Cyberdefence 24

aut. Andrzej Kozłowski 09.01.2020

ETYCZNY HAKER: PROGRAMIŚCI SKUPIAJĄ SIĘ NA FUNKCJONALNOŚCI ZAMIAST NA BEZPIECZEŃSTWIE

„Deweloperzy oprogramowania nie wiedzą nic o bezpieczeństwie i koncentrują się wyłącznie na funkcjonalności” mówi "etyczny haker" Tomáš Volný. Ekspert w specjalnym wywiadzie dla CyberDefence24.pl mówi o największych problemach firm, najczęściej popełnianych błędach na poziomie zabezpieczeń oraz o sposobach na skuteczne wzmocnienie bezpieczeństwa w organizacji, niezależnie od wielkości biznesu.

Jesteś etycznym hakerem. Co to znaczy?

Bycie etycznym hakerem polega na tym, że firmy prywatne zatrudniają nas w celu dokonania audytu ich systemów przykładowo infrastruktury, aplikacji internetowych i bezpieczeństwa fizycznego pracowników.

Przeprowadzasz pentesty sprawdzające bezpieczeństwo systemów i sieci firm. Jakie główne problemy napotykasz? Czy można powiedzieć, że są one podobne niezależnie od tego kogo badacie?

Pierwsze kroki, które podejmujemy przeprowadzając testy penetracyjne są praktycznie takie same, niezależnie od firmy, którą badamy. Należy jednak pamiętać, że sprzęt i serwery używają różnych technologii i oprogramowania, dlatego zawsze to wygląda trochę inaczej. Głównym problemem jest to, że deweloperzy nie wiedzą nic o bezpieczeństwie i koncentrują się wyłączenie na funkcjonalności.

W takim razie czy możemy powiedzieć, że koncepcja security by design jest mitem?

Nie do końca. Czasami zdarza się, że faktycznie bezpieczeństwo w ramach projektowania aplikacji jest ważne, ale realizacja założeń polityki bezpieczeństwa przebiega już o wiele gorzej. Na szczęście jednak ten trend ulega zmianie i aplikacje stają się o wiele lepiej zabezpieczone.

Należy jednak pamiętać, że jedną kwestią jest teoria i to co jest na papierze, a druga rzecz to realizacja. Przeprowadzaliśmy już testy penetracyjne, gdzie na papierze wszystko wyglądało świetnie, było dobrze zaprojektowane, jednak realizacja była straszna. Całkowicie nie zgadzało się z tym co było zaplanowane. Jestem pewien, że istnieją przykłady, gdzie realizacja założeń była poprawna.

Czyli można powiedzieć, że plany bezpieczeństwa organizacji były dobre, ale sposób ich realizacji już nie?

Mieliśmy jeden projekt, kiedy nasz klient zatrudniał zewnętrznych programistów odpowiedzialnych za przygotowanie aplikacji dla niego. Przetestowaliśmy aplikacje przygotowane przez nich

i wykorzystywane w firmie i okazało się, że są one bardzo słabo zabezpieczone. Kiedy klient skierował zapytanie do tych programistów, dlaczego ich produkty mają taki słaby poziom zabezpieczeń, otrzymał odpowiedź, że nie zgłaszał zapotrzebowania na zabezpieczenia przed cyberatakami!

To dość ekstremalny przykład. Czy można zatem powiedzieć, że problem leży z brakiem definiowania zapotrzebowania na bezpieczeństwo przy zamawianiu aplikacji?

To jest trochę jak z zakupem samochodu. W trakcie wyboru modelu nie myślisz i nie dopytujesz sprzedawcy czy samochód wytrzyma wypadek. Jest to dla Ciebie coś normalnego, że powinien być bezpieczny. Podobnie wygląda to w przypadku tworzenia serwerów czy aplikacji. Nie oczekujesz, że zostaną stworzone z podatnościami i błędami. Wydaje się, że jest to naturalne, że będą one bezpieczne. Ufasz osobom, które tworzą oprogramowanie, że znają się na swojej robocie i rozwiązania przygotowane przez nich będą dobre.

Jakie jeszcze największe problemy bezpieczeństwa napotkałeś w swojej pracy?

Testujemy systemy banków, które teoretycznie muszą być dobrze zabezpieczone, a ich aplikacje cechować najwyższy poziom ochrony. W praktyce wygląda to różnie i zależy od danego banku. Czasami, kiedy zaczynam testy penetracyjne, aplikacje jeszcze nie są skończone i dlatego często musimy pracować nad nieukończonych projektach. Liczba znalezionych luk zależy w dużej mierze od klienta. Niektórzy z nich używają aplikacji od tych samych deweloperów oprogramowania, którzy na szczęście uczą się z naszych raportów o popełnionych błędach. Część z nich zamawia aplikacje od innych deweloperów, które mają więcej podatności.

Sprawdzacie również czujność i przygotowanie pracowników firm. Jakie są główne błędy, które są popełniane przez ludzi?

Niestety, pracownicy często nie posiadają wiedzy na temat bezpieczeństwa. Przykładowo phishing jest najlepszą metodą, którą wybieramy aby sprawdzić ochronę sieci i systemów danej firmy. Jest zawsze sposób, najczęściej dość łatwy, aby sprawić, że fałszywy mail będzie wyglądał jak prawdziwy. Ludzie nie myślą o tym i klikają w co popadnie, nie zmieniają również haseł, które również bardzo często są słabe.

Jednym z podstawowych i ważnych elementów bezpieczeństwa to umiejętność stworzenia wystarczająco silnego hasła. Jak nauczyć ludzi żeby stosowali trudne do złamania hasła oraz jaka powinna być polityka firmy w tym obszarze?

