Bezpieczeństwo IT

w Twojej firmie

TestArmy

O autorze

Dawid Bałut

Cyber Security Director w TestArmy

Doświadczony pentester i bug hunter, spędził pół dekady badając zabezpieczenia w setkach firm, w tym takich gigantów jak Apple, Amazon, czy Facebook. Dołączył potem do defensywnej strony mocy, aby przez kolejne 6 lat pracować jako Security Architect dla startupu w Dolinie Krzemowej.

Obecnie zajmuje się budowaniem systemów zabezpieczeń, automatyzowaniem wszystkiego co się da i edukacją pracowników w duchu DevSecOps. W wolnym czasie dzieli się swoimi przemyśleniami w mediach społecznościowych i przygotowuje darmowe materiały do nauki, poruszające kwestie takie jak zarządzanie bezpieczeństwem, empatyczne podejście do zarządzania i rozwój w biznesie.

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.

Nie będzie łatwo, **ale nie musi też być zbyt ciężko**

W dzisiejszym świecie bezpieczeństwa IT często słyszy się o ideach testów penetracyjnych, programach bug bounty i badaniach podatności. Powinieneś sobie jednak zdać sprawę, że choć te rozwiązania są niesamowicie wartościowe, to dla większości firm nie są najważniejsze i najbardziej efektywne kosztowo. Zacznijmy jednak od początku.

Głównym powodem ich nieefektywności jest koncentracja pracy na ostatniej fazie SDLC (Software Development Life Cycle, czyli Cyklu Rozwoju Oprogramowania), kiedy produkt jest już ukończony i gotowy do publikacji. Jeśli rozpoczniemy testy penetracyjne, ale nie zwracaliśmy uwagi na bezpieczeństwo na wcześniejszych etapach, to trzeba liczyć się z zatrważającymi kosztami.

Deweloperzy pracujący z kodem skupiają się zazwyczaj na jak najszybszym ukończeniu swoich zadań, tak żeby tylko zmieścić się w wyznaczonych terminach i dostarczyć funkcjonalne oprogramowanie. Pośpiech przy pracy skutkuje jednak rosnącą liczbą błędów wkradających się do systemów bezpieczeństwa na każdym etapie prac nad kodem. To jest właśnie pole do popisu dla naszych ekspertów, którzy stoją na straży jakości kodu i to dzięki ich pracy deweloperzy mogą się skoncentrować na zadaniach, które są naprawdę istotne dla nich i biznesu. Nasi wyspecjalizowani testerzy są dostępni w każdej chwili i zawsze można skonsultować z nimi działania albo po prostu zlecać im prace testowe. Możesz dać im dostęp do kodu źródłowego swojej aplikacji, a stworzą odpowiednie testy i pomogą programistom dostarczyć gotowy produkt na czas, nie ryzykując przy tym spadku jego jakości.

> ***Ogólna zasada efektywnych systemów bezpieczeństwa jest więc taka, że im wcześniej zaczniesz zwracać uwagę na zabezpieczenia, tym mniejsze koszty poniesiesz później, gdy zajdzie konieczność łatania ewentualnych luk.***

Dzisiejsze Quality Assurance **daje duże możliwości**

Giganci branży hi-tech już od dawna to wiedzą i inwestują ogromne środki w wewnętrzne procesy testowe, które wychodzą daleko poza typowe QA w dawnym rozumieniu. Błędy funkcjonalne są kosztowne, bo tymczasowo zniechęcają użytkowników do korzystania z aplikacji, ale to luki bezpieczeństwa prowadzą do całkiem nieprzewidywalnych rezultatów, z bankructwem firmy włącznie. Firm po prostu nie stać na dopuszczanie do błędów w zabezpieczeniach w produktach udostępnianych klientom. Przyjrzyjmy się kilku najczęstszym powodom, dla których firmy decydują się inwestować w bezpieczeństwo:

1) Chęć odróżnienia się od konkurencji
2) Konkretne wymagania stawiane przez klientów
3) Wymogi prawne
4) Obawa przed konsekwencjami wycieków danych
5) Strach przed wykryciem luk w twoich zabezpieczeniach przez niezależnych testerów i kompromitacją firmy

Przeanalizujmy teraz te powody jeden po drugim:

Chęć odróżnienia się od konkurencji

Jeśli wyprzedzisz konkurencję pod względem bezpieczeństwa, wykorzystaj to marketingowo i pokaż klientom, że razem z twoim produktem kupują zaufanie, niezawodność i szacunek do ich danych (czyli pełną poufność). Nie chodzi jednak tylko o środki bezpieczeństwa w klasycznym rozumieniu tego pojęcia. Jeśli mechanizmy bezpieczeństwa, jak na przykład uwierzytelnianie dwuskładnikowe, zostaną zaimplementowane w przyjazny użytkownikowi sposób, efektem będzie na pewno znaczne podniesienie zadowolenia z korzystania z produktu.

