownicy często używają w celach służbowych swoich prywatnych telefonów komórkowych i komputerów. Pomimo tego, że sporo firm pozwala na dostęp do danych wrażliwych tylko na terenie biura, to wciąż wiele jest takich, które pozwalają na dostęp do nich z poziomu dowolnego, prywatnego urządzenia, nie biorąc (najpewniej nieświadomie) pod uwagę ryzyka jakie ponoszą. Największymi zagrożeniami są w takim wypadku wycieki danych osobowych klientów firmy oraz ataki oprogramowaniem ransomware, zmiany cen produktów, phishing i oszustwa w płatnościach. Wektorem ataku może być zainfekowane urządzenie, bądź nieświadomy użytkownik.

Wciąż stosunkowo niewiele firm stosuje dodatkowe metody zabezpieczeń systemów krytycznych, na przykład Uwierzytelniania Dwuskładnikowego (2FA). Całe szczęście, że standardem jest stosowanie konwencjonalnych metod zabezpieczeń przed atakami, jak programy antywirusowe, certyfikat SSL, szyfrowanie danych po stronie serwera, managery haseł i szkolenia dla pracowników, o czym ostatnio wspominaliśmy na blogu TestArmy.

Odpowiedzi na pytanie:
Czy w Pana/Pani firmie używa się innego sposobu uwierzytelniania użytkownika poza hasłem?



Pojedyncze logowanie (SSO)	0%
Uwierzytelnianie wielopoziomowe (2FA)	20%
certyfikat	0%
podpis elektroniczny	0%
inne (jakie?)	20%
nie używam	40%
nie wiem	20%

Źródło: opracowanie własne TestArmy

Właściciele firm e-commerce z sobie tylko znanych powodów pozwalają na zdalny dostęp do systemów finansowych firm, pomimo braku jakiejkolwiek pewności co do zabezpieczeń na prywatnych urządzeniach swoich pracowników. Nie da się stwierdzić, czy dany pracownik używa oprogramowania antywirusowego, czy jego twardy dysk jest zaszyfrowany, a czy jego zawartość udostępniona w sieci komuś, kogo mogą interesować wrażliwe dane kontrahentów firmy albo hasła do zarządzania platformą e-commerce, które pozwoliłyby zmieniać statusy zamówień w celu zniszczenia reputacji marki lub wyłudzenia "darmowych" zakupów. Większość właścicieli firm e-commerce nie wie nawet, czy byłoby w stanie odciąć dostęp do systemów firmy pracownikom, którzy nagle przestaliby przychodzić do pracy.

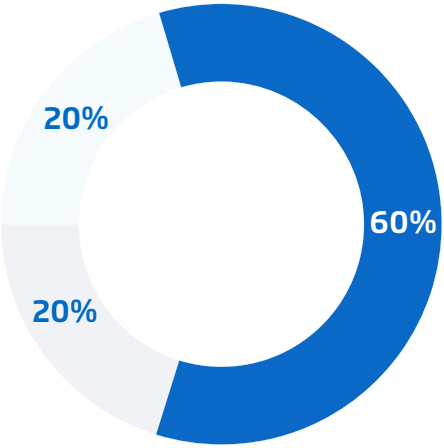
Kilku przedsiębiorców twierdząco odpowiedziało na pytanie, czy przydarzył im się już jakiś nieprzyjemny incydent dotykający bezpieczeństwa firmy.

Mimo, że z pozoru może brzmieć to nieprzyjemnie, to jest to tak naprawdę dobra informacja. Ktoś, kto zrozumiał już, że ataki faktycznie się zdarzają jest gotów zastanowić się nad wdrożeniem technologii monitorujących, które pozwolą w przyszłości rozpoznawać niebezpieczne sytuacje na czas. Co oczywiste, wśród respondentów znalazło się też kilka firm, które o tym, że padły atakiem dowiedziały się bezpośrednio od hakera, który żądał okupu.

Niektóre z ankietowanych firm zatrudniały osobę, która odpowiadała stricte za cyberbezpieczeństwo, co w Polsce okazało się interesującą i obiecującą nowinką. Zdecydowanie za mało mówi się

w naszym kraju na tematy dotyczące zabezpieczania e-commerce.

Odpowiedzi na pytanie:
Czy w wewnętrznych strukturach firmowych znajduje się osoba odpowiedzialna za cyberbezpieczeństwo?



Tak	60%
Nie	20%
Nie wiem	20%

Źródło: opracowanie własne TestArmy

Większość ankietowanych deklaruje zgodność firmy i jej procedur z RODO i posiadanie wszelkich potrzebnych zgód na przetwarzanie danych klientów. Z pewnością pomaga im to, że nie używają rozbudowanych systemów data analytics i nie gromadzą dużych ilości danych, ale w nadchodzącej erze machine learning warto już teraz się przygotować na posiadanie ogromnych ilości informacji.

Wnioski

Niestety wyniki ankiety nie napawają nas optymizmem. Polscy przedsiębiorcy rzadko traktują kwestie cyber zabezpieczeń wystarczająco poważnie, narażając tym samym nie tylko siebie, ale też swoich klientów i pracowników na poważne problemy, nie tylko finansowe.

5 rekomendacji

Pozwoliliśmy więc sobie przygotować listę najważniejszych rekomendacji dla każdego przedsiębiorcy działającego w branży e-commerce:

1. Upewnić się, że dostęp do aplikacji i serwera jest ograniczony tylko do osób które koniecznie muszą mieć do nich dostęp
2. Upewnić się, że firma posiada zasady disaster recovery, które pomogą jej wytrzymać ataki hakerskie typu ransomware, np. poprzez zabezpieczenie niezawodnych kopii zapasowych.
3. Przeprowadzić niezależne testy i audyty bezpieczeństwa, zarówno testy penetracyjne które mają za zadanie sprawdzić poziom bezpieczeństwa aplikacji i serwera, jak i o audyt bezpieczeństwa pod kątem zgodności z GDPR.
4. Zainstalować program antywirusowy na komputerze każdego pracownika łączącego się z systemami firmowymi oraz upewnić się, że dostęp do nich jest chroniony silnymi hasłami i uwierzytelnianiem dwuskładnikowym
5. Przeprowadzić szkolenie podnoszące świadomość bezpieczeństwa wśród pracowników, szczególnie w kontekście ataków socjotechnicznych takich jak np phishing

Więcej porad na naszym kanale YouTube. **Sprawdź!**

Chcesz poznać bezpieczeństwo swojej strony?

Skontaktuj się z nami

Szymon Chruścicki
Business Manager
+48 505 372 870

Dawid Bałut
Head of Security, Board Member
+48 608 451 896

contact@testarmy.com

TestArmy