E-commerce w świetle cyberataków

BEZPIECZEŃSTWO

Kei.pl

Kei.pl

Szanowni Państwo,

Przedstawiamy raport, w którym analizujemy zagrożenia z jakimi borykają się przedstawiciele branży e-commerce w Polsce. Wskazujemy na ogół elementów, ze szczególnym uwzględnieniem kwestii bezpieczeństwa infrastruktury oraz sprawdzonych rozwiązań hostingowych. Do współpracy zaprosiliśmy naszych Partnerów, a także czołowych ekspertów w zakresie bezpieczeństwa online. Liczymy, że przygotowany raport okaże się bogatym zbiorem wartościowej wiedzy, a praktyczne wskazówki pomogą w skutecznym zabezpieczeniu platform e-commerce.

Serdecznie zapraszamy do lektury
Zespół Kei.pl

Spis treści <<

Czy hakerzy zagrażają e-commerce?

Z całą pewnością. W dobie dzisiejszych cyberprzestępców muszą obawiać się wszyscy. Zagrożony jest każdy element gospodarki i biznesu. Atakowane są nie tylko systemy finansowe w bankach, ale też systemy przemysłowe, fabryk oraz sklepów internetowych. Rok 2017 okazał się czasem hakerów i upłynął w atmosferze niepokoju. Najnowsze statystyki nie pozostawiają złudzeń: cyberprzestępcy atakują częściej, a co gorsza coraz skuteczniej. Kradzieże e-walut, wycieki danych, hakowanie oprogramowania, atak na sektory gwarantujące stabilność funkcjonowania państwa: sektor logistyczny, zdrowia bądź energetyczny. Ogólnoświatowe infekcje spowodowały panikę i niekiedy, tak jak w przypadku Ukrainy, paraliż krajowej infrastruktury. Ze względu na rozwój technologii zasięg cyberprzestępców sięga coraz głębiej w struktury społeczne.

Live Cyber Attack Threat Map to najlepszy obraz skali zagrożeń. Każdego dnia odnotowanych jest ponad 6 milionów ataków na firmy całego świata. Polska również pozostaje pod ostrzałem, głównie przez cyberprzestępców zlokalizowanych na terenie Stanów Zjednoczonych. Z największą ilością ataków w Europie boryka się Macedonia, na drugim miejscu uplasowała się Turcja. Pechową listę uzupełnia Rumunia.

>> **Ransomware** – (ang. *ransom* – okup) oprogramowanie blokujące dostęp do danych, wysyłające żądanie zapłaty za odblokowanie. Atakowane są nie tylko systemy finansowe w bankach, ale też systemy przemysłowe fabryk i sklepy internetowe. Choć ataki tego typu zdarzały się już w 2005 roku, prawdziwa fala pojawiła się w 2013. Rozpowszechniane najczęściej w załącznikach wiadomości e-mail. Najnowsze wersje złośliwego oprogramowania są w stanie zaszyfrować dyski lokalne i wymienne, a nawet zmapowane dyski w usłudze typu Dropbox.

(ang.) ransom >> okup
(ang.) software >> oprogramowanie

Każdego dnia w Polsce dochodzi do około 100 tysięcy cyberataków

Źródło: https://threatmap.checkpoint.com/ThreatPortal/livemap.html

IoT – Internet of Things – sieć fizycznych urządzeń, sprzętów, pojazdów i pozostałych elementów z wbudowaną elektroniką i oprogramowaniem. Łączność sieciowa umożliwia tym obiektom łączenie się i wymianę danych. Eksperci szacują, że do 2020 roku na IoT będzie składać się około 30 miliardów obiektów. Przewidywana wartość rynku Internetu Rzeczy w 2020 roku to 7,1 biliona USD.

WannaCry zaatakował m.in. brytyjską służbę zdrowia, firmy: FedEx, Nissan, Telefonica, rosyjskie banki i koleje państwowe, a także indyjskie linie lotnicze Shaheen Airlines

Ataki, które w 2017 roku głośnym echem odbiły się w mediach to ataki typu ransomware: WannaCry oraz Petya. WannaCry okazał się atakiem o największym zasięgu geograficznym. Fala cyberataków miała miejsce w maju 2017 roku i była oparta o złośliwe oprogramowanie szantażujące. Dotknęła 300 tys. komputerów w 150 krajach. Rosja, Tajwan, Ukraina i Indie ucierpiały najbardziej. Atak został zaprojektowany w oparciu o wykorzystanie słabości systemów Microsoft (luka w protokole Windows Server Message Block). Straty oszacowano na 4 mld dolarów.

Petya to rodzaj szyfrującego oprogramowania ransomware, określany przez specjalistów jako groźniejszy niż WannaCry. Szkodliwe oprogramowanie atakowało systemy oparte na Microsoft Windows, infekując nie tylko pliki, ale też szyfrując tabelę systemu plików dysku twardego. Warianty Petyi pojawiły się po raz pierwszy w marcu 2016, jednak prawdziwy wybuch przypadł na czerwiec 2017 roku. Firma Kaspersky Lab dla odróżnienia określiła nową wersję jako NotPetya. Oprogramowanie uniemożliwiało uruchomienie systemu Windows, a następnie domagało się, aby użytkownik dokonał płatności w Bitcoin, w celu odzyskania danych. Wirus sparaliżował głównie Ukrainę, ale media donosiły także o problemach polskich firm. Uwagę komentatorów zwrócił fakt, że zaatakowane zostały nawet zaktualizowane systemy Windows 10.

Dwa zmasowane ataki WannaCry i Petya odsłoniły ułomność cyfrowego świata. Choć zwróciło to oczy przywódców na problem bezpieczeństwa w sieci, trudno oczekiwać, że ransomware zniknie w najbliższym czasie. Wręcz przeciwnie! Możemy spodziewać się, że

Bitcoin – waluta wirtualna stworzona w oparciu o modele szyfrujące. W odróżnieniu od zamkniętych systemów takich jak Mastercard czy VISA to zdecentralizowana i otwarta sieć płatnicza. Działająca na bazie oprogramowania typu open-source oraz społeczności użytkowników. Pomimo wirtualnej formy portfela uważa się, że bezpieczeństwo transakcji jest stosunkowo wysokie.

2018 rok przyniesie kolejną falę ataków. Wraz z bitcoinem jako bezpieczną metodą zbierania okupu, cyberprzestępcy przywiązali się do tego modelu ataku.

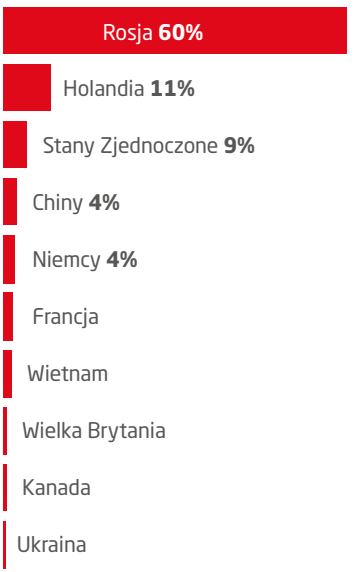
W odpowiedzi na rosnące zagrożenia toczą się światowe debaty nad kwestią cyberbezpieczeństwa. 2018 rok przyniesie zatem nowe dyrektywy i początek działalności RODO.[1] Ataki ransomware zmobilizowały specjalistów ds. bezpieczeństwa w branży IT, którzy na bieżąco opracowują sposoby na uniknięcie zagrożenia. Proces ochrony przed atakami utrudnia fakt, że w związku z rozwojem Internetu Rzeczy hakowaniu podlegają nie tylko komputery, ale też wszystkie urządzenia typu smart.

Dane opublikowane w *Internet Security Threat* Report firmy Symantec obrazują ogrom ataków. Na każde 130 odebranych e-maili 1 zawierał złośliwe oprogramowanie (atak typu malware). Raport podkreśla także, że to średnie firmy zatrudniające do 500 pracowników są głównym celem ataków. Duże firmy korporacyjne, zatrudniające powyżej 1000 pracowników aktualnie znajdują się pod mniejszym ostrzałem.
Dbałość o bezpieczeństwo to obowiązek przede wszystkim osób prowadzących działalność i sprzedaż online. E-sklep jest równie atrakcyjnym celem ataków hakerskich co banki i instytucje finansowe. Amerykański gigant rynku sprzedażowego eBay regularnie boryka się z próbami ataku. W 2014 roku, po tym jak hakerzy wykradli dane z kont użytkowników, przedstawiciele serwisu apelowali do 145 mln klientów o zmianę haseł. Cyberprzestępców nie odstraszył nawet wyrok Sądu Południowego Dystryktu Kalifornii skazujący Amerykanina Anthony'ego Scotta Clarka na 10 lat więzienia za przeprowadzenie ataku DDoS na serwery eBay. Atak przeprowadzony przez młodego cyberprzestępcę zablokował stronę, generując olbrzymie straty finansowe.