Osoby decyzyjne dobrze wiedzą jak druzgocący wpływ na przyjęcie produktu przez klientów może mieć problematyczne UX funkcji bezpieczeństwa.

Konkretne wymagania stawiane przez klientów

W czasach, gdy szpiegostwo przemysłowe jest dla sieciowych złodziei wyjątkowo dochodowym zajęciem, klienci korporacyjni oczekują poczucia bezpieczeństwa, jakie mogą im dać tylko najwyższej jakości produkty i usługi. Klienci indywidualni oczekują usług na tyle bezpiecznych, żeby móc spać spokojnie i nie martwić się o swoją prywatność. W przypadku prezesów spółek dochodzi jeszcze odpowiedzialność za poufność informacji o finansach firmy, czy dokumentów patentowych i za potencjalne skutki wycieku tych informacji do internetowych oszustów i konkurencji. Jeśli twój produkt nie jest dostatecznie bezpieczny, będzie ci po prostu trudno go sprzedać. Klienci, szczególnie ci z branży finansowej, są bardzo świadomi ryzyka, więc jeśli celujesz w takie "grube ryby", to utrzymanie wysokich standardów bezpieczeństwa jest obowiązkowe.

Wymogi prawne

Przy obowiązujących przepisach RODO, żadna firma nie może sobie pozwolić na zaniedbanie kwestii bezpieczeństwa danych. Potencjalne koszty i konsekwencje są zbyt wysokie, aby zignorować potrzebę posiadania rygorystycznych procedur i polityki security, a im wcześniej zaimplementujesz odpowiednie środki, tym łatwiej unikniesz ewentualnych problemów. Kary finansowe przewidywane przez Rozporządzenie mogą nawet zagrozić istnieniu nieźle prosperującej firmy. Nasi eksperci pomogą ci ocenić zagrożenia związane z procesami przetwarzania danych. Dział Security, we współpracy z Działem Prawnym upewni się, że twoje procedury spełniają wszystkie wymogi nowej dyrektywy UE w zakresie ochrony danych osobowych. Implementacja procedur zgodnych z RODO wymaga dokładnego audytu aktualnego stanu całej organizacji. Nasz Zespół Audytorski pomoże zaimplementować

mechanizmy chroniące twoją firmę przed wyciekami danych. Wprowadzimy cię także w zasady i procedury reagowania na incydenty – jeśli faktycznie dojdzie do wycieku, będziesz dobrze wiedział co robić, aby ograniczyć straty.

Obawa przed konsekwencjami wycieków danych

Wycieki danych są bardzo kosztowne. Przy rosnącej popularności ataków ransomware, nawet jedna luka pozwalająca na dostęp do twojego systemu może prowadzić do fatalnych konsekwencji. Do tego dochodzi szpiegostwo przemysłowe, szantaże, wykorzystywanie firmowych komputerów do kopania kryptowalut, malware spowalniające sieć – te niebezpieczeństwa mają zarówno bezpośredni, jak i pośredni wpływ na działanie firmy. Jeśli serwery działają powoli, stracisz po prostu bardziej niecierpliwych klientów, którzy w oczekiwaniu na załadowanie twojej strony przejdą do konkurencji. Mówiąc wprost – mało kogo stać na luki w zabezpieczeniach. Szczególnie start-upy, małe i średnie przedsiębiorstwa, które wciąż jeszcze nie mają ugruntowanej pozycji i reputacji nie mogą pozwolić sobie na pokazanie się od złej strony. Na wczesnym etapie budowania wizerunku każda podejrzana sytuacja może zaważyć na dalszym istnieniu firmy.

Strach przed wykryciem luk w twoich zabezpieczeniach przez niezależnych testerów i kompromitacją firmy

Reputacja znaczy bardzo wiele. Społeczność osób zajmujących się bezpieczeństwem jest bardzo sprawna i wielu jej członków wręcz pasjonuje się przeprowadzaniem badań i wyszukiwaniem podatności w popularnym oprogramowaniu. Ujawnienie informacji o nich, nawet niezamierzone, może skutkować utratą reputacji firmy (oczywiście wszystko zależy od tego, jak sobie z taką sytuacją poradzisz). Jeśli wejdziesz w dialog z takimi specami, możesz zaprezentować się opinii publicznej w dobrym świetle, jeśli jednak twoja reakcja będzie nie do końca przemyślana lub trafisz na wyjątkowo mało komunikatywnego testera, to wylądujesz na z góry przegranej pozycji. Wyszukiwanie podatności i polowanie na błędy to aktualnie bardzo popularne zajęcie, więc lepiej jak najwcześniej zainwestować w zabezpieczenia, niż liczyć na to, że luki nie wyjdą na jaw. Nadzieja to zdecydowanie za mało aby zbudować skuteczną strategię zarządzania ryzykiem.

