CYBERBLOCK S.A.
biuro@cyberblock.pl

ul. Stanisława Moniuszki 1A
00-014 Warszawa

www.cyberblock.pl

CYBER BLOCK

Bezpieczeństwo IT

Audyt bezpieczeństwa IT

Audyt bezpieczeństwa w firmie umożliwia weryfikację funkcjonowania rozwiązań techniczno-organizacyjnych z wytycznymi/normami w zakresie bezpieczeństwa przetwarzanych danych. W jego efekcie firma otrzyma raport podatności/niezgodności, zawierający precyzyjny opis znalezionych przez nas błędów/niezgodności wraz z rekomendacją środków zaradczych.

Cel audytu:

- Weryfikacja funkcjonowania rozwiązań techniczno-organizacyjnych z wytycznymi/normami w zakresie bezpieczeństwa przetwarzanych danych.

Korzyści:

- Sprawdzenie zgodności stosowanych rozwiązań techniczno-organizacyjnych z wytycznymi/normami,
- Poznanie rekomendowanych środków zaradczych,
- Podniesienie bezpieczeństwa przetwarzanych danych.

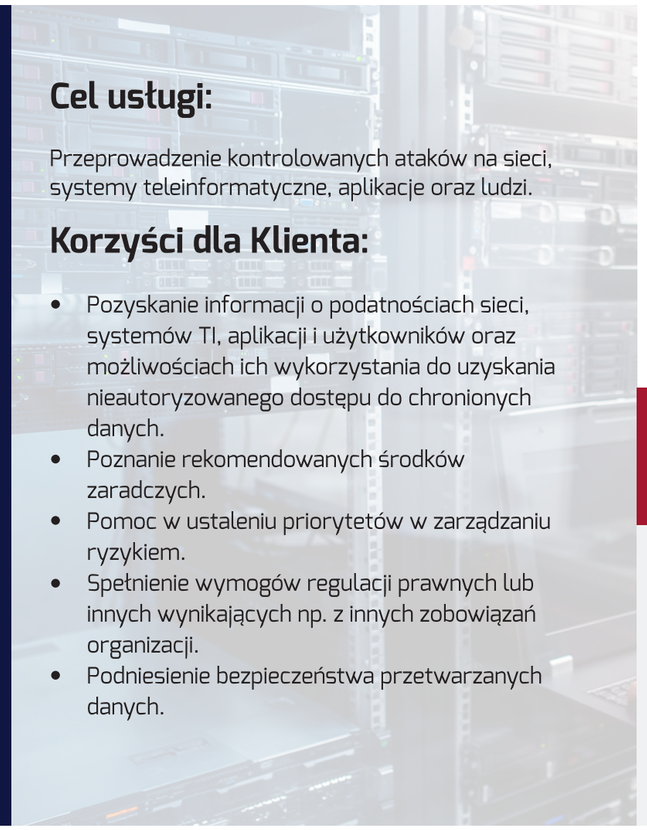
Testy penetracyjne

Rzeczywistą i wiarygodną ocenę stanu bezpieczeństwa IT można uzyskać wyłącznie przeprowadzając Testy Penetracyjne, polegające na przeprowadzeniu kontrolowanych ataków na użytkowane sieci, systemy teleinformatyczne, aplikacje oraz ludzi (od zewnątrz sieci, jak i z jej wnętrza).
Testy mogą być prowadzone wg modelu:

„Blackbox” - prowadzone przy zachowaniu minimalnej wiedzy na temat badanego zakresu,

„Whitebox” - prowadzone przy współpracy z osobami odpowiedzialnymi za administrację i bezpieczeństwo IT oraz z dostępem do dokumentacji dotyczącej badanego zakresu,

„Greybox” - prowadzone zamiennie wg modelu „Blackbox” i „Whitebox” - w zależności od badanego obszaru.



Cel usługi:

Przeprowadzenie kontrolowanych ataków na sieci, systemy teleinformatyczne, aplikacje oraz ludzi.