W 2013 roku ze zmasowanym atakiem DDoS musiał zmierzyć się największy polski serwis aukcyjny allegro.pl. W związku z brakiem dostępu do serwisu wszystkie aukcje prowadzone w tym czasie zostały wydłużone o 24 godziny.

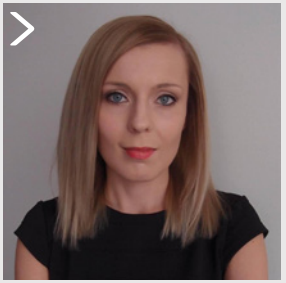
Atakowane są serwery, ale też użytkownicy platform e-commerce. Klienci takich serwisów jak eBay, Amazon czy Alibaba ucierpieli w lipcu 2017 roku. W rozesłanych wiadomościach e-mail poinformowano o anulowaniu zamówienia, a umieszczony w załączeniu plik infekował komputery ofiar. Po kliknięciu w odnośnik automatycznie blokowano przeglądarkę. W komunikacie pojawiał się też numer telefonu, pod który użytkownik miał zadzwonić w celu odzyskania danych. Po drugiej stronie obsługa udająca serwis Microsoft wyłudzała przelewy na konto.

Ponad **60%** podejrzanego globalnego ruchu sieciowego pochodzi z Rosji



F-secure, *State of cybersecurity 2017*
Źródło: https://www.f-secure.com/documents/996508/1030743/cyber-security-report-2017

[1] Więcej o RODO przeczytasz w rozdziale „Ochrona danych osobowych klienta"



Sylwia Walkowicz-Zelek
Dyrektor Działu Realizacji
Agencja reklamowa Brandbay.pl

Wciąż rosnąca liczba użytkowników sklepów internetowych oraz realizowanych transakcji online, czyni serwisy e-commerce głównym celem ataku hakerów. Dlatego też podobnie jak zabezpieczamy swój samochód na parkingu włączając alarm, powinniśmy chronić Klientów naszego sklepu przed zagrożeniami w Internecie. Zapewniając bezpieczeństwo ich danych osobowych, nie tylko będziemy spać spokojnie, ale przede wszystkim zbudujemy z nimi długotrwałe i oparte na zaufaniu relacje. Coraz więcej użytkowników przed dokonaniem zakupu sprawdza bowiem, czy sklep jest wiarygodny i bezpieczny. Dlatego też musimy pamiętać, że jeśli dopuścimy do sytuacji, w której nasi Klienci zobaczą komunikat o tym, że witryna mogła paść atakiem hakerów, trudno będzie nam później przekonać ich, że uporaliśmy się z problemem i teraz jest tu bezpiecznie. Certyfikat SSL jest obecnie absolutnym „must have" nie tylko w kontekście zaoferowania Klientom poczucia bezpieczeństwa, ale również w działaniach marketingowych. Zainfekowany sklep internetowy w krótkim czasie straci swoje pozycje w wynikach wyszukiwania, a sama polityka Google bardzo mocno zmierza w kierunku promowania zaufanych witryn. Brak certyfikatu SSL uniemożliwi również uruchomienie kampanii produktowych Google Adwords czy też poprawną integrację sklepu internetowego z Facebookiem. Krótko mówiąc – bezpieczny sklep będzie sprzedawał więcej, dlatego też jeśli zależy nam na jak najwyższych współczynnikach konwersji, nie powinniśmy dawać naszym Klientom powodów do tego, aby myśleli, że zakupy u nas mogą być ryzykowne.

Przeczytaj więcej:

>> https://www.kei.pl/blog/jak-zwiekszyc-zaufanie-do-swojego-e-biznesu/

Skąd rosnący wzrost zainteresowania hakerską działalnością?

Część działań motywowana jest po prostu dobrą zabawą oraz ogólnymi tendencjami w popkulturze. Ataki zwracają uwagę mediów. Paraliże firm bądź cyber-sabotaże o zabarwieniu politycznym są zwykle szeroko dyskutowane w środkach masowego przekazu. Hakerzy, choć negatywni, to jednak wciąż bohaterzy Internetu. Budzą zainteresowanie, imponują umiejętnościami, mają siłę do wzburzania społeczności. Artykułują siebie jako buntowników w walce z systemem i bywają momenty, w których faktycznie zyskują przewagę nad organami państwowymi. W 2016 roku w Waszyngtonie tuż przed inauguracją prezydencką, w wyniku ataku ransomware policja utraciła kontrolę nad 70% kamer monitorujących... Aspekty polityczne to jeden z motorów działań hakerskich, jednak prawdziwa gra toczy się o pieniądze. Stawką są miliony dolarów rocznie.

Ransomware jako usługa?

Przeprowadzenie ataku hakerskiego jest w zasięgu większości osób. Użytkownicy sieci nie zdają sobie sprawy, że cyberprzestępcą może stać się każdy. Internet daje możliwość wykupienia ataku DDoS, a nawet ataku ransomware ukierunkowanego na konkretną firmę. W sieci istnieją platformy, na których w łatwy sposób, z gotowych modułów można zaprojektować złośliwe oprogramowanie. Funkcjonują giełdy, które

umożliwiają cyberprzestępcom kupno narzędzi. Tętniące życiem podziemie hakerskie codziennie werbuje młodych pasjonatów łamania kodu. Próg umiejętności potrzebnych do wkroczenia w cyberprzestępczy świat bardzo się obniżył.

Jako przykład obrazujący problem może służyć nieinwazyjny ransomware o nazwie Satan. Model RaaS (Ransomware as a service) zachęca do infekowania. W zamian za 30% kwoty z okupu oferuje pełną instrukcję i potrzebne know-how do rozpoczęcia cyberprzestępczej kariery. RaaS daje świetną okazję do wyłudzania danych w sieci bez praktycznie żadnej specjalistycznej wiedzy technicznej. Dostępność platform RaaS to prawdopodobnie jeden z głównych czynników odpowiedzialnych za ogromny wzrost liczby ataków ransomware w ciągu ostatniego roku.

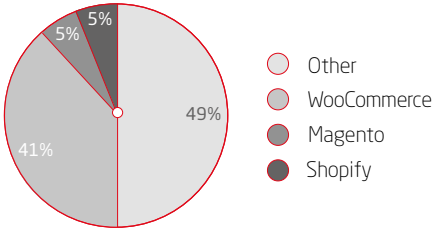
Rozwiązania open source

Choć ataki zza oceanu ze względu na skalę są bardziej spektakularne, polskie e-sklepy również są ciekawym źródłem ataku. Zagrożone są szczególnie sklepy korzystające z masowych, gotowych platform. Startując w e-commerce, oprócz biznesowej strategii należy zadbać o aspekty bezpieczeństwa. Rozwiązania open source to dla większości rozpoczynających sprzedaż online naturalny wybór. Warto jednak pamiętać, że kod źródłowy tych platform jest upubliczniony, tym samym hakerzy mają ułatwiony dostęp do potencjalnych „luk" w oprogramowaniu.

Typ incydentu	Liczba incydentów	%
Atak na bezpieczeństwo informacji	45	2,34
Dostępność zasobów	45	2,34
Oszustwa komputerowe	1069	55,5
Złośliwe oprogramowanie	211	10,69
Włamania	54	2,8
Próby włamań	109	5,66
Gromadzenie informacji	65	3,37

Źródło: Raport CERT „Polska Krajobraz bezpieczeństwa polskiego Internetu 2016 r"

Analizy światowego rynku przeprowadzone przez firmę BuildWith pokazują, że najwięcej e-sklepów działa w oparciu o WooCommerce. Wtyczka WordPressa jest ponad 8 razy bardziej popularna niż Magento czy Shopify, które wspólnie dzielą tytuł drugiej w kolejności najpopularniejszej platformy e-commerce.[1] Główne powody popularności wtyczki WooCommerce to niski koszt, łatwa konfiguracja i wysokie bezpieczeństwo. To ostatnie spełnione tylko we współpracy z użytkownikiem. Jak działają hakerzy? Próbują złamać zabezpieczenia i przejąć dostęp do panelu administracyjnego. Sprawdzają bezpieczeństwo serwera oraz to w jaki sposób przechowywane są dane, usiłując uzyskać dostęp do plików tymczasowych bądź plików użytkowników. Pierwszym przykazaniem e-sprzedawcy dbającego o bezpieczeństwo jest ciągła aktualizacja. Aby zminimalizować ryzyko warto sprawdzić czy dane oprogramowanie jest na bieżąco rozwijane.