Tok myślenia, **a bezpieczeństwo**

W wielu firmach kwestie bezpieczeństwa nie dość, że uważa się za zło konieczne, to jeszcze kosztowne. Diabeł jednak tkwi w szczegółach i podejściu do tematu. Takie negatywne nastawienie do spraw zabezpieczeń nie jest oczywiście rozsądne, bo skoro i tak nie jest łatwo, to po co sobie jeszcze bardziej utrudniać życie? Mówiąc o wskaźniku rentowności wydatków na bezpieczeństwo, mamy na myśli rentowność pośrednią – to znaczy ograniczanie lub wręcz unikanie strat. Dbanie o kwestie security może być dobrą kartą przetargową w negocjacjach z potencjalnymi kontrahentami i przy analizach konkurencyjności. Jeśli więc zaczniesz posługiwać się językiem korzyści i dostrzegać potencjalne zyski, na pewno zdołasz przekonać kadrę kierowniczą do inwestowania również w ten aspekt działalności firmy.

Jako firma programistyczna na pewno podniesiesz sprzedaż koncentrując się na bezpieczeństwie swoich usług i produktów. Klienci mają już dość dobre rozeznanie w temacie i stawia ich to w uprzywilejowanej pozycji. Umiejętność udowodnienia, że twoje usługi są bezpieczniejsze od proponowanych przez konkurencję znacząco podnosi szanse zdobycia kontraktów wśród takich świadomych klientów. W niektórych branżach bezpieczeństwo jest wymogiem krytycznym i to nie cena, parametry, czy użyteczność produktu sprawiają, że klient wybiera konkretnego dostawcę. Tylko gwarancja, że jego dane są bezpieczne, jest w stanie przekonać go, że warto nawiązać współpracę.

Dbanie o kwestie security może być dobrą kartą przetargową w negocjacjach z potencjalnymi kontrahentami i przy analizach konkurencyjności.

Maksymalizacja ROI

Branża security stara się uczyć firmy jak wydawać pieniądze, ale kładzie niedostateczny nacisk na efektywność tych inwestycji, więc maksymalizacja korzyści stała się sporym wyzwaniem. Kilka mądrych decyzji może szybko ustawić cię w pozycji dominującej nad konkurencją, więc zgłębmy nieco bardziej ten temat i sprawdźmy, co da się robić lepiej, aby poprawiać wyniki oraz obniżać koszty.
Wynajmowanie pentesterów z zewnątrz już nie wystarcza. Procesy inżynierii oprogramowania zmieniły się na tyle, że ograniczanie się do testów penetracyjnych nie jest wystarczająco efektywnym rozwiązaniem – robi je praktycznie każda firma, więc nie są żadnym wyróżnikiem na rynku. Jeśli naprawdę chcesz zdobyć zaufanie klienta, to będziesz musiał się trochę bardziej wysilić, bo i konkurencja nie próżnuje. Wiele przedsiębiorstw już w pełni zdaje sobie sprawę z tego tego jak ważne są kwestie security, ale jednak mało kto jeszcze umie tę wiedzę wykorzystać w praktyce.

W biznesie wszystko powinno być podyktowane efektami poprawnej analizy ryzyka, ale aby nim zarządzać, musisz znać ceny rozwiązań alternatywnych. Tylko patrząc na wszystko w szerokim kontekście, da się podjąć dobrą decyzję odnośnie profilu ryzyka.

Security Assurance **nie musi kosztować aż tyle**

TestArmy

Pewnie słyszałeś już o sprawach takich jak testy penetracyjne, ocena podatności, czy „bug bounty". Mówi się o nich często, ale to nie znaczy, że koniecznie trzeba interesować się nimi w pierwszej kolejności. Najpierw warto zadbać o inne kwestie, które długoterminowo mogą dać nawet lepsze efekty.
Spójrzmy na podstawowe fazy rozwoju oprogramowania (SDLC), czyli: planning (planowanie), requirements analysis (analizę wymagań), design (projektowanie), development (rozwój), testing (testy), implementation (implementację) i maintenance (utrzymanie). Konwencjonalne testy penetracyjne wykonywać można na trzech ostatnich etapach (testing, implementation, maintenance).

