NARODOWY INSTYTUT STUDIÓW STRATEGICZNYCH

OFERTA

DLA MIAST, GMIN,

INSTYTUCJI FINANSOWYCH

I PODMIOTÓW KOMERCYJNYCH

DOTYCZĄCA

ZAGADNIEŃ ZWIĄZANYCH Z CYBERBEZPIECZEŃSTWEM

Naszym celem nadrzędnym jest dostarczenie wysoce specjalistycznych usług obejmujących pełne spektrum zagadnień związanych z bezpieczeństwem IT. Naszym głównym atutem jest zespół ekspertów posiadających ponad dziesięcioletnie doświadczenie w bezpieczeństwie IT ofensywnym oraz defensywnym, w tym także implementacji systemów oraz weryfikacji poziomów zabezpieczeń systemów zaimplementowanych. Powyższe cele realizujemy poprzez m.in. udostępnianie Klientom systemów oraz usług, które pozwolą zapewnić najwyższy poziom bezpieczeństwa ich informacji oraz procesów biznesowych. Do głównych naszych specjalizacji należą:

- tworzenie systemów krytycznych dla bezpieczeństwa Klienta np. system autoryzacji użytkowników,
- tworzenie systemów zabezpieczających nietypowe organizacje oraz procesy np. infrastrukturę honeypot symulującą prawdziwą infrastrukturę naszego Klienta,

- testy bezpieczeństwa rozwiązań IT, systemów automatyki przemysłowej oraz urządzeń embedded,

- symulację ataku cyberprzestępcy,

- rekonfiguracja istniejącej infrastruktury mająca na celu zwiększenie poziomu zabezpieczeń,

- prace badawczo-rozwojowe związane z produktami bezpieczeństwa IT np. wybór najlepszego rozwiązania dostępnego na rynku w kontekście już istniejącej infrastruktury Klienta,

- wsparcie przy analizie złożonych technicznie incydentów bezpieczeństwa np. włamanie z wykorzystaniem nieznanej luki,

- inżynierię odwrotną oprogramowania np. firmware urządzenia lub programu malware, który zaatakował Klienta.

- specjalistyczne usługi odzyskiwania danych, kasowania danych oraz informatyki śledzcej z nośników typu: dyski twarde HDD, dyski SSD, macierze RAID w róznych konfiguracjach, telefony, smartfony I urządzenia mobilne, pendrive, karty pamięci I inne nosniki wyposazone w pamięci typu flash.

Posiadamy również doświadczenie w analizie i projektowaniu systemów antyfraudowych służących zarówno do detekcji jak i prewencji incydentów związanych z wyłudzeniami. Posiadamy ogromne doświadczenie w sprawach IT. Posiadamy zespół sprawdzonych programistów IT biegle programujących w wielu językach informatycznych, w szczególności: Pyton, JAVA, JAVA SCRIPT, WINDOWS, ANDROID, iOS itp. *mogących pracować w formule body leasing lub prowadzić zlecone projekty informatyczne.*

Testy penetracji aplikacji.

Jest to usługa związana z prowadzeniem testów penetracyjnych aplikacji webowych lub aplikacji napisanych w technologii klient-serwer, czy też aplikacji na urządzenia mobilne. W zakres testów wchodzą także testy interfejsów aplikacji czy API. Testy mogą być prowadzone w modelu black lub gray box. W wyniku przeprowadzonych prac Klient otrzymuje raport składający się z części technicznej oraz części przeznaczonej dla kadry zarządzającej. Część techniczna opisuje szczegółowo znalezione podatności wraz z rekomendacjami naprawczymi. Część zarządcza, to wysokopoziomowe podsumowanie dla kierownictwa, w którym znajdują się najważniejsze aspekty prowadzonych prac wraz z rekomendacjami wysokopoziomowymi, jeśli takie występują.

Analiza / Doradztwo w projektach w kontekście bezpieczeństwa IT.

Jest to usługa polegająca na uczestnictwie naszych inżynierów w projektach realizowanych przez Klienta i spojrzenie na dany projekt, na dowolnym jego etapie, z punktu widzenia bezpieczeństwa teleinformatycznego. Ocenie podlegają wszystkie te aspekty projektu, które mogą spowodować zwiększenie ryzyka po stronie Klienta w przypadku wdrożenia ocenianego projektu. W wyniku przeprowadzonych prac Klient otrzyma raport, który zawierał będzie ocenę analizowanego projektu, ewentualne rekomendacje czy szczegóły techniczne, jeżeli będą one konieczne do lepszego wyeksponowania potencjalnych ryzyk płynących z realizacji ocenianego projektu dla Klienta.

Inżynieria odwrotna oraz audyt kodu.