Źródło: https://trends.builtwith.com/shop/WooCommerce

W 2016 roku cyberprzestępcy wyłudzili ponad

1 mln dolarów

za pomocą ataku ransomware. Gangsterskie działania tego typu, polegają na blokowaniu dostępu do danych i żądania okupu za ich przywrócenie.

53% sklepów internetowych doświadczyło cyberataku

* www.greywizard.com

[1] W Katie Keitch, How Many Websites Use WooCommerce? Usage Stats 2017,[online] << https://barn2.co.uk/woocommerce-stats/>>

Ochrona antywirusowa

Opracowane we współpracy z Marken Systemy Antywirusowe, oficjalnym dystrybutorem produktów Bitdefender w Polsce

Bitdefender

Wraz z rozwojem Internetu rozpowszechniły się również technologie, które umożliwiają szeroki dostęp praktycznie każdemu użytkownikowi do zasobów sieciowych. Jedną z funkcjonalności, która jest dziś w dużej mierze wykorzystywana przez użytkowników, jest handel w sieci. Począwszy od dużych firm, które prowadzą rozbudowane sklepy internetowe, po prywatnych użytkowników sprzedających i kupujących towary na aukcjach internetowych. Handel w sieci wiąże się oczywiście z płatnościami online. I tutaj właśnie użytkownik danego sklepu lub portalu aukcyjnego narażony jest na największe niebezpieczeństwo utraty nie tylko danych, ale również swoich oszczędności. Od szkodliwego oprogramowania, które może przechwycić dane logowania użytkownika do kont bankowych, aż po różnego rodzaju pułapki, jak np. **strony podszywające się pod bankowe**.

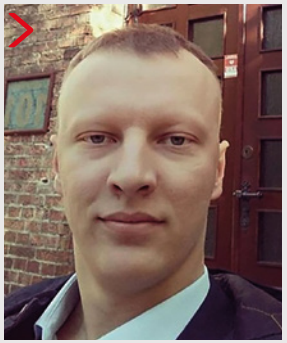
Każdego dnia wielu użytkowników na świecie zupełnie nieświadomie wpisuje swoje dane logowania do banków, bez uprzedniego sprawdzenia autentyczności strony, na której przebywają. Często w wyniku takiego działania użytkownik narażony jest na utratę swoich dóbr, a jego dane personalne mogą zostać wykorzystane w celu dokonania przestępstwa. Rozwój sieci wymusił na firmach zajmujących się bezpieczeństwem stworzenie wyspecjalizowanego oprogramowania, którego zadaniem jest pomoc użytkownikom w ochronie swoich danych. Powstały przydatne funkcje, takie jak zabezpieczenie płatności elektronicznych, czy ochrona samej przeglądarki np. przed pobraniem niebezpiecznego oprogramowania (mogącego wyłudzić konkretne dane) i sprawdzenie strony WWW pod kątem bezpieczeństwa (czy np. nie znajdują się na niej niebezpieczne skrypty).

Dzięki takim technikom użytkownicy mogą czuć się bezpieczniej podczas zdalnych zakupów w Internecie. Warto też zauważyć, że same sklepy i portale internetowe z aukcjami też powinny dbać o bezpieczeństwo swoich klientów. Odpowiednio częste sprawdzanie bezpieczeństwa takich stron jest kluczowe dla reputacji danej firmy. Trzeba pamiętać, że głównym celem ataków są nasze pieniądze. Dotyczy to w równej mierze firm, jaki i zwykłych użytkowników.

Nowe rodzaje ataków i przechwytywania informacji sprawiają, że producenci programów antywirusowych wprowadzają i nieustannie rozwijają technologie umożliwiające coraz lepsze zabezpieczenie użytkowników. Niestety, nawet najnowocześniejsza technologia nie zastąpi zdrowego rozsądku i w dużej mierze to od nas zależy na jakie niebezpieczeństwa każdego dnia się narażamy.

W 93% przypadków potrzeba mniej niż 60 sekund na przeprowadzenie ataku.

* 2016 Data Breach Investigations Report



Temat ochrony antywirusowej przybliża rozmowa przeprowadzona z Mariuszem Osińskim, Inżynierem Technicznym w Bitdefender.

„Musimy przygotować się również na ataki na wielu frontach – nasze smartfony są na celowniku"

Mariusz Osiński
inżynier techniczny w Bitdefender

Kei.pl **Co sądzi Pan o rozwiązaniach typu open source w branży e-commerce?**

Mariusz Osiński: *Jeśli chodzi o oprogramowanie, to mogę powiedzieć jak to wygląda w przypadku zabezpieczeń. Zaryzykowałbym jednak stwierdzenie, że funkcjonuje to na podobnej zasadzie również w innych obszarach.*

Ciężko generalizować, ale software zabezpieczający typu open source przeważnie sprowadza się do podstawowej ochrony i nie zapewnia odpowiednich technologii wykrywania ukierunkowanych ataków. Niestety, często też okazuje się, że skuteczność tego typu rozwiązań jest wielce wątpliwa, pomimo zapewnień ze strony twórców.

Trzeba pamiętać, że za zamkniętym oprogramowaniem komercyjnym stoi sztab ludzi – przeważnie bardzo dobrze wykwalifikowanych – którzy odpowiadają nie tylko za stworzenie softu, ale także za jego ulepszenia i wprowadzanie poprawek na bieżąco. Można również oczekiwać od nich pełnego wsparcia technicznego. Czy to samo możemy zawsze powiedzieć o rozwiązaniach typu open source?

Otwarte oprogramowanie niesie ze sobą szereg niebezpieczeństw i choć nie jest to regułą, warto każdorazowo zbadać temat i mieć pewność, że nasz biznes będzie bezpieczny. Ostatnia rzecz, o którą chcemy się każdego dnia martwić to bezpieczeństwo naszej firmy i jej klientów. A w związku z rychłym zaostrzeniem przepisów odnośnie bezpieczeństwa danych osobowych – nie warto ryzykować swojej reputacji i finansów.

Kei.pl **Rok 2017 upłynął pod znakiem ataków typu ransomware. Wystarczy wspomnieć WannaCry czy Petya. Czy możemy spodziewać się kolejnej fali ataków?**

Mariusz Osiński *Niestety tak. Przewiduje się, że ataki typu ransomware nasilą się jeszcze bardziej. Musimy brać pod uwagę fakt,*

że coraz więcej osób jest dziś online. Dotyczy to zarówno indywidualnych użytkowników, jak i biznesów. Prawie każdy ma dziś konto bankowe i coraz więcej pracy wykonujemy na komputerach lub telefonach, przechowując tam mnóstwo danych.

Ataki typu ransomware są ukierunkowane na zdobywanie pieniędzy. A gdzie użytkownicy, ich dane i potencjalny zarobek – tam i hakerzy. Nie warto łudzić się, że ktoś pozyskujący pieniądze w ten sposób zrezygnuje z tworzenia szkodliwego oprogramowania. Musimy przygotować się również na ataki na wielu frontach – nasze smartfony są na celowniku.

Kei.pl **Dlaczego phishing działa i jak go uniknąć?**

Mariusz Osiński *Phisihing to specyficzna forma wyłudzania informacji lub pieniędzy. Niestety głównym problemem jest tutaj użytkownik, który ślepo wierzy, że to co widzi na ekranie jest autentyczne. Lepiej dwa razy zastanowić się zanim klikniemy w link lub wpiszemy gdzieś swoje dane logowania, bo może się okazać, że trafiliśmy na podrobioną stronę.*

Programy zabezpieczające oczywiście pomagają w wykrywaniu tego typu zagrożeń, ale to sam użytkownik powinien ostrożniej podchodzić do operacji, które wykonuje na swoich urządzeniach.

Przede wszystkim należy zachować czujność i sprawdzać podstawowe informacje o stronach, na których dokonujemy operacji (certyfikaty, poprawność adresów w przeglądarce, etc).