Jeśli wdrożymy prace nad bezpieczeństwem aplikacji na fazie testów (czyli piątej), to znaczy, że nic nie robiliśmy przez poprzednie cztery etapy, kiedy jeszcze można było identyfikować i naprawiać problemy względnie małym kosztem. Wiele firm zaczyna rozważać kwestie bezpieczeństwa i wynajmuje pentesterów dopiero po zakończeniu prac nad kodem, pomijając aż sześć wcześniejszych kroków!

W firmach, z którymi współpracowałem, zauważyć można było następujące wymagania:

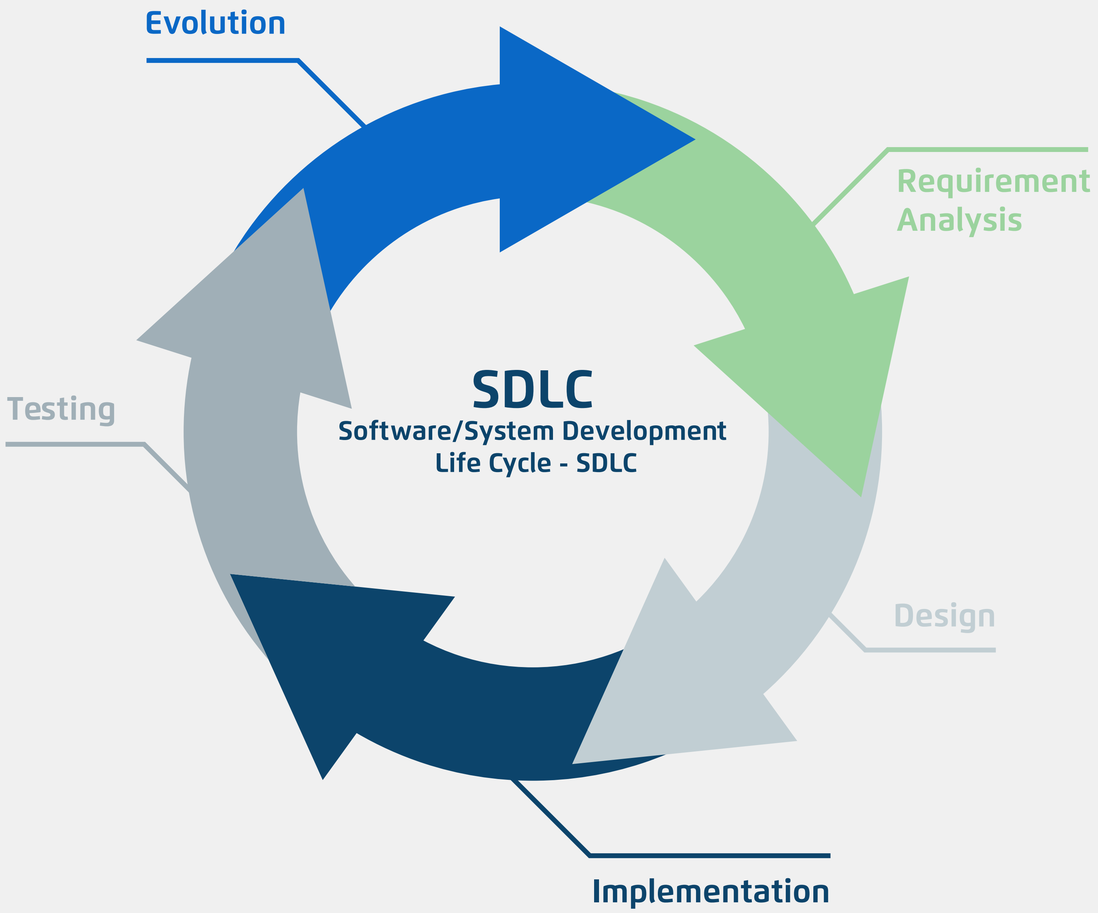
- Program musi być gotowy szybko
- Program musi być przetestowany i stabilny
- Program musi być dostarczony klientowi jak najszybciej
- Prace muszą odbywać się nawet wtedy, gdy inżynierowie są zmęczeni i rozkojarzeni

Aby zgasić problem w zarodku, najlepiej zainwestować w to, co najważniejsze dla każdej organizacji – mądrą kadrę. Edukacja inżynierów oprogramowania, właścicieli produktu i wewnętrznych inżynierów QA pozwoli pracować nad bezpieczeństwem oprogramowania już na pierwszych fazach rozwoju programu. Jeśli masz w zespole świadomych zagrożeń inżynierów, to z pewnością zauważą oni jakieś

> ***Edukacja inżynierów oprogramowania, właścicieli produktu i wewnętrznych inżynierów QA pozwoli pracować nad bezpieczeństwem oprogramowania już na pierwszych fazach rozwoju programu.***

wady już w projekcie i logice biznesowej, tym samym zmniejszając liczbę błędów, które trzeba będzie rozwiązać w przyszłości.