Korzyści dla Klienta:

- Pozyskanie informacji o podatnościach sieci, systemów TI, aplikacji i użytkowników oraz możliwościach ich wykorzystania do uzyskania nieautoryzowanego dostępu do chronionych danych.
- Poznanie rekomendowanych środków zaradczych.
- Pomoc w ustaleniu priorytetów w zarządzaniu ryzykiem.
- Spełnienie wymogów regulacji prawnych lub innych wynikających np. z innych zobowiązań organizacji.
- Podniesienie bezpieczeństwa przetwarzanych danych.

Testy socjotechniczne

Wiedza pracowników firmy na temat zagrożeń teleinformatycznych powinna być poddawana regularnej kontroli. Diagnoza przeprowadzona za pomocą testów z wykorzystaniem socjotechniki pozwala na zbudowanie świadomości zagrożeń oraz szybkie i wymierne ustalenie priorytetów w zakresie działań związanych z bezpieczeństwem. Zakres testów obejmuje interakcje pośrednie oraz bezpośrednie, które mogą być realizowane np. przez przeprowadzenie ataku socjotechnicznego na pracowników firmy.

Cel audytu:

Sprawdzenie odporności pracowników na stosowanie metod socjotechnicznych w celu wydobycia poufnych informacji o firmie, stosowanych hasłach itp.

Korzyści:

- Podniesienie świadomości pracowników w zakresie stosowania socjotechniki w atakach komputerowych.
- Ocena ilościowa obrazująca jaka liczba pracowników jest podatna na ataki z użyciem socjotechniki.
- Wykazanie słabych punktów w komunikacji firmy, które mogą zostać wykorzystane do ataków socjotechnicznych.
- Potwierdzenie jakości treningów oraz szkoleń użytkowników systemów TI.
- Podniesienie bezpieczeństwa przetwarzanych danych.

Szkolenia z zakresu bezpieczeństwa IT

Oferta szkolenia z zakresu bezpieczeństwa IT jest dedykowana osobom, które pracują z komputerem i wykorzystują sieć internetową. Dzięki szkoleniu przekazujemy naszym Klientom wiedzę na temat form ataku jakie stosują cyberprzestępcy oraz sposobów obrony przed takimi działaniami.

Szkolenie trwa od 2-4 godzin i jest prowadzone w formie wykładu, podczas którego demonstrujemy potencjalny atak. Zakres szkolenia każdorazowo dostosowujemy do indywidualnych potrzeb naszych Klientów.

Zakres tematyki szkoleń:

- Ataki socjotechniczne (email, WWW, komunikatory, telefon),
- Jak i skąd przestępcy pozyskują dane na Twój temat?
- Jakie hasło jest bezpieczne?
- Ataki na sieci WiFi,
- Jak bezpiecznie korzystać z komputera i telefonu?

Doradztwo

Naszym Klientom oferujemy doradztwo oraz wsparcie w zakresie:

- Dynamicznej analizy złośliwego oprogramowania (na podstawie przesłanej wiadomości ocenimy, czy zawiera złośliwe oprogramowania i zwrotnie przekazujemy rekomendację dotyczącą dalszego postępowania),
- Wdrażania szyfrowania wiadomości email, szyfrowania połączeń głosowych itp.

Bezpieczeństwo informacji

zabezpieczenia kontrinwigilacyjne

Dbając o bezpieczeństwo informacji wykonujemy audyt wykrywający techniki inwigilacyjne. Wynikiem audytu jest pisemny raport, w którym proponujemy zabezpieczenia przed ulotem informacji drogą elektroniczną.

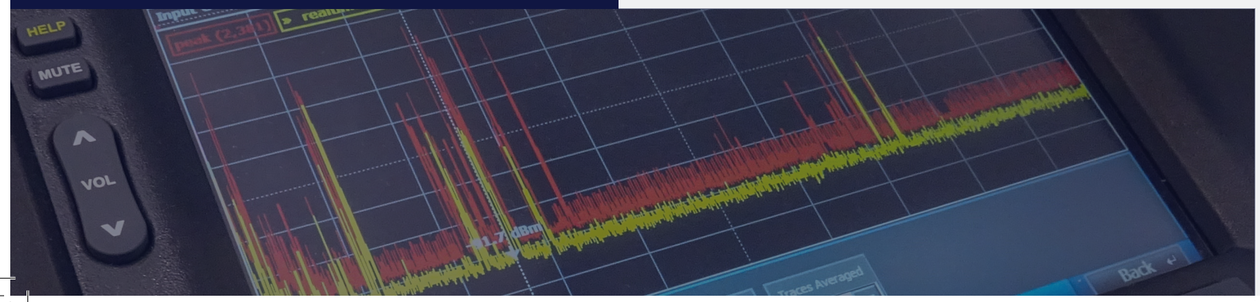
Audyt WTI[1]