Kei.pl **Firewall, IDS i możliwość filtrowania stron internetowych ochronią przed zagrożeniami internetowymi typu włamania i phishing?**

Mariusz Osiński *Do tego typu filtrowania służą raczej moduły rozwiązań zabezpieczających, które integrują się z przeglądarkami internetowymi. Mają one mechanizmy weryfikujące kod na stronach i technologie sprawdzania reputacji w chmurze. Jednak nawet najprostsze zabezpieczenie, wyposażone w klasycznego firewalla może okazać się na wagę złota. Jeśli wpadniemy w pułapkę, może nas ono ocalić przed poważnymi konsekwencjami.*

Kei.pl **Czy odpowiedni antywirus może zoptymalizować prędkość i wydajność na platformach?**

Mariusz Osiński *Oprogramowanie zabezpieczające zdecydowanie nie wpływa na podniesienie wydajności platform, bo nie do tego ono służy. Niektóre rozwiązania mogą wręcz nam tę prędkość działania zmniejszyć, więc warto poszukać software'u, które w testach wykazuje minimalny wpływ na wydajność. Nadrzędnym celem programu zabezpieczającego jest wykorzystanie zasobów sprzętowo-systemowych do jak najlepszej ochrony środowisk, na których pracuje. Oczywiście, cały czas trwają prace nad rozwojem technologii, które będą skuteczniejsze w wykrywaniu obecnie występujących zagrożeń, jednocześnie minimalizując zasoby do tego potrzebne. Każdego dnia słyszy się o nowych zagrożeniach, więc specjaliści ds. zabezpieczeń w ostatnich latach działają coraz intensywniej, poszukując rozwiązań i odpowiadając na potrzeby użytkowników, chroniąc ich sprzęt, czas oraz pieniądze.*

Rozmawiała
Ilona Kuźniarz
Kei.pl

Komu zagrażają ataki DDoS?

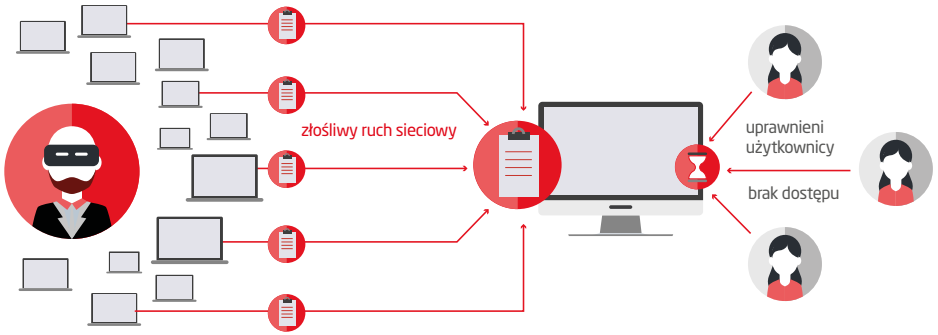
Opracowane we współpracy z Atende Software Sp. z o.o.

ATENDE SOFTWARE

Problematyka bezpieczeństwa w cyberprzestrzeni przestaje być tylko domeną rządów i administracji publicznej. Coraz częściej cyberataki dotykają również małego i średniego biznesu, a ich podłożem staje się szantaż, czy nieuczciwa konkurencja. Paraliż infrastruktury informatycznej przekłada się na realne straty finansowe i wizerunkowe, szczególnie w sektorze e-commerce.

Ostatnie lata przyniosły szczególnie duże nasilenie jednego z typów ataków, określanego mianem DDoS (*distributed denial of service*). Atak ten polega, w dużym uproszczeniu, na „zalewaniu" łączy internetowych i serwerów ofiary setkami milionów przypadkowych pakietów. Celem atakującego jest wysycenie łącza internetowego, co w konsekwencji prowadzi do odcięcia atakowanego podmiotu od Internetu.

Ataki DDoS są prowadzone z różnych powodów – początkowo miały podłoże ideologiczne i polityczne, jednak na przestrzeni ostatnich lat obserwowana jest postępująca „komercjalizacja" tej branży. Grupy przestępcze utrzymują



serwisy internetowe, przez specjalistów określone mianem CaaS (crime as a service), które po uiszczeniu niewielkiej opłaty, zazwyczaj nieprzekraczającej kilkunastu dolarów miesięcznie, dają dostęp do botnetów, złożonych z setek tysięcy zainfekowanych komputerów czy urządzeń IoT (np. kamer internetowych). Użytkownik takiego serwisu, właściwie jednym kliknięciem może uruchomić atak, który zdewastuje infrastrukturę teleinformatyczną ofiary. Rozpowszechnienie ataków DDoS wynika z ich wysokiej skuteczności.

Najmniejsze obserwowane obecnie ataki bez problemu przekraczają poziom kilku gigabitów na sekundę, a te największe, obserwowane w 2016 i 2017 r. – osiągają poziom nawet 1200 gigabitów na sekundę.

Z perspektywy małej czy średniej firmy można założyć, że praktycznie każdy atak DDoS znacząco przekracza pojemność typowego łącza internetowego.

Skuteczna ochrona przed atakami DDoS najczęściej wymaga współpracy ze specjalistycznymi podmiotami, które dysponują technologią, umożliwiającą efektywne analizowanie i filtrowanie ruchu sieciowego oraz odpowiednią pojemnością łączy internetowych. Coraz częściej tego typu technologia jest wykorzystywana przez operatorów hostingu. W ten sposób są między innymi chronione zasoby należące do firmy Kei.pl, która wykorzystuje oprogramowanie redGuardian, stworzone przez rodzimą firmę Atende Software. Oprogramowanie to umożliwia bardzo wydajne przetwarzanie ruchu sieciowego na standardowych serwerach klasy PC – w praktyce możliwe jest osiągnięcie poziomu ponad 100 milionów pakietów na sekundę na pojedynczym serwerze. Jest to poziom wydajności do tej pory zarezerwowany dla platform opartych o układy FPGA lub ASIC. Stało się to możliwe dzięki wykorzystaniu technologii dostępnych w najnowszych procesorach Intel (DDIO – data direct I/O, CAT – cache allocation technology). Odbierane pakiety oraz istotne dane (np. listy adresów IP) są ładowane bezpośrednio do pamięci podręcznej procesora, z pominięciem pamięci operacyjnej, a operacje na pakietach sieciowych są wykonywane przy pomocy instrukcji wektorowych AVX2.

Dzięki redGuardian, klienci chronieni są przed praktycznie wszystkimi atakami DDoS, w tym tymi najbardziej uciążliwymi, wykorzystującymi protokoły:

- NTP
- DNS
- SSDP

Rozwiązanie ponadto implementuje mechanizmy stanowe, które umożliwiają mitygację ataków typu TCP flood (SYN, ACK). Możliwa jest również ewaluacja zawartości pakietów z wykorzystaniem wyrażeń regularnych.

Można powiedzieć, że ochrona przed atakami DDoS działa trochę jak polisa ubezpieczeniowa – zwykle się o niej nie myśli, ale w sytuacji kryzysowej staje się bardzo potrzebna. Dlatego lepiej zawczasu się przygotować.

Przestój w e-commerce kosztuje. E-sprzedawca traci pieniądze za każdym razem, gdy klienci nie mają dostępu do sklepu internetowego. Co gorsza, kupujący mają tendencję do zapamiętywania złych wrażeń w kontakcie ze stroną WWW. Problemy jakie napotkają przy zakupie nie zachęcą do powrotu przy kolejnym buszowaniu w sieci. Tacy klienci mogą nawet udać się wprost na witrynę konkurencyjnej firmy. Kupujący nie wiedzą o tym, co dzieje się za kulisami, wiedzą tylko, że witryna jest wyłączona lub działa bardzo wolno – dlatego uciekają.

W kontekście ukierunkowanych ataków, warto pamiętać, że zaufanie klienta to konwersje. Ataki DDoS powodują przede wszystkim pogorszenie komfortu użytkownika poruszającego się po sklepie, ale mogą być także zasłoną dymną dla innych szkodliwych działań. Zabezpieczenie się przed atakiem może ochronić DDoS przed kolejnymi naruszeniami, takimi jak kradzież danych klientów.

Przemysław Frasunek
Dyrektor Działu Rozwiązań Multimedialnych i Działu Systemów Bezpieczeństwa w Atende Software.

Polski haker. Absolwent Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych. Od 1999 roku pasjonat zagadnień związanych z bezpieczeństwem teleinformatycznym oraz autor ponad 40 raportów o błędach w powszechnie używanym oprogramowaniu. Lider kilkudziesięciu audytów bezpieczeństwa oraz autor cyklu szkoleń z zakresu bezpieczeństwa systemów i aplikacji.

Ochrona danych osobowych klienta

Opracowane we współpracy z Mastela Wałecki i Partnerzy Kancelaria Radców Prawnych

KANCELARIA RADCÓW PRAWNYCH
MASTELA • WAŁECKI • PARTNERZY

W dzisiejszym e-commersowym świecie cyfrowe dane klientów wymagają należytej ochrony. Hakerzy atakując e-sklep ukierunkowują się głównie na bazy danych użytkowników (nazwiska, adresy, telefony), które następnie wykorzystują do własnych celów bądź sprzedają na czarnym rynku.