Opracowaliśmy ramy „świadomości bezpieczeństwa", z których możesz korzystać, aby pomóc swoim inżynierom lepiej wykonywać swoje obowiązki. Każdy z nas już i tak jest przeładowany ważnymi zadaniami, a programiści nie mają czasu, aby uczyć się nowych, skomplikowanych zagadnień, takich jak właśnie bezpieczeństwo, na własną rękę. Inwestycja w profesjonalnych trenerów i materiały szkoleniowe pozwala na dłuższą metę obniżyć koszty tworzenia oprogramowania. Delikatnie ukierunkowując nastawienie deweloperów nie spowolnisz harmonogramu publikacji, bo po prostu przy pracy będą oni korzystali z rozwiązań, które będą dobrze rozumieć.



Możesz być twardy, ale elastyczny

TestArmy

Kwestie bezpieczeństwa przez całe dekady były hamulcem niemal każdej firmy. Cały czas powodowały dodatkowe koszty i były problematyczne pod wieloma innymi względami. Przyzwyczailiśmy się do produkcji oprogramowania w modelu lawinowym, a zapewnianie bezpieczeństwa traktujemy zazwyczaj tak samo. Dla wielu firm czasy tego systemu pracy dobiegły już jednak końca i powinno tak być również, jeśli chodzi o procedury wdrażania zabezpieczeń. Szczególnie, że dysponujemy wszelkimi środkami technicznymi, aby zmienić ten wadliwy system. Przy czym chodzi tylko o filozofię pracy, doświadczenie i chęci. Przesunięcie spraw bezpieczeństwa w na lewą stronę osi czasu SDLC znacznie podnosi efektywność ich implementacji. Pamiętając o odpowiednich praktykach na każdym etapie prac, zapewnimy sobie potem zdecydowanie więcej czasu na ewentualne poprawki i ulepszenia. Głównym powodem trudności związanych z kwestiami security jest to, że przyzwyczailiśmy się do robienia wszystkiego ręcznie. Faktycznie, patrząc z tej perspektywy, ciężko sobie wyobrazić co można zmienić, żeby było prościej. Trzeba bardzo mocno automatyzować procesy, żeby mieć pewność, że cały kod jest bezpieczny zanim jeszcze zostanie wdrożony – i trzeba robić to mądrze. Zwyczajne pobranie i uruchomienie zautomatyzowanego skanera to za mało, trzeba rozumieć jak aplikacja działa i które narzędzia zewnętrzne mogą się przydać przy pracy z danym zestawem technologii. Należy wskazać tym narzędziom jak mają się łączyć z aplikacją i jak wykonywać miarodajne testy. Następnie trzeba przetworzyć dane, które się uzyska i oddzielić wartościowe informacje od tych, które nie mają sensu. To wszystko jest konieczne, bo nie chcemy przecież zasypywać deweloperów śmieciowymi komunikatami, które tylko zmniejszą ich produktywność.

Dostępne są gotowe, efektywne kosztowo narzędzia i metody wspierania inżynierów już na etapie projektowania. Dysponujemy też narzędziami wspierającymi deweloperów podczas pisania kodu oraz takimi, które pomogą zespołowi IT OPS wdrożyć produkt w bezpieczny sposób. To wszystko jest też w twoim zasięgu, ale musisz się odważyć i w końcu podjąć decyzję: czy chcesz zainwestować w strategię długoterminową? Kiedy już wszystko zacznie funkcjonować jak należy, koszty utrzymania systemu znacznie spadną i skorzystasz na mniejszej liczbie błędów w kodzie (które wymagałyby wypuszczania kosztownych łatek i przeprojektowywania gotowego produktu).

Przeprowadzimy cię przez wdrożenie procesów bezpieczeństwa.

Dowiedz się jak

Testy penetracyjne i **bezpieczeństwo ofensywne**

TestArmy

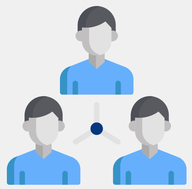
Co jeśli już ukończyłeś aplikację albo wszystkie procesy Bezpiecznego SDLC są już dawno wdrożone? W pewnym punkcie nie da się uniknąć przeprowadzenia końcowych testów penetracyjnych i mogą one przynieść bardzo interesujące rezultaty.

