Katalog usług

w zakresie bezpieczeństwa IT w organizacji

Poznańskie Centrum
Superkomputerowo-Sieciowe
Dział Bezpieczeństwa ICT
Ul. Jana Pawła II 10, 61-139 Poznań

Kontakt:
Gerard Frankowski
email: gerard.frankowski@man.poznan.pl
tel. 61 858 20 67, 693 91 00 24
fax 61 858 21 51

Poznań, kwiecień 2017

SPIS TREŚCI

1 Informacje o Oferencie

Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS, http://www.pcss.pl), afiliowane przy Instytucie Chemii Bioorganicznej PAN, jest jednostką naukowo-badawczą o charakterze non-profit. PCSS jest operatorem sieci krajowej PIONIER, sieci miejskiej POZMAN, uczestnikiem ponad 100 polskich i europejskich projektów naukowo-badawczych oraz centrum komputerowym, udostępniającym usługi na terenie całego kraju. W związku z tym PCSS od szeregu lat zajmuje się także problematyką bezpieczeństwa w ramach działającego od 1996 r. **Działu Bezpieczeństwa ICT** (wcześniej Zespołu Bezpieczeństwa, http://security.psnc.pl) – grupy doświadczonych specjalistów z zakresu bezpieczeństwa informacji oraz bezpieczeństwa teleinformatycznego. Członkowie grupy zajmują się świadczeniem usług z zakresu bezpieczeństwa dla Klientów zewnętrznych oraz utrzymaniem odpowiedniego poziomu bezpieczeństwa infrastruktury teleinformatycznej PCSS oraz zasobów sieci optycznych PIONIER i POZMAN. Poza pracą operacyjną Dział uczestniczy w projektach badawczych i wdrożeniowych, gdzie służy swoją wiedzą i doświadczeniem.

Pracownicy Działu (a wcześniej Zespołu) Bezpieczeństwa realizowali już szereg zewnętrznych projektów z zakresu bezpieczeństwa dla różnych podmiotów gospodarczych, w tym dla banków, organizacji samorządowych i międzynarodowych, a także przedsiębiorstw komercyjnych. Spośród najważniejszych zrealizowanych projektów w ciągu ostatnich lat należy wymienić:

- **UNFCCC – COP14** – testy penetracyjne sieci, audyt infrastruktury oraz monitorowanie bezpieczeństwa podczas trwania Konferencji Klimatycznej COP14 (formalna realizacja zamówienia dla Międzynarodowych Targów Poznańskich).
- **UNFCCC – COP19** – testy penetracyjne sieci oraz audyt infrastruktury dla potrzeb Konferencji Klimatycznej COP19 (formalna realizacja zamówienia dla Międzynarodowych Targów Poznańskich).
- **Kancelaria Sejmu Rzeczpospolitej Polskiej** – testy penetracyjne infrastruktury z zewnątrz oraz analiza odporności na ataki DDoS.
- **Gospodarczy Bank Wielkopolski** – szereg niezależnych zleceń w latach 2009-2011, m.in. testy penetracyjne aplikacji bankowości elektronicznej, testy penetracyjne punktu styku sieci wewnętrznej z Internetem, testy penetracyjne usługi poczty elektronicznej, konsultacje w zakresie integracji sieci wewnętrznej.
- **Bank Spółdzielczy w Sztumie** – kompleksowy audyt bezpieczeństwa, m.in. testy penetracyjne sieci wewnętrznej oraz stron internetowych, analiza Polityki Bezpieczeństwa Informacji, testy penetracyjne aplikacji bankowej, audyt infrastruktury IT.
- **Bank Spółdzielczy w Dusznikach** – kompleksowy audyt bezpieczeństwa, m.in. testy penetracyjne sieci wewnętrznej oraz stron internetowych, analiza Polityki Bezpieczeństwa Informacji, audyt infrastruktury IT, ataki socjotechniczne.