Jak stosować zasady przechowywania i ochrony danych osobowych?

Pomimo sporego nagłośnienia w mediach wielu przedsiębiorców nadal nie dostosowało się do nadchodzących zmian przepisów w zakresie ochrony danych osobowych. Przedsiębiorcy działający w branży e-commerce są szczególnie narażeni na negatywne konsekwencje związane zarówno z kontrolą organu nadzoru, jak i roszczeniami klientów, gdyż właśnie na nich ze względu na korzystanie z serwisów internetowych, a zwłaszcza wszelkiego rodzaju formularzy online ciąży więcej obowiązków związanych z prawem do ochrony danych osobowych niż na tzw. przedsiębiorcy stacjonarnym. Co więcej, stosowane przez nich niezgodne z prawem praktyki ze względu na łatwą i szeroką dostępność (Internet) jest dużo łatwiejsza do wychwycenia.

Właściciele e-sklepów często błędnie zakładają, iż problem ochrony danych osobowych (dalej: DO) nie dotyczy prowadzonego przez nich biznesu. Wynika to z braku wiedzy na temat tego czym jest przetwarzanie DO lub też błędnego przekonania, że prawdopodobieństwo, że grożą im negatywne konsekwencje jest nikłe. Tymczasem każdy przedsiębiorca, który przetwarza (czyli m.in. gromadzi, usuwa, przechowuje, modyfikuje) DO ma obowiązek ich legalnego przetwarzania oraz ochrony przed nieupoważnionym dostępem, usunięciem lub modyfikacją poprzez zastosowanie odpowiednich zabezpieczeń natury organizacyjnej oraz technicznej i wdrożenie stosownych rozwiązań.

E-commerce jest nieodłącznie związany z przetwarzaniem DO, prowadząc tego typu biznes przetwarzamy m.in. takie DO jak:

- imię i nazwisko klienta,
- adres email,
- adres dostawy,
- numer telefonu,
- numer rachunku bankowego.

Zresztą w obecnie obowiązującej ustawie o świadczeniu usług drogą elektroniczną mamy cały rozdział 4 poświęcony właśnie przetwarzaniu DO. Właściciele serwisów internetowych świadcząc usługi elektroniczne wykorzystują dopasowane do specyfiki ich działalności regulaminy świadczenia usług drogą elektroniczną. Kwestia spełnienia obowiązków informacyjnych wobec swoich klientów w zakresie ochrony danych osobowych może zostać włączona do takiego regulaminu, aczkolwiek nie musi – można stworzyć oddzielny dokument.

Polityka prywatności i regulaminu serwisu

Decyzja w tym temacie powinna zostać podjęta w zależności od długości i skomplikowania regulaminu. Adresując swoje usługi do konsumentów musimy pamiętać o tym aby stosować jasny i zrozumiały przekaz, który musi jednak spełniać warunki wynikające z przepisów prawa, w tym przepisów dotyczących ochrony danych osobowych. Stąd niekiedy łączenie zbyt wielu aspektów w jednym dokumencie może być zbyt nieczytelne. Dodatkowo warto zwrócić uwagę, że wielu przedsiębiorców

niepotrzebnie wymaga od klientów zgody na przetwarzanie danych osobowych w celu realizacji umowy o świadczenie usług, podczas gdy powinni tylko dopełnić wobec klientów obowiązków informacyjnych (jeśli klient chce skorzystać z naszych usług to pewne dane są niezbędne dla realizacji umowy i w tym wypadku żadna dodatkowa zgoda nie jest potrzebna, a wręcz jest niewskazana). Co innego oczywiście gdy w ramach realizacji zlecenia przedsiębiorca chce uzyskać od klienta zgodę na przesyłanie informacji handlowych, np. w formie newslettera.

Wpływ RODO na branżę e-commerce

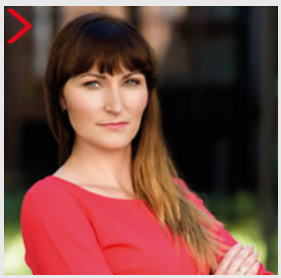
W świetle art. 13 mającego zastosowanie od 25 maja 2018 r. RODO[1] jeżeli przedsiębiorca zbiera dane osobowe od osoby, której dane dotyczą podczas pozyskiwania danych (czyli np. poprzez znajdujący się na stronie WWW formularz zamówienia lub formularz kontaktowy) zobowiązany jest do podania m.in. następujących informacji:

- swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela;
- celów przetwarzania DO, oraz podstawy prawnej przetwarzania;
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców;
- o okresie, przez który DO będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacji o prawie do żądania od administratora dostępu do DO dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- w niektórych przypadkach – informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- informacji o prawie wniesienia skargi do organu nadzorczego;
- informacji, czy podanie DO jest wymogiem ustawowym, umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

Aby legalnie przetwarzać DO, w tym zabezpieczyć się zarówno przed odpowiedzialnością administracyjną w postaci m.in. (ale nie tylko) wysokich sankcji finansowych, jak i

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);

roszczeń klientów (w tym odszkodowawczych, a związanych z naruszeniem ich prawa do legalnego przetwarzania DO) konieczne jest m.in. właściwe sformułowanie dokumentu, którego akceptacja przez klienta będzie warunkowała możliwość przesłania uzupełnionego formularza (czy to kontaktowego, czy też dot. zamówienia). Niestety kwestia spełnienia obowiązków informacyjnych na portalu internetowym to tylko jeden z istotnych elementów legalnego przetwarzania danych osobowych. Adaptacja do wymagań stawianych przez RODO nie jest rzeczą ani łatwą, ani tanią oraz niejednokrotnie wymaga pomocy profesjonalistów z dziedziny prawa i bezpieczeństwa IT. W świetle grożących przedsiębiorcy sankcji, w tym także w zakresie PR-u należy uznać, że adaptacja ta jest jednak niezbędna, co każdy przedsiębiorca powinien mieć na uwadze.



Barbara Kubala-Zielińska
Kancelaria Radców Prawnych
Mastela Wałecki Partnerzy

Radca prawny. Specjalizuje się w doradztwie z zakresu kontraktów handlowych i umów w obrocie gospodarczym. Zaangażowana w sprawy związane z obsługą bieżącą podmiotów gospodarczych, zwłaszcza w zakresie stosunków B2B, ze szczególnym uwzględnieniem prawa ochrony danych osobowych i specyfiki e-commerce (świadczenia usług drogą elektroniczną). Interesuje się szeroko rozumianym prawem gospodarczym, w tym prawem Unii Europejskiej oraz polityką zarządzania zasobami ludzkimi. W Kancelarii pełni też rolę PR Managera.

Certyfikaty SSL, szyfrowane bezpieczeństwo

Opracowane we współpracy z //CertyfikatySSL.pl

„Certyfikaty SSL to standard w branży e-commerce" – pomimo, że pod takim stwierdzeniem podpisze się większa część e-sprzedawców, w sieci nie brakuje serwisów wyłamujących się z tej ogólnoświatowej tendencji. Kierunek w kwestii szyfrowanego połączenia narzucają nie tylko wielkie platformy (eBay, Amazon), ale też coraz bardziej świadomi klienci. Czujność konsumentów potwierdzają statystyki. Brak protokołu HTTPS zniechęca klienta na ostatnim etapie procesu zakupowego. Aż 15% internautów nie finalizuje zakupów ze względu na obawę o bezpieczeństwo płatności.[1]

Według nowej polityki Google szyfrowany protokół wymagany jest nie tylko od serwisów z płatnościami, ale też wszystkich stron gromadzących dane klientów, np. za pośrednictwem formularza kontaktowego. Najpopularniejsze przeglądarki, takie jak Firefox czy Chrome wysyłają jasny komunikat: „Twoje połącznie z witryną nie jest bezpieczne". Po takim ostrzeżeniu klient z pewnością zrezygnuje z dalszego serfowania po stronie, a swoje poszukiwania sfinalizuje na stronie konkurencji. 72% ankietowanych przyznało, że zamknęło kartę strony, która wydała im się niebezpieczna, jednocześnie 92% z nich zadeklarowało, że nie opuściłoby strony wyposażonej w certyfikat SSL.[2]

Serwisy, które wdrożyły certyfikaty SSL odnotowały wzrost liczby rejestracji nowych użytkowników do

87%

Jednocześnie konwersja ze sprzedaży wzrosła do

30%

* badania Symantec

[1] *VWO eCommerce. Cart Abandonment Report 2016*

[2] Badania TNS Research

Zaufanie w przestrzeni online

Troska o bezpieczeństwo klienta w połączeniu z atrakcyjną ceną i dopasowaną strategią przekładają się na sukces sprzedażowy. Warto pamiętać, że agresywne działania promocyjne przyciągną klienta, ale do wypracowania długotrwałej relacji potrzeba czegoś więcej. Znaczna część użytkowników zrażonych negatywnymi doświadczeniami wybiera wyłącznie bezpieczne połączenia i sprawdzone źródła. W sieci jest pełno naciągaczy. W obronie przed oszustami klienci coraz częściej podejmują wysiłek weryfikacji i sprawdzają podstawowe dane rejestrowe. Przedsiębiorca nastawiony na efektywny e-biznes, musi liczyć się z koniecznością ujawnienia nazwiska, numeru NIP czy adresu siedziby sklepu. Automatycznym potwierdzeniem weryfikacji danych są certyfikaty SSL o wyższym poziomie walidacji OV (Organization Validation) i EV (Extended Validation). Informacje zawarte w pasku strony są dla użytkownika potwierdzeniem co do wiarygodności domeny, a także autentyczności danych właściciela.

