SOFLAB

Bezpieczeństwo IT
Audyty bezpieczeństwa i testy penetracyjne

Czy nasza usługa **jest dla Ciebie?**

- **Potrzebujesz ochronić dane** i zachować ciągłość działania.
- **Chcesz zaimplementować narzędzia bezpieczeństwa,** ale nie masz zasobów.
- **Potrzebujesz spersonalizowanych raportów,** aby spełnić wymagania zgodności i wymogi prawne.
- **Masz zespół techniczny**, ale potrzebujesz wyższego poziomu wiedzy na temat bezpieczeństwa.
- **Chcesz mieć pewność,** że Twoja wewnętrzna infrastruktura jest bezpieczna i nie ma możliwości nieautoryzowanych działań pracowników lub partnerów pracujących wewnątrz sieci, które spowodują ujawnienie tajemnic firmy.

Dzięki połączeniu wiedzy i technologii Soflab Technology pomaga organizacjom zoptymalizować bezpieczeństwo i jakość w całym cyklu życia oprogramowania.

106 dni
zajmuje firmom w Europie wykrycie cyberataku

56%
organizacji nie potrafi wykryć złożonych cyberataków

1,5 mln zł
wyniósł średni koszt strat poniesionych w wyniku ataku hakerskiego na polskie przedsiębiorstwo w 2017 roku

Niezawodność, bezpieczeństwo i szybkość **w działaniu**

W Soflab Technology korzystamy z wiedzy doświadczonych specjalistów, aby zaoferować rozwiązania bezpieczeństwa IT, które są odpowiedzią na kluczowe wyzwania, przed którymi stoją dziś organizacje. Dbanie o bezpieczeństwo rozwiązań IT oraz danych w nich zawartych stało się krytyczne dla ochrony danych firm i jej ciągłości działania. Soflab pomaga skutecznie dbać o to, aby nie doszło do zdarzeń mogących zagrozić biznesowej przyszłości firmy i odpowiedzialności prawnej osób nią zarządzających.

- zapobiegaj stratom finansowym
- chroń markę przed utratą reputacji
- zarządzaj ryzykiem
- określ rzeczywisty poziom zabezpieczeń organizacji
- odpowiadaj na zaawansowane zagrożenia
- spełnij wymogi zgodności z przepisami

Co **robimy?**

„Najlepszą obroną jest atak", „lepiej zapobiegać niż leczyć" – te stwierdzenia rzadko znajdują zastosowanie jednocześnie w tej samej sytuacji. Wyjątkiem jest bezpieczeństwo IT.

Prewencja raczej nie kojarzy się z działaniami ofensywnymi, a jednak w przypadku testów penetracyjnych okazuje się, że **aby skutecznie bronić się przed atakiem, warto wcześniej zaatakować** własny system w sytuacji kontrolowanej, aby znaleźć wszelkie jego słabe punkty, lub błędy konfiguracyjne. Dzięki przeprowadzeniu takiego audytu bezpieczeństwa możemy zapobiec ich odkryciu i wykorzystaniu przez osoby niepowołane.

Portfolio **naszych usług**

Weryfikacja dokumentacji projektowej pod kątem założeń bezpieczeństwa

Zapewniamy kompleksowe uzgodnienie każdego projektu z aktualnie obowiązującymi regulacjami prawnymi, w tym **RODO.** Dołączenie specjalisty od bezpieczeństwa do zespołu wdrożeniowego już na etapie projektowania danego rozwiązania, pozwala na uniknięcie wielu błędów oraz daje szanse na duże oszczędności w późniejszym etapie cyklu życia aplikacji lub infrastruktury IT.

Testy penetracyjne

Wykonujemy testy penetracyjne, czyli kontrolowane próby przełamania zabezpieczeń, w zależności od potrzeb Klientów bez znajomości szczegółów budowy systemu **(testy black-box),** z częściową wiedzą **(grey-box),** jak i testy połączone z przeglądem kodu **(testy white-box).**

Testy bezpieczeństwa przeprowadzamy w oparciu o standardy OWASP (Open Web Application Security Project), w szczególności OWASP TOP 10 Classification, OWASP ASVS (Application Security Verification Standard) i OWASP Testing Guide 4.0 (w tym najlepsze praktyki w testowaniu bezpieczeństwa).

Wykonujemy **testy bezpieczeństwa aplikacji mobilnych** z wykorzystaniem emulatorów oraz na fizycznych urządzeniach mobilnych, w oparciu o klasyfikację podatności i zagrożeń z listy TOP 10 Mobile Risks organizacji OWASP.