- **Urząd Miasta Poznania** – 2 kompleksowe audyty bezpieczeństwa sieci, cykliczne audyty bezpieczeństwa śluzy internetowej, cykliczne audyty bezpieczeństwa serwerów WWW i bazodanowych, projekt reorganizacji i zabezpieczenia sieci.
- **Zakład Ubezpieczeń Społecznych** – analiza bezpieczeństwa Platformy Usług Elektronicznych – ZUS PUE, w tym testowe ataki DDoS.
- **Zespół Elektrowni Pątnów – Adamów – Konin S.A.** (ZEPAK) – testy penetracyjne usług oraz sieci z zewnątrz i z wewnątrz, audyt zabezpieczeń infrastruktury.
- **Kopalnie Węgla Kamiennego Adamów i Konin** – testy penetracyjne usług oraz sieci z zewnątrz i z wewnątrz, audyt zabezpieczeń infrastruktury.
- **arvato services Polska** (**grupa Bertelsmann Media Sp. z o.o.**) – wewnętrzne testy penetracyjne środowiska sieciowego (2 niezależne zlecenia).
- **Aquanet S.A.** – kompleksowy audyt bezpieczeństwa
- **Centrum Unijnych Projektów Transportowych** – audyt zgodności z wymogami normy PN-ISO/IEC 27001.
- **IBS.pl Sp. z o.o.** – analiza bezpieczeństwa aplikacji internetowej.
- Spółka z grupy **INEA** – analiza bezpieczeństwa aplikacji internetowej.
- **internetowykantor.pl** – testy penetracyjne aplikacji internetowej.
- **Kompania Piwowarska S.A.** – analiza bezpieczeństwa aplikacji intranetowej.
- **Międzynarodowe Targi Poznańskie S.A.** – przygotowanie i realizacja kompleksowych szkoleń bezpieczeństwa w ramach Międzynarodowych Targów Zabezpieczeń SECUREX 2012 oraz 2014.
- **Narodowy Fundusz Zdrowia** oddział Katowice – 2 niezależne zlecenia testów penetracyjnych 7 aplikacji internetowych.
- **Telefonia Dialog S.A.** – testy penetracyjne aplikacji internetowej oraz usługi SIP Proxy, testy penetracyjne aplikacji Wideomonitoring (2 niezależne zlecenia).
- **Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach** – analiza bezpieczeństwa środowiska teleinformatycznego.
- **Zakład Usług Informatycznych Novum Sp. z o.o.** – kompleksowy audyt bezpieczeństwa, m.in. testy penetracyjne z zewnątrz i z wewnątrz, audyt zabezpieczeń infrastruktury, przegląd polityk i procedur bezpieczeństwa.

Wybrane listy referencyjne dostępne są do wglądu na życzenie Zamawiającego (możliwe jest przesłanie skanu drogą elektroniczną lub zapoznanie się z oryginałem dokumentu w siedzibie PCSS).

Dział realizuje (bądź zrealizował) również inne zadania w zakresie ochrony systemów IT:

- udział w projekcie Polskiej Platformy Bezpieczeństwa Wewnętrznego (we współpracy m.in. z KG Policji w Warszawie oraz KW Policji w Poznaniu) – usługi na rzecz wspomagania pracy operacyjnej Policji, sądów, prokuratur,

- udział w projekcie Zintegrowanej Platformy Teleinformatycznej dla potrzeb Policji – odpowiedzialność za bezpieczeństwo całości Platformy, wdrożenie systemów bezpieczeństwa (system monitorowania, system detekcji intruzów),
- udział w projekcie Centrum Innowacji Microsoft w zakresie „Bezpieczeństwa i usług outsourcingowych",
- implementacja oraz rozwój systemów i rozwiązań bezpieczeństwa: rozproszony system detekcji intruzów MetaIDS, system administracji i raportowania SARA, system ochrony przed atakami DoS/DDoS, zaawansowany system detekcji anomalii w sieciach – projekt SECOR,
- zadania bezpieczeństwa o różnym charakterze w projektach naukowo-badawczych, m.in.: EGEE-II/EGEE-III, GN3/GN3+/GN4, PRACE (europejskie), Clusterix, e-Podręczniki do kształcenia ogólnego, Krajowy Magazyn Danych, MAN-HA, PL-Grid/PL-Grid+/PL-GridNG, Progress, SGIGrid, UNIZETO (krajowe),
- działalność w ramach Klastra „Obszar Zaawansowanych Technologii Bezpieczeństwa i Obronności",
- zabezpieczanie dostępu do sieci wirtualnej Urzędu Miasta Poznania,
- działalność zespołu PIONIER CERT,
- prowadzenie zamkniętych i otwartych szkoleń w zakresie bezpieczeństwa teleinformatycznego dla przedstawicieli Policji, Prokuratury oraz Sądownictwa, studentów, programistów, administratorów, pracowników IT itd.,
- publikacja raportów dotyczących m.in. bezpieczeństwa sieci mobilnych, serwerów WWW, zabezpieczeń sesji internetowych, przeglądarek internetowych oraz bezpieczeństwa portali bankowości elektronicznej,
- cykliczne audyty sieci, usług i systemów wewnętrznych PCSS.