Rodzaje walidacji

to najprostszy z certyfikatów wydawany w oparciu o potwierdzenie własności domeny. Procedura może polegać na wysłaniu wiadomości autoryzacyjnej na adres e-mail w danej domenie.

- **DV (domain validation)**

to najprostszy z certyfikatów wydawany w oparciu o potwierdzenie własności domeny. Procedura może polegać na wysłaniu wiadomości autoryzacyjnej na adres e-mail w danej domenie.

- **OV (organization validation)**

to certyfikaty, których wystawienie poprzedzone jest weryfikacją podmiotu ubiegającego się o wydanie certyfikatu SSL, prawa do używania danej domeny, oraz weryfikacją telefoniczną osoby reprezentującej daną organizację.

- **EV (extended validation)**

to najwyższy poziom walidacji. Wydanie certyfikatu poprzedzone jest złożeniem wniosku do Urzędu Certyfikacji, które potwierdzają własność domeny oraz wiarygodność podmiotu.

Typy certyfikatów SSL

Certyfikaty można podzielić nie tylko ze względu na rodzaj walidacji, ale także liczbę domen, które mają obsłużyć i typ oprogramowania, które mają zabezpieczać.

- **Certyfikaty Wildcard**

Pozwalają chronić nieograniczoną liczbę subdomen w domenie głównej, przy wykorzystaniu jednego certyfikatu SSL. Przykładowo jednocześnie chronią przyklad.pl, panel.przyklad.pl, blog.przyklad.pl, etc.

- **Certyfikaty Multi-domain**

Pozwalają zabezpieczyć nawet 250 stron internetowych pod różnymi adresami www za pomocą jednego certyfikatu. Przykładowo jednocześnie chronią przyklad1.pl, przyklad2.com, etc.

- **Code Signing**

Podobnie jak stronę www, można zabezpieczyć też oprogramowanie. Do tego celu służą certyfikaty Code Signing. Potwierdzają one autentyczność wydawcy, gwarantują integralność zawartości, zabezpieczają oprogramowanie przed manipulacją, zabezpieczają kanał dystrybucji, zapobiegają ostrzeżeniom przy pobieraniu i instalacji oprogramowania.

- **Certyfikaty e-mail (S/MIME)**

Do zabezpieczenia poczty elektronicznej służą certyfikaty e-mail, które zapewniają ochronę poprzez dodanie cyfrowego podpisu oraz szyfrowanie wiadomości i przesyłanych załączników. Certyfikaty e-mail chronią przed podszywaniem się pod nadawcę, „podsłuchiwaniem", kradzieżą danych zawartych w e-mailu, fałszowaniem wiadomości lub załączników.

Prowadzisz sklep internetowy?

- Zainstaluj certyfikat SSL, podczas konfiguracji wybierz klucz 2048-bitowy.
- Włącz mechanizm HSTS informujący przeglądarkę, że przy otwieraniu stron ma automatycznie używać protokołu HTTPS.
- Zabezpiecz serwisy działające w subdomenach lub osobnych domenach certyfikatami WildCard i MultiDomain.
- Pamiętaj o przedłużeniu certyfikatu na kolejny okres abonamentowy.

pamiętaj!

Ela Kornaś,
Dyrektor Marki Domeny.pl/
Certyfikatyssl.pl

W dyskusjach na temat branży e-commerce trudno pominąć kwestię certyfikatów SSL. Nikt przecież nie chce „zabłysnąć" w mediach jako serwis, z którego wyciekły wrażliwe dane klientów. Szyfrowanie SSL często porównuje się do klucza i sejfu, ale protokół HTTPS to coś więcej. Klucz, sejf, a w nim informacje, których nie sposób odczytać. To także gwarancja skuteczności sięgająca $1.000.000. Dzięki certyfikatom zaszyfrowane dane nie mają wartości. Nawet jeśli zostaną wykradzione, stają się bezużyteczne dla cyberprzestępców.

Mówiąc językiem technicznym, każda sesja SSL składa się z dwóch kluczy: klucza publicznego, który szyfruje oraz prywatnego, który odszyfrowuje. Kiedy internauta używa przeglądarki, aby połączyć się z zabezpieczoną stroną WWW, następuje uzgadnianie SSL na linii przeglądarka - serwer. Wysyłane jest żądanie do serwera, zmienia się wygląd paska adresu (zielony pasek, kłódka). Dla sesji przeglądania strony internetowej ustanawiane jest bezpieczne połączenie z unikalnym kluczem. Zaczyna się bezpieczna transmisja danych.

Socjotechnika,

czyli o sztuce podstępu

Ochrona danych osobowych klientów, infrastruktury czy poufnych danych nie jest możliwa bez synergii działań. Na bezpieczeństwo danych klientów e-sklepów składają się rozwiązania techniczne, a także odpowiednio przeszkolony personel. Priorytetem w działaniach specjalistów od bezpieczeństwa jest edukowanie pracowników. Osoba, która na co dzień pracuje z dużą ilością danych może doprowadzić do ich wycieku przez zwykłe zaniedbanie. Aby zminimalizować ryzyko niezwykle ważne jest stworzenie wewnętrznych procedur związanych z bezpieczeństwem. To obowiązek nie tylko korporacyjny, ale istotna kwestia dla nawet małych e-commersowych biznesów.

>> **Inżynieria społeczna** – prawa i teorie socjologiczne w praktyce. Metaforycznie określana jako sztuka sterowania ludźmi. Cyberprzestępcy wykorzystują te metody w celu dotarcia do poufnych informacji. Inżynieria społeczna stosowana jest także przez handlowców jako sposób dotarcia bezpośrednio do osób decyzyjnych.

22% firm utraciło klientów wskutek ataku hakerskiego

* Cisco Annual Cybersecurity Report

Człowiek najsłabszym ogniwem? Niestety w kwestii cyberbezpieczeństwa organizacji tak. Hakerzy nie zawsze korzystają z zaawansowanych technologii. Należy pamiętać, że luki w wewnętrznych procesach są równie często wykorzystywane do sabotażu. Dobry haker nie skupia swoich działań na sprzęcie, a doskonale manipuluje ludźmi. Za każdym kierowanym na platformę atakiem stoi człowiek, który poza technologią wykorzystuje narzędzia inżynierii społecznej. Hakerzy stosują sztuczki socjotechniczne także po zainfekowaniu komputera by zmusić osobę do opłacenia okupu. Wykorzystują wizualizację z odliczaniem i upływającym czasem w celu podkreślenia niepokoju i niepewności. Posługują się mrocznymi nazwami zaciągniętymi z popkultury.

Reguła ograniczonego zaufania
Sztuczki socjotechniczne otwierają drogę do obejścia zaawansowanych systemów. Wiedza handlowca czy pracownika biura obsługi klienta w obszarze zagadnień IT i bezpieczeństwa sieciowego najczęściej jest ograniczona. Jednocześnie osoby te mają dostęp do szeregu poufnych danych klientów.

Ważna jest organizacja pracy personelu. W kwestii osoby zarządzającej bezpieczeństwem jest posiadanie dostępów przez pracowników wyłącznie do danych, które są mu potrzebne do pracy. Konto administratora w sklepie internetowym to dostęp do wszystkich zasobów. Z tego poziomu możemy wykonać jak najwięcej modyfikacji. Użytkownik nie powinien mieć uprawnień administratora ani dostępu do zasobów sieciowych, z których nie korzysta w codziennej pracy. Ograniczenia uprawnień minimalizują ryzyko błędów i omyłkowych wycieków danych. Atak na nieuświadomionego pracownika najczęściej odbywa się przy użyciu poczty elektronicznej z wykorzystaniem załączenia złośliwego kodu.