Lokalizujemy:

- Urządzenia rejestrujące,
- Odsłuch radiowy (analogowy, cyfrowy, z widmem rozproszonym, transmisją pulsacyjną, WiFi i GSM),
- Podsłuch w podczerwieni i laserowy,
- Podsłuch po sieci energetycznej,
- Podsłuch po sieciach niskonapięciowych, TV, sieci telefonicznej,
- Podsłuch stetoskopowy (przy dostępie do pomieszczeń przyległych),
- Ukryte mikrokamery przewodowe i bezprzewodowe,
- Lokalizatory GPS i GSM,
- Keyloggery komputerowe.

Wykrywanie techniki inwigilacyjnej realizujemy przez:

- Wywiad źródłowy,
- Oględziny i inspekcję miejsca badania,
- Pomiary i analizę pełnego spektrum częstotliwości radiowych w zakresie 1 MHz -21 GHz (sygnał analogowy, cyfrowy, z widmem rozproszonym),
- Badania detektorem łączy nieliniowych ścian, podłóg, sufitów (Wykrywanie wszelkich urządzeń podsłuchowych, rejestrujących, lokalizujących),
- Analizę obecności krótkich impulsów w częstotliwościach 2G (GSM, iDEN AMPS, PHS, PCS), CDMA (American 3G) WCDMA (3G Europejskiej),
- Badanie na obecność podsłuchów laserowych IR.
- Badanie linii telefonicznych i linii niskonapięciowych, linii energetycznej,
- Fizyczną inspekcję urządzeń elektronicznych i komputerów,
- Badanie termowizyjne.



Analiza sieci bezprzewodowych Wi-Fi oraz przesyłanych urządzeń peryferyjnych

Po badaniu anty-podsłuchowym sporządzamy pisemny protokół z przeprowadzonych czynności wraz z sugestiami ewentualnych zmian dla poprawy bezpieczeństwa informacji. Dostarczamy również zobowiązanie poufności. Ponad to nasz klient otrzymuje wskazówki i informacje jak zmniejszyć ryzyko i skutki inwigilacji.

W naszej pracy wykorzystujemy najnowsze systemy (detektory NLJD) i urządzenia m.in. najbardziej zaawansowany wykrywacz podsłuchów na świecie – urządzenie OSCOR Green firmy REI (USA), który zastąpił ceniony aczkolwiek nieprodukowany już i wycofywany ze służb OSCOR 5000.

Sprawdzenie i analiza telefonów komórkowych, tabletów i kart SIM

Po analizie telefonów komórkowych i urządzeń mobilnych jesteśmy w stanie odzyskiwać ich hasła, skasowane dane, SMS-y oraz wykrywać w nich aplikacje szpiegujące.

Nasza firma stosuje najbardziej zaawansowane metody wykorzystywane przez informatykę śledczą, m.in. urządzenie UFED Touch Ultimate produkcji Izraelskiej, które oferuje najskuteczniejsze dekodowanie, odzyskiwanie danych z telefonu i innych urządzeń mobilnych, a także pozwala na ich analizę i stworzenie raportów. Sprzęt ten wykorzystuje metody zarówno logicznego, jak i fizycznego odzyskiwania danych z karty SIM, SMS z telefonu i innych plików i danych, nawet usuniętych. Dzięki UFED Touch Ultimate wszelkie hasła, dane czy systemy plików ze smartfonów, tabletów czy telefonów komórkowych mogą zostać skutecznie odzyskane. Analiza urządzeń przenośnych oraz ekstrakcja danych z UFED Touch Ultimate to absolutny przełom, który wykorzystuje wszystkie najnowocześniejsze i najskuteczniejsze metody oraz możliwości: wykrywanie aplikacji szpiegujących i inwigilujących typu SpyPhone,

Analiza komputerów pod kątem nieuprawnionego monitoringu (urządzenia i oprogramowanie)

- Wykrywanie nieuprawnionego oprogramowania typu keylogger lub innego (np. rootkity) wykradającego dane użytkownika,
- Wykrywanie sprzętowych urządzeń typu keylogger,

Zabezpieczenia

Oferujemy konfigurację i zabezpieczenia pomieszczeń przed ulotem informacji zarówno w formie stałej ,,klatka faradaya, oraz przy pomocy urządzeń separujących i zagłuszających.