2 Szczegółowy katalog usług

PCSS świadczy kompleksowy zakres usług w dziedzinie bezpieczeństwa teleinformatycznego, obejmujący w szczególności prace wymienione poniżej.

2.1 Usługi audytorskie

Usługi audytorskie koncentrują się wokół oceny aktualnego poziomu zabezpieczeń jednego lub wielu elementów infrastruktury Zamawiającego. W zależności od potrzeb, częste zastosowanie mają kompleksowe audyty teleinformatyczne, składające się z wielu elementów wymienionych poniżej, odnoszących się do poszczególnych składników lub warstw badanej sieci teleinformatycznej.

2.1.1 Audyt wstępny

Usługa obejmuje identyfikację podstawowych słabości związanych z bezpieczeństwem w obszarze IT. Główny nacisk podczas realizacji tej usługi położony jest na weryfikację:

- bezpieczeństwa fizycznego,
- odpowiedniego projektu sieci,
- konfiguracji kluczowych urządzeń sieciowych,
- zdalnego dostępu do sieci,
- polityki filtrowania ruchu i skuteczności systemów antywirusowych,
- bezpieczeństwa stacji roboczych.

Prace wykonywane są z pełną wiedzą o analizowanych systemach i w ścisłej, bieżącej współpracy z pracownikami Zamawiającego.

2.1.2 Testy penetracyjne

Usługa ta ma na celu sprawdzenie szczelności całej sieci organizacji lub jej wybranego komponentu (w tym pojedynczej aplikacji). Może być realizowana zarówno w modelu *black box* (brak informacji o budowie sieci lub charakterystyce systemów), *clear box* (pełne informacje o budowie sieci), jak i *gray box* (częściowe informacje o budowie sieci).

2.1.3 Testy penetracyjne z zewnątrz sieci

Testy polegają na próbie zaatakowania wskazanych systemów lub usług z sieci publicznej, a więc z pozycji, jaką może przyjąć dowolny złośliwy użytkownik. Usługa jest realizowana najczęściej w modelu *black box* (ilość posiadanej informacji wstępnej jest minimalna – np. lista adresów IP lub URL usługi).

Prace wykonywane są najczęściej zdalnie z minimalną potrzebą ingerencji pracowników badanej organizacji.

2.1.4 Testy penetracyjne od wewnątrz sieci

Usługa w istotny sposób dopełnia testy penetracyjne z sieci publicznej, ponieważ ruch w sieci wewnętrznej traktuje się jako względnie zaufany, a zabezpieczenia sieci korporacyjnej odbiegają często jakością od systemów chroniących infrastrukturę przed penetracją z Internetu. Testy przeprowadzane są zwykle w modelu *black box* lub *gray box* i polegają na próbie zaatakowania sieci wewnętrznej przy założeniu posiadania dostępu do podłączonej doń maszyny. Ataki prowadzone są najczęściej z pozycji prawowitego, ale nieuprzywilejowanego użytkownika sieci (np. pracownik kadrowy, gość, menedżer), dysponującego oprogramowaniem i dokumentacją standardowo udostępnianą takiemu użytkownikowi. Prace realizowane są zwykle w siedzibie Zamawiającego, ale nie wymagają ścisłej współpracy z Jego pracownikami.

2.1.5 Ocena konfiguracji i skuteczności systemów bezpieczeństwa

Usługa, której celem jest ocena wdrożonych w przedsiębiorstwie (instytucji, organizacji) systemów bezpieczeństwa oraz wskazanie obszarów, w których dane rozwiązanie nie sprawdza się. Usługa ta obejmuje analizę działania systemów zapór ogniowych, systemów IDS/IPS, systemów antywirusowych, systemów filtrowania treści oraz innych, spełniających podobne funkcje w organizacji.