Pentesterzy to specjaliści od badania bezpieczeństwa, ale różnią się od reszty podobnych sobie nie tylko wiedzą techniczną. Przedstawiciele tej specjalności muszą charakteryzować się specyficznym nastawieniem psychologicznym, które sprawia, że potrafią myśleć i działać jak hakerzy, a tym samym wyszukiwać luki w bezpieczeństwie systemów, które mogłyby zostać przegapione przez testerów QA i inżynierów oprogramowania. Programistów uczy się i wymaga się od nich, aby myśleli jak konstruktorzy i typowi internauci, którzy nie chcą nikomu zrobić krzywdy. Testerzy penetracyjni jednak potrafią przyjąć dużo bardziej ofensywny sposób myślenia i robią to na tyle często i długo, że ich umysły nauczyły się już w kreatywny sposób wynajdywać nowe sposoby na wykorzystanie dziur w systemach zabezpieczeń.

1. Testy penetracyjne i działania Red Teaming

2. Testowanie bezpieczeństwa infrastruktury sieciowej

3. Testy socjotechniczne



4. Blue Teaming

Zewnętrzni testerzy penetracyjni sprawdzają systemy od A do Z, zapewniając proceduralne wytyczne dotyczące problemów, które mogłyby się zagnieździć w twoich aplikacjach i infrastrukturze. Zdolny zespół zidentyfikuje błędy i dostarczy szczegółowych informacji o tym, co można zrobić lepiej, żeby nie trzeba było mierzyć się z podobnymi problemami w przyszłości. Po zaangażowaniu odpowiednich testerów, będziesz mógł skorzystać z ich wiedzy aby udoskonalić swoje SDLC. Chociaż usługi takich speców mają liczne zalety, nie zapominaj, że są one przede wszystkim wisienką na torcie – a przecież w pierwszej kolejności potrzebujesz właśnie tortu. W przeciwnym wypadku narazisz się tylko na frustrację i utratę pieniędzy.

Typy testów bezpieczeństwa

TestArmy

Dostępne są rozmaite typy audytów bezpieczeństwa, ale wszystkie mają jeden wspólny cel – zidentyfikować i załatać luki w systemach klienta. Potrafimy określić poziom bezpieczeństwa systemów IT, takich jak na przykład aplikacje webowe za pomocą rozmaitych środków oceny podatności na ataki, jakości kodu źródłowego i konfiguracji.

Testy penetracyjne i działania Red Teaming (ofensywne testy bezpieczeństwa) są najbardziej wyrafinowanymi działaniami, na które można się zdecydować. Ich celem jest symulacja prawdziwego ataku i zachowujemy się podczas nich dokładnie tak jak prawdziwi hackerzy, którzy próbują włamać się do twoich systemów IT. Następnie wskazujemy luki, które wymagają załatania, aby wzmocnić twoje zabezpieczenia. Prawdziwi złoczyńcy będą po czymś takim musieli się naprawdę postarać, aby spenetrować system, bo mamy lata doświadczenia w prowadzeniu testów penetracyjnych każdego typu (white-box, grey-box i black-box.)

W trakcie działań Red Teaming wejdziemy również w taką interakcję z Twoimi wewnętrznymi zespołami, która pomoże zbudować silniejszą infrastrukturę i sprawniejsze systemy monitorowania. Nauczycie się jak przechwytywać agresorów szybciej i jak odcinać im dostęp do swoich systemów zanim zdążą wyrządzić prawdziwe szkody.

Testowanie bezpieczeństwa infrastruktury sieciowej ma na celu wzmocnienie całej, tak zwanej, „Triady CIA" Twojej organizacji. Nasze testy są tak przemyślane, aby poprawić tajność, dostępność i integralność twoich systemów i danych.