Inżynieria odwrotna to usługa polegająca na odwróceniu binarnej wersji aplikacji do postaci grafu czy drzewa prezentującego rozpoznane działanie aplikacji. Najczęstszymi pracami tego typu jest analiza złośliwego oprogramowania realizowana dla instytucji finansowych, których klienci bardzo często padają ofiarą tego typu ataków. Audyt kodu, to inaczej testy penetracyjne typu white box, czyli sytuacja, w której mamy dostęp do kodu źródłowego badanej aplikacji. Celem prowadzonej analizy jest wyłapanie jak największej liczby błędów mogących skutkować wystąpieniem potencjalnych podatności z OWASP TOP 10 w przypadku aplikacji webowych czy podatności np. typu buffer overflow w przypadku aplikacji natywnych. Oba powyższe działania kończą się raportem, w którym przedstawione są wyniki inżynierii odwrotnej bądź znalezione podatności w przypadku analizy kodu. Oprócz części technicznej tak samo i w tym przypadku mamy część przeznaczoną dla kierownictwa, w której wyniki omówione są wysokopoziomowo.

Bezpieczeństwo sprzętu, projekty związane z kartami mikroprocesorowymi.

Są to projekty związane z analizą urządzeń, projektowaniem urządzeń, bądź analizą lub projektowaniem aplikacji dla kart mikroprocesorowych np. JAVA card. Projekty te nie muszą być ściśle związane z bezpieczeństwem teleinformatycznym. W tym

przypadku zakres i sposób prezentacji wyników prac ustalany jest indywidualnie i jest zależny od realizowanego wspólnie przez nas i Klienta projektu.

Zaawansowana analiza incydentów bezpieczeństwa i analiza powałmaniowa.

W przypadku, kiedy Klient posiada zespół, który zajmuje się obsługą incydentów bezpieczeństwa i zespół ten stwierdzi, że incydent jest zbyt złożony lub zbyt zaawansowany technologicznie, aby mogli sobie sami poradzić, świadczymy usługę trzeciej linii wsparcia dla takich sytuacji. Polega to na wsparciu zespołu obsługującego incydenty w zaawansowanej analizie tych przypadków. Dla skutecznego działania potrzebna jest ścisła współpraca pomiędzy naszymi inżynierami a inżynierami Klienta bądź zapewnienie dostępu do systemów objętych incydentem bezpieczeństwa dla naszych inżynierów. W ramach takiego wsparcia analizowane są logi systemowe, logi z urządzeń sieciowych oraz innych urządzeń (np. IPS/IDS, FW), oraz prowadzone są działania z dziedziny informatyki śledczej mające na celu ustalenia szczegółowego łańcucha zdarzeń. W przypadku odnalezienia złośliwego oprogramowania, które jest źródłem incydentu możliwe jest wykonanie inżynierii odwrotnej takiego oprogramowania zgodnie z opisem przedstawionym w punkcie poświęconym inżynierii odwrotnej.
Ponadto pomagamy w przeprowadzeniu analizy powłamaniowej, której celem jest dokładne ustalenie kto, kiedy i w jaki sposób przełamał zabezpieczenia Klienta i przeprowadził skuteczny atak. Prace te prowadzone są w bardzo podobny sposób do tego z analizy incydentów bezpieczeństwa.

Testy profilowane.

Są to testy penetracyjne sprawdzające odporność organizacji na ataki cybernetyczne. Atakowany jest nie pojedynczy system a wyznaczone cele w organizacji. Celami mogą być np. Active Directory, systemy ERP, systemy kadrowo-płacowe, systemy automatyki przemysłowej czy inne krytyczne dla organizacji elementy infrastruktury teleinformatycznej. Test taki musi składać się z minimum trzech celi, a na każdy z nich przypada około trzydziestu dni roboczych realizacji.
W wyniku przeprowadzonych prac Klient otrzymuje raport składający się z części technicznej oraz części przeznaczonej dla

kierownictwa. Część techniczna opisuje szczegółowo znalezione podatności wraz z rekomendacjami naprawczymi. Część zarządcza, to wysokopoziomowe podsumowanie dla kierownictwa, w którym znajdują się najważniejsze aspekty prowadzonych prac wraz z rekomendacjami.

Ataki socjotechniczne.

Ataki socjotechniczne polegają na próbie przekonania użytkowników, aby wykonali korzystną dla nas akcję, która z reguły jest zakazana w funkcjonujących Politykach Bezpieczeństwa w firmach. W ramach ataku przeprowadzane są kampanie mailingowe, phishing czy w wyjątkowych sytuacjach kontakt telefoniczny. Efektem takiego ataku jest ocena świadomości pracowników Klienta na temat zagrożeń atakami cybernetycznymi. Do dobrych praktyk należy przeprowadzenie szkoleń awarenesowych dla pracowników wraz z zaprezentowaniem wyników testu.

Bezpieczeństwo miękkie – ISO 27001, ISO 22301, ABI.

Pomagamy naszym Klientom także w utrzymywaniu i wdrażaniu norm związanych z bezpieczeństwem informacji takich jak ISO 27001 czy 22301. Możemy także wspomagać działania Administratora Bezpieczeństwa Informacji. Projekty z tego obszaru traktujemy bardzo indywidualnie, dlatego każdorazowo uzgadniamy zakres, charakter oraz szczegółową formę współpracy.