PCSS posiada doświadczenie w zakresie bezpiecznej konfiguracji firewalli, routerów, *load balancerów* oraz koncentratorów VPN, w tym również działających w trybie wysokiej dostępności (ang. *High Availability*). Posiadamy. opartą na własnym doświadczeniu, wiedzę w zakresie obsługi rozwiązań: CheckPoint VPN-1, Cisco ASA, Juniper SSG, Linux, OpenBSD, Brocade ServerIron i innych.

Istnieje również możliwość umieszczenia wskazanego systemu bezpieczeństwa w sieci własnej PCSS, sieci miejskiej POZMAN lub sieci krajowej PIONIER w celu jego dogłębnego przetestowania w samodzielnie wytworzonych szczególnych warunkach.

2.1.6 Przegląd konfiguracji systemów oraz usług

W ramach usługi analizowana jest konfiguracja podzbioru usług lub systemów w infrastrukturze Zamawiającego. Listę analizowanych systemów może wskazać Zamawiający (np. systemy przechowujące krytyczne dla Zamawiającego dane), może ona również powstać w wyniku przedstawienia sugestii przez Dział Bezpieczeństwa. Zastane na systemach ustawienia porównywane są z aktualnymi zaleceniami wydanymi przez producentów konkretnego rozwiązania, specjalistów bezpieczeństwa, niezależnych ekspertów, a także na podstawie własnego doświadczenia audytorów. Należy przy tym wskazać, że w ocenie uwzględniane są szczególne uwarunkowania panujące w badanej infrastrukturze – np. wymuszające ustawienia niezgodne z zaleceniami bezpieczeństwa.

Audytor nie musi mieć bezpośredniego dostępu do systemów – istnieje możliwość zbadania zgranych przez Administratora systemu w obecności audytora danych do dalszej analizy lub wykonywanie przez Administratora w systemie poleceń wskazanych przez audytora (aczkolwiek druga opcja w znaczący sposób spowalnia proces analizy).

2.1.7 Testy sieci pod względem wydajności i odporności na ataki DoS/DDoS

Usługa polega na przeprowadzeniu symulacji ataków DoS oraz DDoS i testach wydajnościowych infrastruktury sieciowej Zamawiającego.

2.1.7.1 Symulowane ataki DoS/DDoS

Możliwe jest przeprowadzenie wymienionych poniżej ataków:

- ataki na pasmo sieciowe – ataki polegające na zalewaniu infrastruktury sieciowej dużymi wolumenami ruchu sieciowego, z wykorzystaniem technik amplifikacji, takich jak: SMURF czy DNS amplification. Przykłady: SYNFlood, UDP/ICMP Flood, HTTP GET Flood
- ataki na urządzenia sieciowe – polegające na wyczerpaniu zasobów urządzeń przekazujących bądź filtrujących ruch, takich jak bramy sieciowe czy firewalle. Proponowane ataki to np. atak na liczbę obsługiwanych sesji, atak przy pomocy małych pakietów, ataki przy pomocy fragmentów, ataki wykorzystujące pakiety IP zawierające nieprawidłowe informacje w nagłówkach.
- ataki na aplikacje – testy podatności na ataki typu DoS oraz DDoS na aplikacje takie jak serwery www/https oraz bramy SIP. Są to między innymi: HTTP GET Flood, Slowloris - atak wolnych klientów, SIP DoS/DDoS.

2.1.7.2 Przeprowadzanie testów wydajności urządzeń

Usługa umożliwia przeprowadzenie we własnym laboratorium sieciowym testów (także testów porównawczych) dostarczonych przez Zamawiającego urządzeń, mogących służyć do łagodzenia skutków ataków DDoS – np. firewalli, routerów, load balancerów i koncentratorów VPN. Jako wynik dostępny będzie szczegółowy raport, zawierający realnie określone parametry urządzenia lub urządzeń. Testy pomogą w oszacowaniu możliwości zakupionego przez Zamawiającego urządzenia, lub też mogą stanowić pomoc w dalszych decyzjach inwestycyjnych.