Cel realizacji zabezpieczeń:

Ochrona pomieszczeń przed:

Inwigilacją zewnętrzną
- Zagłuszanie sygnału GSM (emisji i transmisji na zewnątrz),
- Zagłuszanie sygnału Wi-Fi,
- Zabezpieczenie strefy pomieszczenia przed ingerencją z zewnątrz (Zabezpieczenie okien, Zabezpieczenie ścian, Zabezpieczenie stropu - przestrzeń nad podwieszanym sufitem)

Możliwością nieautoryzowanego utrwalania dźwięku (nagrywanie wewnątrz pomieszczeń) – zagłuszarki nagrywania,

Wnoszeniem urządzeń elektronicznych .

Klatka Faradaya

Klatki Faradaya, (nazywane inaczej kabinami elektromagnetycznymi), chronią one przed działaniem zewnętrznych pól elektromagnetycznych.
Gwarantują bezpieczeństwo w zakresie:

- Ekranowania,
- Filtrowania,
- Zabezpieczenia elektrostatycznego.

Klatki Faradaya nie przepuszczają fal – ani do wewnątrz, ani na zewnątrz, dzięki czemu pomieszczenie antypodsłuchowe jest bezpieczne.

Przygotowane pomieszczenia antypodsłuchowe zabezpieczają przed:

- Podsłuchem radiowym,
- Podsłuchem poprzez telefony komórkowe,
- Podsłuchem IR i laserowym,
- Przed podsłuchem sejsmicznym,
- Skrytym rejestrowaniem rozmów,
- Przechwytem emisji z komputerów, ekranów itp.

Audyt oraz projektowanie systemu bezpieczeństwa informacji

Audyt

Zakresem prowadzonego audytu objęte jest:

- Ustalenie administratora danych w odniesieniu do analizowanych informacji (dane należące do administratora oraz powierzone),
- Precyzyjne określenie zbiorów danych osobowych,
- Sprawdzenie podstaw prawnych przetwarzania danych osobowych z uwzględnieniem ich zakresu i zasad wynikających z przepisów ustawy o ochronie danych osobowych,
- Analiza posiadanej dokumentacji,
- Analiza zabezpieczenia systemów informatycznych pod kątem ich zgodności z przepisami prawa,
- Sprawdzenie wdrożenia i funkcjonowania procedur i zasad ochrony danych osobowych w odniesieniu do osób mających dostęp do danych,
- Sprawdzenie innych elementów mających wpływ na poziom zabezpieczenia przetwarzanych danych osobowych.

Audyt zakończony jest raportem, w którym nie tylko opisujemy stan faktyczny oraz stopień ryzyka, ale również proponujemy konkretne rozwiązania podnoszące poziom ochrony danych osobowych w firmie – np. wzór treści klauzul dotyczących zgody na przetwarzanie danych, obowiązków informacyjnych itd.

Projektowanie systemu bezpieczeństwa informacji:

- Opracowywanie dokumentacji w ramach Systemu Zarządzania Bezpieczeństwem Informacji (SZBI),
- Opracowanie dokumentacji bezpieczeństwa dla systemów teleinformatycznych, w których przetwarzane będą informacje niejawne i zgodności procedur Klientów z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (SWB, PBE, Analiza ryzyka),
- Opracowywanie dokumentacji bezpieczeństwa zasobów Klientów w zakresie danych osobowych i zgodności procedur z wytycznymi przedstawionymi w Rozporządzeniu o ochronie danych osobowych (RODO).

Korzyści:

- Weryfikacja systemu zarządzania bezpieczeństwem organizacji gospodarczej,
- Ochrona procesów biznesowych i systemu informacyjnego w firmie,