Audyt konfiguracji zabezpieczeń infrastruktury, poszczególnych systemów/usług

Audyt przeprowadzamy **za pomocą technik manualnych oraz przy użyciu narzędzi automatycznych.** Obejmuje: analizę, weryfikację podejścia do konfiguracji, sprawdzenie bezpieczeństwa konfiguracji z użyciem narzędzi automatycznych i analizę ryzyka opartego na wynikach i zalecenia optymalizacji bezpieczeństwa. Przedmiotem testów są m.in.: uprawnienia, nieautoryzowany dostęp, konfiguracja oraz brakujące poprawki.

Audyt bezpieczeństwa infrastruktury teleinformatycznej

W ramach audytu wykonujemy testy penetracyjne, skanowanie podatności, jak i przeglądy konfiguracji **kluczowych elementów infrastruktury teleinformatycznej.**

Testy obejmują: sieci i podsieci, urządzenia sieciowe, hosty, oraz protokoły sieciowe, porty TCP i UDP, platformy systemowe, usługi sieciowe i inne.

Szeroki zakres metod wdrażania obejmuje:

- rozpoznawanie topologii sieci/serwera;
- testowanie wykrytych urządzeń sieciowych;
- testowanie sieci bezprzewodowych.

Jak to **robimy?**

Każda zapora może zostać przerwana, jest to tylko kwestia czasu i umiejętności. Zawsze jest ryzyko. Nasza usługa polega na tym, aby je zminimalizować.

- **Identyfikujemy podatności** firmy oraz funkcjonujących w niej systemów na świadome i nieświadome incydenty bezpieczeństwa.
- **Oceniamy zdolność do wykrywania i wytrzymania typowych ataków.**
- **Pomagamy** w określeniu **krytycznych zmian lub działań w zakresie bezpieczeństwa i w przygotowaniu planu działań budujących bezpieczeństwo w firmie.**

Angażujemy się w różnych momentach cyklu rozwoju oprogramowania. To wyróżniające nas na rynku podejście pozwala nam wspierać naszych Klientów na każdym etapie projektu, umożliwiając zaplanowanie niezbędnych prac testowych, identyfikacje potencjalnych zagrożeń i wyznaczenie założeń projektowych dla wdrażanego rozwiązania. Dostarczamy praktyczne wnioski w przejrzystej formie. Raport wyników zawiera opis rekonstrukcji błędu, możliwe zagrożenia i działania naprawcze.

Testowanie odporności na ataki DoS/DDoS

Celem jest wykrycie braku ochrony przed niechcianymi działaniami, co prowadzi do zablokowania dostępu do danej usługi w Internecie. Weryfikujemy najczęstsze rodzaje ataków DDoS:

UDP flood attack

Wykonywane przez dedykowane skrypty, które generują pakiety UDP o losowych rozmiarach i przedziałach czasowych przypisanych do szacowanego obciążenia.

HTTP flood attack

Na podstawie symulacji różnych metod (POST i GET) obsługiwanych przez aplikację. Wygenerowany ruch aplikacji nie będzie odpowiadał standardowemu użytkownikowi, ale oczekiwanemu obciążeniu zasobów.

Audyt statyczny kodu źródłowego

Głównym celem jest **zidentyfikowanie nieskutecznych konstrukcji i fragmentów kodu, które odzwierciedlają złe praktyki programistyczne lub błędy bezpieczeństwa.** Analiza statyczna pozwala:

- zwiększyć wydajność i stabilność,
- unikać typowych błędów programowania,
- narzucać zasady i standardy kodowania,
- zwiększyć bezpieczeństwo na każdym kolejnym etapie testowania.

Analiza oparta jest na standardach OWASP, w szczególności na klasyfikacji OWASP Top 10 i OWASP Mobile Top 10, ale także na weryfikacji zgodności z: SANS 25, HIPAA, Mitre CWE, CVE NIST, PCI DSS, MISRA, BSIMM.