2.1.7.3 Wsparcie w czasie trwania ataku

Treścią usługi jest udział konsultantów w przypadku wystąpienia ataku DDoS wymierzonego w infrastrukturę Zamawiającego. Elementem usługi jest stała gotowość do reakcji w określonym czasie od powiadomienia o ataku. W razie wystąpienia ataku konsultant przybędzie do siedziby Zamawiającego (lub, jeżeli będzie zapewniona taka możliwość, przeprowadzać będzie zdalną analizę bieżącej sytuacji w sieci) i prowadzić będzie bieżące doradztwo, pozwalające maksymalnie złagodzić

skutki trwającego ataku. Na życzenie Zamawiającego, pracownik nie musi wykonywać w systemie żadnych aktywnych działań, a jedynie prowadzić analizę sytuacji (np. odczyty parametrów ruchu z urządzeń sieciowych) i sugerować administratorowi do wykonania konkretne działania.

2.1.8 Testy kodu źródłowego

Usługa ta koncentruje się na analizie kodu źródłowego przekazanego przez Zamawiającego celem wykrycia i wyeliminowania błędów bezpieczeństwa. Usługa ta może być realizowana w dwóch wariantach:

- analiza kodu, identyfikacja błędów oraz możliwości ich wykorzystania przez atakującego jedynie w kontekście konfiguracji środowiska produkcyjnego,
- analiza kodu, identyfikacja wszystkich możliwych do wykorzystania błędów w dowolnym kontekście konfiguracyjnym.

Testy wykonywane są na podstawie przekazanego kodu i dokumentacji, ewentualnie z dostępem do środowiska testowego – przy minimalnej ingerencji pracowników Zamawiającego. Analiza odbywać się może na zasadzie wykorzystania istniejących oraz samodzielnie utworzonych narzędzi automatycznych oraz – którą to technikę poleca się jako czasochłonną, ale najbardziej efektywną – manualnego przeglądu (czytania) kodu źródłowego.

2.1.9 Testy kodu binarnego

Usługa ta skupia się na wyszukiwaniu błędów w plikach binarnych aplikacji. Realizowana jest wtedy, kiedy z różnych względów Zamawiający nie chce lub nie jest w stanie przekazać kodu źródłowego analizowanej aplikacji. Prace mogą odbywać się *offline* (na podstawie przekazanego pliku) lub – jeżeli wymaga tego sytuacja – w lokalizacji Zamawiającego, z ewentualną częściową współpracą Jego pracowników.

Innym wariantem usługi jest analiza dostarczonego pliku binarnego pod kątem ewentualnych złośliwych działań, jakie ten mógłby wykonać po uruchomieniu.

2.2 Usługi doradcze i wdrożeniowe

2.2.1 Projektowanie bezpiecznych sieci

Usługa mająca na celu stworzenie – w oparciu o przekazane założenia i ograniczenia – projektu sieci dla organizacji. Projekt jest tworzony zarówno pod kątem spełnienia koniecznych wymagań bezpieczeństwa, jak również pod kątem niezawodności oraz efektywności.

2.2.2 Nadzór nad tworzeniem sieci i wdrażaniem systemów bezpieczeństwa

Celem usługi jest sprawowanie nadzoru pod kątem poprawności implementacji mechanizmów bezpieczeństwa podczas tworzenia sieci w organizacji lub podczas wdrażania systemów odpowiedzialnych za utrzymanie bezpieczeństwa.

2.2.3 Audyt strony trzeciej

Usługa ta ma na celu ocenę skuteczności i poprawności rozwiązań lub procedur funkcjonujących w określonym przedsiębiorstwie (organizacji, instytucji), a wdrożonych przez firmę trzecią, lub też kontrolę stanu bezpieczeństwa w firmie świadczącej usługi Zamawiającemu.

2.2.4 Wdrażanie systemów bezpieczeństwa

Usługa skupia się na wdrażaniu w przedsiębiorstwie (organizacji, instytucji) rozwiązań z dziedziny bezpieczeństwa. Zakres wdrożeń obejmuje systemy zapór ogniowych, systemy IDS/IPS, systemy filtrowania treści oraz inne mechanizmy zabezpieczające, a także uszczelnianie systemów operacyjnych.