Firmowy CRM, program rozliczeniowo-księgowy, dysk online – dostęp do tych narzędzi powinien być ograniczony. W sprawnym regulowaniu tej kwestii pomaga wykorzystanie szyfrowanych łączy, czyli VPN (ang. *Virtual Private Network*).

VPN to sieć prywatna tworząca pewnego rodzaju tunel odizolowany od publicznej sieci (np. sieci internetowej), który jednocześnie pozwala na wymianę ruchu sieciowego.

Dzięki temu połączenie np. z systemem zarządzającym firmową bazą klientów czy firmowym serwerem WWW mogą nawiązać tylko pracownicy – zarówno w ramach pracy w biurze firmy jak i pracy zdalnej. Bezpieczeństwo sieci VPN opiera się na trzech głównych filarach:

- uwierzytelnieniu
- autoryzacji
- szyfrowaniu

Prognozy ekspertów na 2018 rok wskazują, że nowe zagrożenia w świecie bezpieczeństwa online będą celowane właśnie w użytkowników.

„Aby zwiększyć bezpieczeństwo połączenia VPN można zastosować różne metody autoryzacji, znane przede wszystkim z bankowości elektronicznej – tokeny, karty kodów jednorazowych czy hasła SMS."

Grzegorz Pawelec,
Dyrektor Pionu Biznesu
Kei.pl

Celem ataku nie jest komputer sam w sobie. Atakowany jest jego użytkownik. Utarło się powiedzenie, że najwięksi hakerzy świata nie łamią kodu - łamią ludzi. W istocie niektóre z informacji udało się wyciągnąć po prostu poprzez telefoniczną rozmowę z pracownikiem. Haker zadzwonił, zapytał, uzyskał odpowiedź.

Najlepszą bronią w walce z hakerami działającymi w oparciu o techniki inżynierii społecznej są wiedza i ograniczone zaufanie.

Kampanie phishingowe opierają się na atakach ransomware, które w 70% przypadkach rozpowszechniane są w postaci załącznika bądź linku w wiadomości e-mail. Każdy przekaz odnośnie bezpieczeństwa danych w e-commerce rozpoczyna problem odpowiedniego edukowania pracowników. Prowadzenie szkoleń i odpowiedniego systemu ochrony danych minimalizuje zagrożenie.

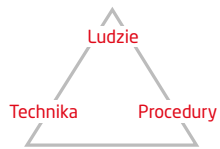
Spam czy wiadomość biznesowa?

Odpowiedź na to pytanie nie zawsze jest oczywista. Przesyłane wiadomości e-mail stają się coraz bardziej dopracowane. Najczęściej samo otwarcie pliku załączonego do maila powoduje zainfekowanie komputera złośliwym

Spear phishing – rodzaj phishingu o bardziej ukierunkowanym charakterze. Personalizacja wiadomości wywołuje u użytkownika wrażenie, że zna adresata – prywatną osobę bądź instytucję. Treść takich wiadomości odwołuje się do osobistych informacji czy wspólnego znajomego. Podszywanie się pod znajomych ma na celu np. wyłudzenie haseł.

Źródło: https://www.facebook.com/AliorBankSA/

Bezpieczeństwo w cyberprzestrzeni:



oprogramowaniem. Eksperyment przeprowadzony przez firmę F-Secure pokazuje, że 52% pracowników, którzy otrzymali sfałszowanego maila stylizowanego na wiadomość z portalu LinkedIn kliknęło w link.[1] Cyberprzestępcy liczą na nieuwagę osób po drugiej stronie monitora. Podszywając się pod operatorów telekomunikacyjnych wyłudzają pieniądze i dane. Maile które otrzymują użytkownicy wyglądają wiarygodnie. Zawierają logo firm, często Allegro, Poczty Polskiej, PayPal. Treść w mailach stosunkowo niewiele różni się od oryginalnych, a w załącznikach znajdują się rzekome faktury od operatorów telekomunikacyjnych.

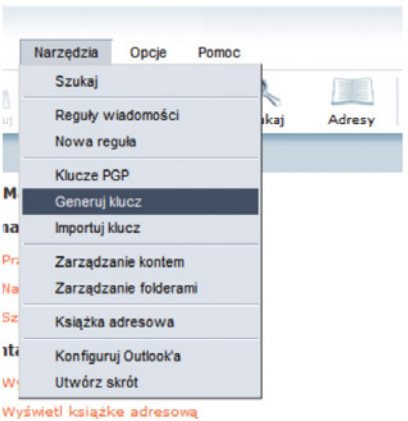
Zaszyfrowana wiadomość e-mail?

Można szyfrować prościej. Wystarczy skorzystać z usług dostawcy hostingu, który oferuje możliwość szyfrowania wiadomości e-mail w standardzie. Centrum Danych Kei.pl posiada autorski panel WebMail, który poza standardową obsługą skrzynki oferuje możliwość generowania kluczy szyfrujących (PGP). Generowane klucze mogą być zabezpieczone hasłem. Ich ważność może być bezterminowa lub wynosić określoną liczbę dni. Oczywiście za pomocą WebMaila można także wysyłać i odbierać szyfrowane wiadomości.

[1] R F-Secure: wielu zagrożeń można uniknąć [w:] Dane w przedsiębiorstwie. Zarządzanie i ochrona, CRN 2017, nr 4.

Głównym sposobem na odkrycie oszustwa jest czujność i wysoka podejrzliwość w stosunku do wszystkich przesyłek, także tych oczekiwanych, przychodzących pocztą elektroniczną.

Z każdym dniem możemy spodziewać się coraz lepiej opracowanej próby oszustwa. Ważne by aktualizować wiedzę pracowników. Część firm wykorzystuje firmy zewnętrzne do przeprowadzenia testów bezpieczeństwa. Firmy przeprowadzają kontrolowany atak w oparciu o inżynierię społeczną, w celu wskazania niezabezpieczonych aspektów w strukturze.



Richard Ku, wiceprezes firmy Trend Micro w rozmowie z agencją informacyjną Newseria wskazuje, że skala cyberprzestępstw oparta o wymuszenia i próby okupu rośnie w skali

53% korespondencji elektronicznej zawiera treści typu spam

90% pracowników narusza zasady polityki bezpieczeństwa firmy

700% rocznie. Szczególnie rozpowszechniane są ataki typu:

- BEC (Businnes Email Compromise)
- APT (Advanced Persistent Threats)

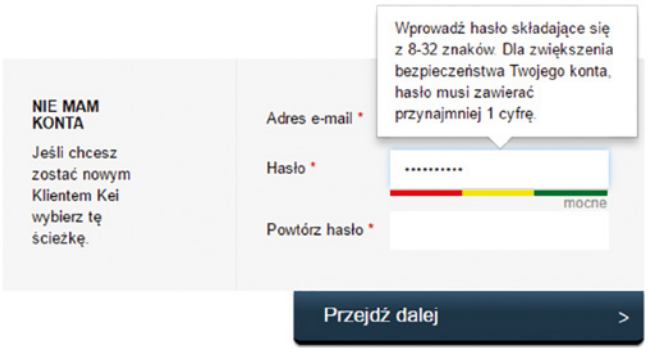
Według eksperta z powodu ataków opartych na metodach inżynierii społecznej firmy straciły 140 mln dolarów.

Ważne by każdy z pracowników posiadał indywidualne konto z odrębnym loginem i hasłem. Warto zadbać by pracownicy pamiętali o częstej zmianie haseł. Istotne jest także wymuszanie silnych haseł, zawierających znaki specjalne.

Jak stworzyć bezpieczne hasło?

Przeczytaj więcej >> https://www.kei.pl/blog/bezpieczne-haslo-jak-stworzyc-zapamietac/

Testy penetracyjne – to autoryzowany, stymulowany atak na system komputerowy, przeprowadzany w celu oceny bezpieczeństwa systemu. Test ma na celu zidentyfikowanie słabych punktów (określanych również jako „luki"), w tym możliwości uzyskania przez niepożądane osoby dostępu do funkcji i danych systemu.