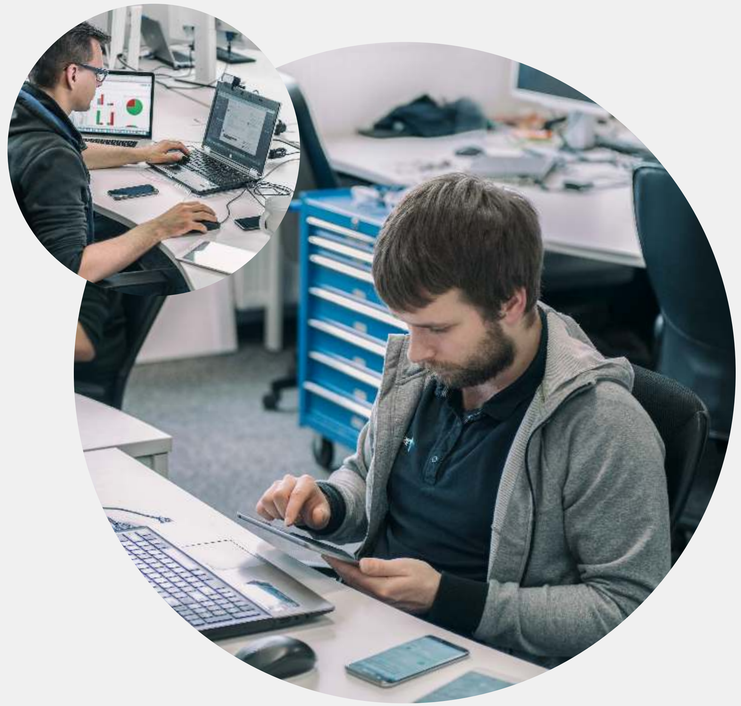
Zarówno zewnętrzne, jak i wewnętrzne testy infrastrukturalne naprowadzą cię na ścieżkę poprawy bezpieczeństwa sieci i wydajności. Testy wykonywane się przez naszych ekspertów zdalnie lub w siedzibie audytowanej organizacji. Dzięki weryfikacji laptopów, sieci i routerów wi-fi, drukarek, kamer internetowych, smartfonów pracowników i innych urządzeń sieciowych podłączonych do firmowego LANu szacujemy poziom zagrożenia atakiem i udzielamy pragmatycznych porad jak udoskonalić system. Wszystkie nasze działania są potem podsumowane w szczegółowym raporcie, pełnym zidentyfikowanych podatności i sugerowanych sposobów na rozwiązanie problemów.

Najsłabszym ogniwem nie jest technologia

To procesy, polityka i nasza własna świadomość zagrożeń sprawiają, że jesteśmy podatni na ataki. Jeśli firma nie poświęca dość środków na edukację pracowników o powadze zachowania higieny bezpieczeństwa, mogą oni bardzo łatwo paść ofiarą ataku socjotechnicznego.

Ataki socjotechniczne nie są niestety tematem tak znanym i często poruszanym, jak testy penetracyjne. Przez to prawdziwi hackerzy mają ułatwione zadanie i w wielu przypadkach bez problemu uzyskują pożądane informacje. Bo i po co właściwie marnować setki godzin na szukanie luk w oprogramowaniu, jeśli można zadzwonić do recepcji firmy podając się za administratora IT i poprosić o przekierowanie wrażliwych dokumentów na podany adres mailowy? Większość osób wykazuje na tyle empatii, że łatwo nadużyć ich zaufania, sympatii, czy strachu. Sprawny atak socjotechniczny może się ograniczyć do jednej rozmowy telefonicznej, podczas której hacker zdobywa ważne informacje osobiste lub dane uwierzytelniania, których użyje potem, aby uzyskać dostęp do systemu.

Testy socjotechniczne mają na celu wykorzystanie czynnika ludzkiego systemów IT poprzez zmanipulowanie ofiary w taki sposób, aby wykonała ona określone czynności na szkodę swojej firmy. Do takich czynności zalicza się na przykład ujawnienie wrażliwych informacji, umożliwienie dostępu do tajnych zasobów firmy osobie z zewnątrz oraz ujawnienie atakującemu danych uwierzytelniających. Wykonujemy stosowne symulacje, aby ocenić podatność załogi i jej zachowanie w obliczu tego rodzaju zagrożenia, a oceny dokonujemy poprzez ścisłą obserwację zachowania i podejścia pracowników twojej firmy. Nasi eksperci wprowadzają w życie zaawansowane scenariusze ataku, aby wyłudzić wrażliwe informacje, wykrywając przy tym słabe punkty w systemach bezpieczeństwa firmy.

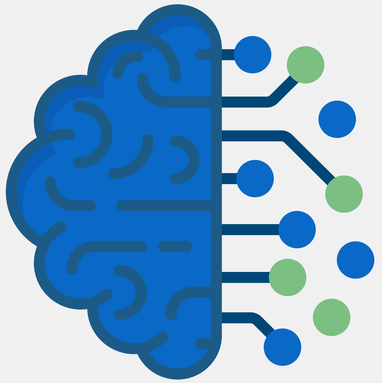


Najsłabszym ogniwem nie jest technologia

To procesy, polityka i nasza własna świadomość zagrożeń sprawiają, że jesteśmy podatni na ataki. Jeśli firma nie poświęca dość środków na edukację pracowników o powadze zachowania higieny bezpieczeństwa, mogą oni bardzo łatwo paść ofiarą ataku socjotechnicznego.