2.2.5 Przegląd oraz tworzenie polityk i procedur bezpieczeństwa

Usługa ta obejmuje działania zmierzające do oceny lub stworzenia dla organizacji odpowiedniej polityki bezpieczeństwa oraz procedur zarządzania pomocnych w realizowaniu i utrzymywaniu założonego poziomu bezpieczeństwa informacji. Analiza może odbywać się

2.3 Usługi świadczone w modelu ciągłym

Usługi świadczone w modelu ciągłym przewidziane są dla Partnerów, którzy planują nawiązać ścisłą i długookresową współpracę. Sposób ich świadczenia znacząco zmniejsza narzut przeznaczony na etap uzgodnień formalnoprawnych, zapewniając jednocześnie atrakcyjne warunki realizacji usług na zasadach uwzględniających albo łączących abonament i pracę akordową.

2.3.1 Stałe konsultacje bezpieczeństwa

Usługa polega na utrzymywaniu stałej gotowości do współpracy konsultantów z zakresu bezpieczeństwa IT i jest przewidziana szczególnie dla organizacji, które przechodzą poważną restrukturyzację swojej sieci (łączenie firm, dodawanie nowego wydziału, zmiana siedziby itd.). W ramach prac konsultanci bezpieczeństwa mogą przygotowywać raporty na pożądany temat, przeprowadzać analizy porównawcze, oceny projektów, uczestniczyć w spotkaniach konsultacyjnych czy też wykonywać dowolne inne usługi wymienione w niniejszym dokumencie.

2.3.2 Ciągły monitoring bezpieczeństwa infrastruktury

Celem usługi jest bieżące zapewnienie ochrony przed najnowszymi zagrożeniami charakterystycznymi dla infrastruktury organizacji. Wykonawca, mając do dyspozycji listę rozwiązań, systemów i usług, które należy objąć stałą ochroną, analizuje dostępne źródła informacji przygotowanych przez dostawców oprogramowania, niezależnych ekspertów oraz dostępne w tzw. drugim obiegu. Po wykryciu zagrożenia Zamawiający jest niezwłocznie informowany o jego charakterystyce i proponowanych krótko- oraz długoterminowych krokach naprawczych.

2.3.3 Okresowe analizy bezpieczeństwa

Bezpieczeństwo IT zapewnić można dla określonych warunków otoczenia – ich zmiana może poważnie wpłynąć na obniżenie osiągniętego uprzednio poziomu zabezpieczeń. Zmiany mogą mieć przy tym dwojaki charakter – wynikać z modyfikacji poczynionych w systemie (nowa funkcjonalność aplikacji, dodatkowe konto użytkownika) oraz z ciągle uaktualnianego stanu wiedzy na temat zagrożeń. Usługa – przewidziana zwłaszcza do ochrony systemów średnio i wysoce krytycznych – przewiduje cykliczne analizy bezpieczeństwa, prowadzone np. co 6 lub 12 miesięcy. Przedmiotem analizy może być cała sieć, a także pojedynczy system albo usługa. Najczęściej pierwszy z audytów cyklicznych charakteryzuje się większą czasochłonnością (i jest tożsamy z odpowiednim opisem usługi wymienionym wcześniej), a pozostałe koncentrują się głównie na badaniach związanych ze zmianami zaszłymi w systemie lub stanie wiedzy na temat zabezpieczeń. Cennym efektem ubocznym mogą być tu badania porównawcze poziomu bezpieczeństwa na przestrzeni kolejnych audytów, które pozwalają np. ocenić jakość środków technicznych i organizacyjnych stosowanych przez Zamawiającego w celu ochrony systemów.

2.4 Usługi uzupełniające

2.4.1 Analiza powłamaniowa

Celem usługi jest przeprowadzenie szczegółowej analizy systemu, który już stał się celem ataku. Efektem analizy jest wskazanie sposobu ataku oraz jego źródeł (na podstawie dostępnych informacji, jeżeli będą mogły być uznane za wiarygodne), zabezpieczenie śladów na potrzeby późniejszego postępowania oraz usunięcie wykrytej luki. Możliwe jest również wsparcie konsultacyjne w zakresie zgłoszenia zdarzenia odpowiednim organom.