Wymuszanie silnych haseł warto wprowadzić na każdym poziomie, zarówno w komunikacie do klientów jak i do pracowników firmy
Źródło: www.kei.pl

Bezpiecznym hasłom przyglądają się także eksperci Google. Przy wsparciu badaczy z Kalifornijskiego Uniwersytetu w Berkeley ustalono, że cyberprzestępcy przejmują średnio 250000 kont tygodniowo. Najczęściej posługują się metodami phishingowymi, popularnie stosowany jest także keylogging. (Źródło: Google Security Blog)

Warto zachęcać pracowników by każdy zauważony, niepokojący sygnał był zgłaszany do działu IT. Nawet jeśli pracownik popełni błąd i przez swoje oficjalne działanie zainfekuje komputer, musi mieć świadomość, że w swobodnej atmosferze zgłosi swój problem odpowiednim osobom, co pozwoli na szybką reakcję i przyśpieszy proces badawczy.

Bezpieczny hosting dla e-sklepu

Bezpieczny hosting dla e-sklepu
W temacie bezpieczeństwa e-commerce stale poruszana jest także kwestia hostingu. Wielu właścicieli prostych i małych e-commersów decyduje się na hosting współdzielony, co znaczy, że dzielą swój serwer z innymi użytkownikami.

>> **Keylogger** – typ oprogramowania, które potrafi przechwycić i nagrać aktywność wykonywaną przy użyciu klawiatury zaatakowanego komputera. Keylogger jest w stanie przejąć całą komunikację bez wiedzy użytkownika oraz wysyłać zapisane dane do zewnętrznego komputera. Istnieją również legalne narzędzia do monitorowania, stosowane między innymi przez organy ścigania.

W Kei.pl administratorzy czuwają nad bezpieczeństwem danych klientów współdzielonego hostingu. Do ochrony poczty elektronicznej wykorzystuje się wiele zintegrowanych ze sobą narzędzi. Między innymi skanera antyspam oraz skanera antywirusowego. Osobno monitorowana jest poczta wychodząca. Monitorowany jest także wolumen, źródło i zmiany w nich zachodzące. Konta klientów zabezpieczone są przed wysyłką spamu. Jeśli klient zacznie wysyłać spam to trafi na wszelkie blokady i jego skrzynka zostanie zablokowana.

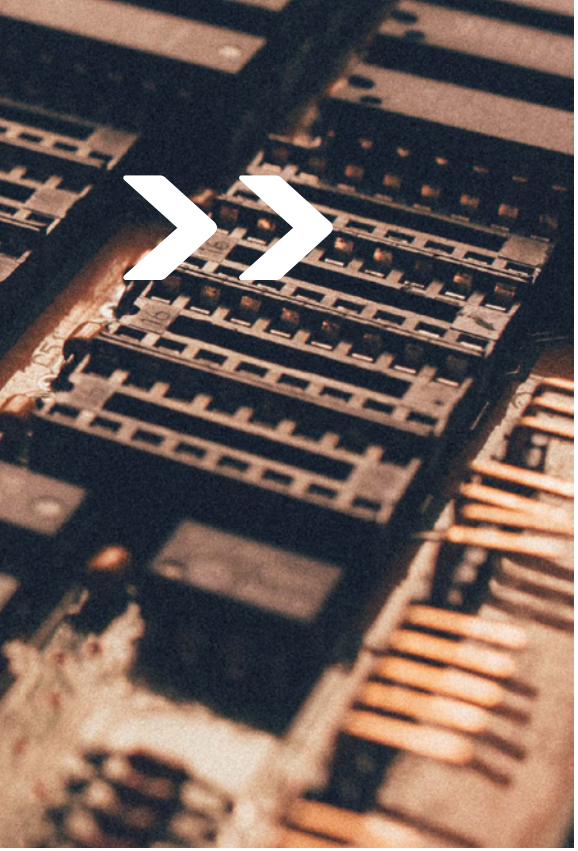
W naszej infrastrukturze korzystamy z firewalli, w tym również z firewalla aplikacyjnego. Skanujemy dane oraz blokujemy połączenia m.in. połączenia HTTP metodą POST zawierające złośliwy kod (wirusy/złośliwe oprogramowanie) – podkreśla Marcin Szopa, architekt IT z Centrum Danych Kei.pl

Backup
Jeśli z jakiś względów utracimy swoje dane np. wskutek nieumyślnego skasowania lub błędu aplikacji, która w niewłaściwy sposób nadpisała zawartość plików, ostatnią deską ratunku pozostaje odzyskanie danych z backupu. W Kei.pl backup pełnych danych wykonywany jest raz dziennie w godzinach nocnych i zawiera takie informacje jak:

- konfiguracja usług (WWW, poczta, etc)
- pliki umieszczone na koncie FTP
- stan zawartości skrzynek pocztowych w onecie wykonywania backup
- struktura i zawartość umieszczona w bazach danych

Dzięki przechowywaniu tych wszystkich informacji przez minimum trzy dni wstecz jesteśmy w stanie zapewnić użytkownikom najwyższy stopień bezpieczeństwa świadczonych usług. Backupy dniowe umieszczone są na osobnych serwerach przeznaczonych tylko i wyłącznie do trzymania danych archiwalnych co w znaczący sposób wpływa na zwiększenie poziomu bezpieczeństwa informacji. Serwery backupowe pracują w specjalnie przygotowanej wersji systemu, który w optymalny sposób rozmieszcza zawartość archiwizowanych plików dbając przy tym o ich kompletność oraz pozwalając na łatwe zarządzanie backupem w celu szybkiego odzyskania danych klienta. Systemy te działają w odseparowanym środowisku które w 100% zabezpiecza dane przed dostępem niepowołanych osób.

Przeczytaj więcej >>
https://www.kei.pl/blog/cala-prawda-o-backupie/



Agata Kawula,
Kierownik ds. Produktu
Kei.pl

Pod względem bezpieczeństwa serwer dedykowany góruje nad hostingiem współdzielonym. Z plusów niewspółdzielonego środowiska, w którym znajdują się usługi newralgiczne, czyli np. strona internetowa sklepu czy też poczta tylko jednego klienta, szeroko korzystają przedstawiciele branży e-commerce. W Kei.pl serwer zarządzany to usługa w pełni skonfigurowana. Rozpoczynając od systemu operacyjnego, konfiguracji silników bazodanowych i wirtualizacji, a kończąc na autorskich panelach do sprawnego zarządzania serwerem. Wersja Admin zapewnia pełną opiekę wykwalifikowanych administratorów oraz dedykowanego opiekuna handlowego. Z tej usługi najczęściej korzystają klienci, którym zależy na bogatym wsparciu w zarządzaniu usługą oraz minimalizacji kosztów związanych z samodzielną administracją. Serwer zarządzany Kei.pl właśnie to oferuje. Podsumowując, klient korzystając z tego wariantu, może cieszyć się swobodą i niezależnością przy jednoczesnym profesjonalnym wsparciu 24/7/365.

Twierdza dla e-biznesu

Pliki sklepu internetowego potrzebują bezpiecznego miejsca. Centrum Danych Kei.pl przypomina twierdzę. W fizycznych zabezpieczeniach pomaga korzystanie z usług wyspecjalizowanej agencji ochrony, a także monitoring CCTV działający w środku i na zewnątrz budynku. Sercem Centrum Danych jest serwerownia. Dostęp do niej mają wyłącznie pracownicy o najwyższych uprawnieniach.

> Ochrona przeciwpożarowa

W obiekcie działa system wczesnego ostrzegania przeciwpożarowego i system gaszenia gazem. Dodatkowo drzwi do serwerowni mają podwyższoną odporność ogniową, co uniemożliwia rozprzestrzenianie się pożaru. Nawet w razie pożaru i rozpylenia gazu gaśniczego serwery pracują bez przerwy.

Sprawdź ofertę serwerów dedykowanych >>

https://www.kei.pl/serwery-dedykowane

> Zasilanie awaryjne

Najważniejszym paliwem dla Centrum Danych poza dostępem do sieci jest energia elektryczna. W celach zabezpieczenia stosowany jest zabezpieczony system zasilania awaryjnego. W przypadku długiego przestoju w dostawie prądu ciągłość w poprawnym funkcjonowaniu Centrum Danych zapewniają agregaty prądotwórcze. Działanie wszystkich urządzeń w infrastrukturze Kei.pl podtrzymują wysokiej mocy zasilacze awaryjne UPS i agregaty prądotwórcze o łącznej mocy prawie 1000 kVA.

ROZWIĄZANIA DEDYKOWANE INDYWIDUALNYM PROJEKTOM

Certyfikaty SSL

Domeny

Serwery VPS

Hosting SSD

Serwery dedykowane

www.kei.pl
+48 801 308 408
handlowy@kei.pl

Kei.pl