To jest problem, że organizacje popełniają olbrzymie błędy jeśli chodzi o politykę haseł. Wiele firm wymaga, np. żeby hasło miało 15 znaków, małe i duże litery, które pracownik musi zmieniać raz w miesiącu. Taka polityka jest bardo zła, ponieważ pracownicy używają tych samych haseł z małymi zmianami np. dodają aktualny miesiąc na końcu hasła czy piszą je na kartkach, które zostawiają w widocznych miejscach lub nawet przyklejają do ekranów komputera. Co gorsze część osób odpowiedzialnych za bezpieczeństwo w firmach uważa, że jest to poprawna polityka i trudno zmienić ich tok myślenia. A to jest bardzo złe zachowanie, które nie powinno mieć miejsca.

Zawsze jak jestem w różnych organizacjach to rekomenduje użytkownikom, żeby nie zmieniali haseł zbyt często, a już na pewno nie w regularnych, miesięcznych odstępach. Zamiast tego lepiej jest dać większą swobodę pracownikom i np. ustalić konkretne kryteria, które muszą spełniać hasła. Powinny one być przede wszystkim długie, 15 albo więcej znaków.

Długość jest najważniejsza?

Dokładnie tak. Kiedy użytkownicy dodają małe lub duże litery a z dodatkowymi numerami jest nawet

lepiej, znacznie poprawiają siłę hasła. I co najważniejsze nie muszą takich haseł zmieniać często. Trzeba również skończyć z niepotrzebnym ich komplikowaniem haseł, a zamiast tego uświadomić pracownikom, że mogą używać np. sentencji czy kilku, losowych słów połączonych ze sobą i to również może być bardzo silne hasło. Jeśli powiem im, że hasło ma mieć co najmniej 15 znaków to będą oni przerażeni. Jak maja oni je zapamiętać? Tłumaczę wtedy, że można stworzyć długie, łatwe do zapamiętania hasło jak np. drużynapiłarskarozgrywamecz.

Można powiedzieć, że może polityka tworzenia mocnych haseł zapomina o zachowaniu odpowiedniego balansu pomiędzy bezpieczeństwem a praktycznością.

Tworzymy coraz bardziej skomplikowane hasła, które są trudne do zapamiętania dla użytkowników, ale łatwe do odgadnięcia dla hakerów. Powinniśmy to robić zupełnie inaczej. Kilka firm rezygnuje z haseł.

Na rzecz jakich innych technologii?

Bazują na mobilnych aplikacjach, które są używane przez ich pracowników. Wykorzystywane są również kody QR. Innym dobrym przykładem jest używanie inteligentnych kart.
Posiadasz inteligentną kartę i używasz pinu do zalogowania się do komputera. Jeśli tylko na chwilę opuszczasz stanowisko pracy, to wyjmujesz inteligentną kartę i automatycznie się wylogowywujesz.

Jednym z najpoważniejszych zagrożeń jest phising. Co można zrobić, żeby ten problem zminimalizować?

Jedną z rzeczy, którą naprawdę polecam przedsiębiorstwom jest certyfikat S/MIME. Certyfikat ten może być używany jako cyfrowa sygnatura wysyłanych wiadomości email. Mówi on, że nadawca wysyłający daną wiadomość jest de facto prawdziwą osobą. Kiedy otrzymam maila który pochodzi z pracowniczego adresu, ale nie jest podpisany cyfrową sygnaturą to mogę spodziewać się, że może to być próba phisingu. Ważne jest również budowanie świadomości pracowników i ostrzeganie, że jeżeli otrzymują wiadomość, która wygląda w określony sposób to może to być to próba phisingu. Trzeba ich szkolić, że jeżeli mail nie ma sygnatury pomimo, że pochodzi z zaufanej domeny mailowej, to nie powinni otwierać żadnych załączników, bo może to być niebezpieczne. Taki certyfikat oczywiście kosztuje, ale są to stosunkowo niewielkie koszta, praktycznie niezauważalne dla firm, a mogą zdecydowanie zwiększyć bezpieczeństwo. To rozwiązanie może być również używane do szyfrowania maili. Jeśli mamy w firmie incydent bezpieczeństwa np. ktoś włamie się na serwer poczty elektronicznej to nie może odczytać wiadomości, ponieważ wszystko jest zaszyfrowane. Rekomendujemy takie rozwiązanie firmom.

Czy coraz więcej przedsiębiorstw używa takich rozwiązań?

Tak widzimy wzrastające zainteresowanie tego typu rozwiązań. Jest ono łatwe do wykorzystania przez pracowników, ponieważ za pomocą jednego przycisku mogą się podpisać. Może ono być domyślnie włączone i wysyłać zaszyfrowane wiadomości.

Przeprowadzasz testy penetracyjne w przedsiębiorstwach z różnych sektorów. Czy możesz powiedzieć, który sektor jest najbardziej wrażliwym na ataki, a który najbardziej odporny?

Nie mogę wskazać jednego konkretnego sektora, który jest bardziej lub mniej bezpieczny. Nie można powiedzieć, że sektor bankowy jest lepiej przygotowany niż sektor transportowy. To zależy od konkretnej firmy. Widziałem i testowałem aplikacje bankowe, które miały naprawdę dużą liczbę podatności, ale spotkałem się również z bardzo dobrze zabezpieczonymi aplikacjami. Badałem też strony firmy, które były przygotowane na potencjalne cyberataki oraz takie, które były bardzo podatne. Wszystko zależy od danego przedsiębiorstwa.