2.4.2 Realizacja szkoleń

Usługa obejmuje kilka zasadniczych typów szkoleń, dedykowanych dla różnych grup użytkowników. Istnieje jednak możliwość przygotowania szkolenia niewymienionego na poniższej liście.

2.4.2.1 Szkolenia dla Kadry Kierowniczej

Krótkie szkolenia przeznaczone dla Kadry Kierowniczej, unaoczniające aktualne zagrożenia bezpieczeństwa IT w kontekście biznesowym działania organizacji oraz uzasadniające potrzebę przypisania dużej wagi temu tematowi. Elementem szkolenia jest również porównanie specyfiki wewnętrznej i zewnętrznej oceny bezpieczeństwa.

2.4.2.2 Szkolenia dla Administratorów

Szkolenia koncentrują się na zabezpieczaniu oraz utwardzaniu (ang. *hardening*) poszczególnych systemów i usług będących składnikami infrastruktury Zamawiającego. Przekazywane są informacje na temat zabezpieczeń sieci na poszczególnych warstwach modelu OSI, poczynając od fizycznej, a kończąc na aplikacyjnej. Prezentowany materiał obejmuje również np. utwardzanie systemów operacyjnych z rodzin MS Windows, Unix/Linux, OpenBSD, serwerów Web (m.in. IIS oraz Apache), bazodanowych (np. Oracle, MS SQL, MySQL), aplikacji Web (PHP, ASP, ASP.NET, JSP, Python), serwerów poczty elektronicznej (np. MS Exchange, Postfix), środowisk wirtualizacji (VMWare), rozwiązań podwyższających bezpieczeństwo (np. VPN, IPSec, stunnel), zastosowanie technik kryptograficznych w ochronie systemów oraz wiele innych tematów.

2.4.2.3 Szkolenia dla Projektantów i Programistów

Szkolenie zorientowane jest przede wszystkim na bezpieczeństwo wytwarzanego oprogramowania, dlatego przewidziane jest przede wszystkim dla organizacji tworzących aplikacje na potrzeby własne lub na sprzedaż. W zakres realizowanego materiału wchodzą informacje dla projektantów (dotyczące znaczenia bezpieczeństwa w cyklu życia oprogramowania, metod zapewnienia takiego bezpieczeństwa, modelowania zagrożeń i doboru rozwiązań dodatkowych, np. kryptografii) oraz – w znacznie szerszym zakresie – dla programistów.

Deweloperzy aplikacji dowiedzą się m.in. o wysokopoziomowym bezpieczeństwie aplikacji (rozumianym jako odpowiedni dobór funkcjonalności oprogramowania), jak również o wybranych kwestiach szczegółowych mających wpływ na bezpieczeństwo – np. błędy mechanizmów uwierzytelniania i autoryzacji, ochrona wrażliwych danych w pamięci, kwestie bezpiecznej wymiany plików), a także wzorcach bezpiecznego programowania w językach C/C++, Java, Perl, Python, PHP, ASP/ASP.NET i technikach unikania najpowszechniejszych błędów w kodzie źródłowym (np. przepełnienia bufora, XSS czy SQL Injection). Istotnym elementem szkolenia jest wstęp do statycznej analizy kodu źródłowego, wykształcający umiejętność użycia darmowych skanerów kodu źródłowego i interpretacji zwróconych przez nie wyników, a także pozwalający na podjęcie próby opracowania własnej, optymalnej metodyki czytania kodu źródłowego.

2.4.2.4 Szkolenia dla Użytkowników nietechnicznych

Szkolnie przewidziane dla każdego użytkownika stacji roboczej, w szczególności tzw. użytkownika niezorientowanego technicznie. Ma na celu podwyższenie poziomu świadomości na temat zagrożeń

związanych z korzystaniem z Internetu w miejscu pracy. Dzięki temu wykształcone zostaną podstawowe umiejętności, pozwalające na uniknięcie powszechnych zagrożeń bezpieczeństwa. Drastycznie zmniejszy to prawdopodobieństwo nieświadomej utraty wrażliwych informacji przez organizację. Istotnym elementem szkolenia jest wykład na temat zagrożeń socjotechnicznych.