Ataki socjotechniczne nie są niestety tematem tak znanym i często poruszanym, jak testy penetracyjne. Przez to prawdziwi hackerzy mają ułatwione zadanie i w wielu przypadkach bez problemu uzyskują pożądane informacje. Bo i po co właściwie marnować setki godzin na szukanie luk w oprogramowaniu, jeśli można zadzwonić do recepcji firmy podając się za administratora IT i poprosić o przekierowanie wrażliwych dokumentów na podany adres mailowy? Większość osób wykazuje na tyle empatii, że łatwo nadużyć ich zaufania, sympatii, czy strachu. Sprawny atak socjotechniczny może się ograniczyć do jednej rozmowy telefonicznej, podczas której hacker zdobywa ważne informacje osobiste lub dane uwierzytelniania, których użyje potem, aby uzyskać dostęp do systemu.

Testy socjotechniczne mają na celu wykorzystanie czynnika ludzkiego systemów IT poprzez zmanipulowanie ofiary w taki sposób, aby wykonała ona określone czynności na szkodę swojej firmy. Do takich czynności zalicza się na przykład ujawnienie wrażliwych informacji, umożliwienie dostępu do tajnych zasobów firmy osobie z zewnątrz oraz ujawnienie atakującemu danych uwierzytelniających. Wykonujemy stosowne symulacje, aby ocenić podatność załogi i jej zachowanie w obliczu tego rodzaju zagrożenia, a oceny dokonujemy poprzez ścisłą obserwację zachowania i podejścia pracowników twojej firmy. Nasi eksperci wprowadzają w życie zaawansowane scenariusze ataku, aby wyłudzić wrażliwe informacje, wykrywając przy tym słabe punkty w systemach bezpieczeństwa firmy.



A co jeśli...

W błyskawicznie ewoluującym świecie cyberbezpieczeństwa trzeba zawsze patrzeć w przyszłość ze zdrową dawka pesymizmu. Nigdy nie wiadomo kiedy zostaniesz zaatakowany, więc po prostu zawsze musisz być gotowy na najgorsze. Większość firm nawet nie bierze pod uwagę możliwości utraty danych i konieczności utrzymywania zawsze aktualnych kopii bezpieczeństwa, nie testuje też swoich procedur jak należy. Aby zbudować lepszy od nich wizerunek trzeba stale wdrażać nowoczesne rozwiązania i pamiętać o czyhających zagrożeniach.

Minimalizacja kosztów wynikających ze złamania zabezpieczeń wymaga wcześniej przygotowanej strategii, która obejmuje efektywną komunikację i taktykę odzyskiwania danych. Większość z nas pamięta o tworzeniu i testowaniu kopii bezpieczeństwa, ale to tylko jedna z wielu metod ograniczania strat wynikających z włamania do systemu. Mowa o praktycznych procedurach do stosowania w celu minimalizacji strat na reputacji, strat finansowych i utraty klientów. Po prostu musisz mieć kompleksowy plan działania, który obejmuje każdy aspekt działania firmy.

Stało się!

Radzenie sobie ze skutkami złamania zabezpieczeń jest stresujące samo w sobie i nikt nie chce w międzyczasie zaprzątać sobie dodatkowo głowy sprawami czysto technicznymi, takimi jak analiza powłamaniowa i prowadzenie śledztwa. Nasz zespół Ekspertów Śledczych IT pomoże ci przygotować się i poradzić sobie z niebezpiecznymi sytuacjami, kiedy już do nich dojdzie.

Jednostka Blue Teaming przeanalizuje zagrożenia, przeprowadzi śledztwo dotyczące włamania i pomoże zareagować w taki sposób, aby straty biznesowe wynikające z incydentu pozostały na jak najniższym poziomie.

Sprawna reakcja jest kluczem do zapewnienia ciągłości funkcjonowania firmy. Priorytetem są zawsze utrzymanie stabilności systemów i zachowanie pozytywnego wizerunku firmy. Włamanie do systemu może przydarzyć się każdemu i to właśnie sposób poradzenia sobie z nim determinuje długofalowe konsekwencje incydentu.

Jak ograniczyć straty?

Skontaktuj się z Szymonem!

Kontakt

Szymon Chruścicki
Business Manager

+48 505 372 870

TestArmy Group S.A.

+48 600 993 557
contact@testarmy.com
www.testarmy.com