Testy socjotechniczne, testy procedur i zabezpieczeń fizycznych

Nasi audytorzy przeprowadzą **kontrolowany atak socjotechniczny,** aby zweryfikować poziom zabezpieczeń, przestrzegania procedur bezpieczeństwa oraz poziom świadomości bezpieczeństwa informacji w organizacji np.:

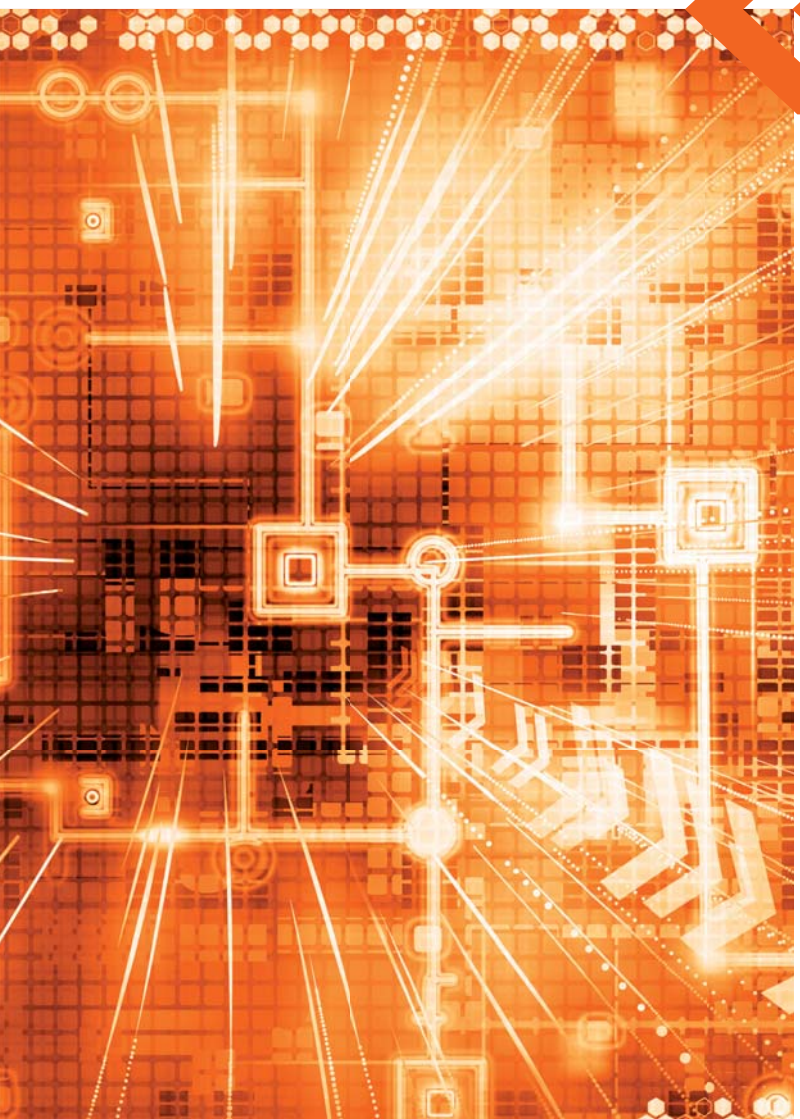
- próba nakłonienia pracownika do uruchomienia oprogramowania z dostarczonego pendrive;
- kampania e-mailingowa;
- próba nieautoryzowanego wejścia do budynku.

Możliwe jest przeprowadzenie **szkolenia dla pracowników** z zakresu bezpieczeństwa teleinformatycznego i aktualnych zagrożeń technicznych i socjotechnicznych.

Techniki **testowania**

Podczas testów zostaną wykorzystane ręczne i automatyczne techniki testowania. Obie wzajemnie się uzupełniają:

- **Wykorzystujemy różne narzędzia automatyczne,** jak np. Nessus, Burp Proxy Professional, OWASP ZAP, SOAP UI, Metasploit oraz własny framework programistyczny, co zmniejsza ryzyko pomijania luk bezpieczeństwa przez jeden z programów.
- **Audyt ręczny** obejmuje manualną weryfikację aplikacji lub podatności i służy do wykrywania błędów logicznych, lub zaimplementowanej funkcjonalności. Ręczne przeprowadzanie ataków pozwala na efektywne pomijanie lub analizę filtrów ochrony zaimplementowanej w aplikacji oraz systemach firewall.



Dlaczego **Soflab**

know-how
na podstawie wielu projektów
w różnych branżach

zespół
kompetentnych ekspertów

gotowe, sprawdzone,
oparte na praktyce
procedury testowania

doświadczenie i dobór
odpowiednich technologii
i narzędzi

autorska metodyka testów
Soflab Test Approach

własny Testlab urządzeń
do testów aplikacji mobilnych

SOFLAB

Zapytaj o specjalną ofertę dla Ciebie:
oferta.security@soflab.pl