Istnieje możliwość, we współpracy z administratorami usług i oficerami bezpieczeństwa Zamawiającego, sprofilowania szkolenia pod procedury oraz warunki obowiązujące w konkretnej organizacji.

Wszystkie typy szkoleń mogą odbywać się zarówno w siedzibie Zamawiającego, jak i w siedzibie PCSS. Dysponujemy salami różnej wielkości, wyposażonymi w projektory, rzutniki multimedialne, a także wielkoformatowe ekrany TV. Istnieje również możliwość skonfigurowania własnym sumptem 10 stanowisk warsztatowych lub zorganizowania warsztatów *Bring Your Own Laptop*. Możliwe jest również przeprowadzenie szkolenia przez system wideokonferencji, a także nagranie materiału video do późniejszego wykorzystania. Szkolenia mogą być prowadzone w językach: polskim oraz angielskim. Program szkoleń dostosowany jest w każdym przypadku do potrzeb Zamawiającego – możliwa jest zarówno realizacja krótkiego szkolenia ogólnego, jak i kilkudniowych kompleksowych warsztatów. Istnieje także możliwość realizacji dedykowanego szkolenia, nieobejmującego tematyki wskazanej powyżej (np. warsztaty dla specjalistów ds. bezpieczeństwa, obsługi incydentów sieciowych, Administratorów Danych Osobowych, Administratorów Bezpieczeństwa Informacji, szkolenia w zakresie wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji itd.).

2.4.3 Gry symulacyjne

Usługa skupia się na prowadzeniu gry symulującej realne zagrożenie dla bezpieczeństwa informacji organizacji Zamawiającego. Grupą docelową gry są administratorzy sieci oraz kadra zarządzająca bezpieczeństwem. Szczegółowe warunki i scenariusz gry symulacyjnej są ustalane każdorazowo z Zamawiającym (scenariusze mogą różnić się bardzo znacząco).

2.4.4 Ataki socjotechniczne

Faktyczne ataki wymierzone w użytkownika, uznawanego za najsłabsze ogniwo w łańcuchu zabezpieczeń, zwykle rozpoczynają zaawansowany, kompleksowy atak ukierunkowany na uzyskanie stałej tylnej furtki dostępu do infrastruktury organizacji (APT – ang. *Advanced Persistent Threat*). W ramach usługi audytorzy sprawdzą, jak zachowają się pracownicy testowanej Organizacji w niespodziewanych, stworzonych przez audytorów, okolicznościach.

Ataki obejmować mogą zarówno scenariusze uwzględniające środki komunikacji zdalnej (np. dedykowany phishing, rozmowy telefoniczne), jak i takie, w których audytorzy osobiście pojawiają się w lokalizacji Zamawiającego. Ataki są ukierunkowane na uzyskanie nieautoryzowanego dostępu do

danych, systemów albo fizycznych lokalizacji, a ich efektem jest stwierdzenie miejsc i warunków, w których nie są spełniane założenia procedur bezpieczeństwa obowiązujących w Organizacji.

Rozpoczęcie ataków jest poprzedzone procesem uzyskania odpowiednio sformułowanych zezwoleń na ich przeprowadzenie od Kierownictwa Organizacji.

* * *

Przedstawiony powyżej opis usług jest jedynie formą skróconą oraz ogólną. W celu uzyskania szczegółowych informacji, umożliwiających dostosowanie propozycji zakresu usługi do specyfiki organizacji Zamawiającego, prosimy o kontakt na adres podany na stronie 1.

3 Usługi bezpieczeństwa w ramach Konsorcjów

Poznańskie Centrum Superkomputerowo-Sieciowe współpracuje w ramach **Wielkopolskiego Klastra Teleinformatycznego** (http://wkt.pl) z lokalnymi firmami działającymi w sektorze IT, co pozwala świadczyć **dodatkowe usługi powiązane z bezpieczeństwem**. W przypadku zainteresowania kwestiami takimi jak **analiza procesów biznesowych**, **analiza zgodności ze wskazaną normą**, **audyty sieciowe** (poza sektorem bezpieczeństwa) zapraszamy do kontaktu z przedstawicielem PCSS.