Załącznik nr 1 do OPZ „ Zakres audytu wewnętrznego”

Audytowane obszary IT

Audyt bezpieczeństwa wewnętrznego odbywać się będzie w 5 głównych obszarach

1) Audyt konfiguracji systemów operacyjnych na wybranych stacjach oraz domeny Windows odbywać się będzie w oparciu o metodę whitebox, czyli audytor zna konfigurację i uwarunkowania zamawiającego w danym obszarze. Celem przeprowadzonych prac jest wykazanie skuteczności stosowanego herdeningu (utwardzenia) systemu operacyjnego. W ramach zadania nastąpi :
   a) Sprawdzenie udostępnionych usług sieciowych.
   b) Sprawdzenie działających w systemie procesów.
   c) Sprawdzenie podziału przestrzeni dyskowej na odpowiednie strefy.
   d) Sprawdzenie wdrożenia metod ochrony
   e) Sprawdzenie uprawnień do najistotniejszych zasobów.
   f) Sprawdzenie wdrożonego mechanizmu instalacji aktualizacji.
   g) Sprawdzenie wdrożonego mechanizmu kopii zapasowych.
   h) Sprawdzenie wdrożonego systemu logowania zdarzeń.
   i) Sprawdzenie zabezpieczenia systemu w fazie boot.
   j) Sprawdzenie wykorzystywanego sposobu zarządzania systemem.
   k) Sprawdzenia systemów: Windows Server, Linux.
   l) Inwentaryzacja otwartych portów oraz ich wpływ na potencjalne zagrożenia.

2) Audyt bazy danych SQL prowadzony będzie metodą whitebox i obejmować będzie analizę aktualnej konfiguracji. W ramach prowadzonych prac zostanie wykonane :
   a) Sprawdzenie wdrożenia podstawowych zasad utwardzenia (hardening) bazy (np.: dostępność domyślnych użytkowników tzw. guest, partycjonowanie bazy, składowanie logów, logowanie nietypowych zdarzeń, dostępność wybranych niebezpiecznych procedur i funkcji składowanych).
   b) Sprawdzenie komunikacji z klientem bazodanowym - wykorzystanie mechanizmów kryptograficznych (logowanie się klienta oraz transfer danych).

c) Recenzja architektury bazy (wykorzystane mechanizmy autoryzacji oraz uwierzytelniania; segmentacja uprawnień, wykorzystanie widoków; wykorzystanie procedur składowanych).
d) Weryfikacja sposobu wykonywania kopii zapasowych.
e) Analiza sposobu udostępnienia RDBMS na poziomie sieciowym.
f) Analiz baz: SQL Server, Oracle, MySQL, PostgreSQL

3) Audyt sieci LAN ma na celu przeprowadzenie badań i weryfikację obecnie stosowanych zabezpieczeń sieci lokalnej wraz z wykazaniem słabych punktów i sposobem uszczelnienia. W zakresie badania sieci lokalnej wykonane zostaną następujące czynności :
   a) Analiza topologii sieci
   b) Weryfikacja podziału LAN na strefy sieciowe (w tym wykorzystanie firewalli oraz VLAN/PVLAN)
   c) Wykazanie podatności w wybranych podsieciach
   d) Weryfikacja dostępnych mechanizmów uwierzytelniania dostępnych sieci
   e) Weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI
   f) Weryfikacja dostępu do Internetu z LAN
   g) Weryfikacja zasad utrzymania sieci

4) Audyt styku sieci lokalnej z Internetem powadzony będzie metodą blackbox (Wykonawca nie zna architektury i zabezpieczeń Zamawiającego). W zakres audytu wchodzić będą :
   a) Weryfikacja zasad utrzymania sieci
   b) Próba wybranych ataków typu DoS
   c) Analiza topologii brzegu sieci
   d) Testy szczelności systemów firewall

5) Audyt urządzeń sieciowych prowadzony będzie metodą blackbox. Test obejmować musi skanowanie dowolnych urządzeń sieciowych jak switch, serwer, firewall z poziomu sieci Internet. W skład prowadzonych działań wchodzić będzie :
   a) Skanowanie aktywnych hostów w wybranej podsieci
   b) Skanowanie portów TCP/UDP
   c) Próba ominięcia firewall z wykorzystaniem min. fragmentacji IP
   d) Określenie ścieżki sieciowej do urządzeń
   e) Próba detekcji typu oraz wersji usług sieciowych
   f) Próba detekcji typu i wersji oprogramowania
   g) Określenie i zlokalizowanie znanych podatności w oprogramowaniu

h) Próba komunikacji w obrębie protokołu ICMP wraz z generowaniem pakietów o dużym rozmiarze.

Harmonogram realizacji audytu

Obszar	Zadania	Termin realizacji obszaru (OD - DO)
Audyt konfiguracji systemów operacyjnych	Sprawdzenie udostępnionych usług sieciowych.	
	Sprawdzenie działających w systemie procesów.	
	Sprawdzenie podziału przestrzeni dyskowej na odpowiednie strefy.	
	Sprawdzenie wdrożenia metod ochrony	
	Sprawdzenie uprawnień do najistotniejszych zasobów.	
	Sprawdzenie wdrożonego mechanizmu instalacji aktualizacji.	
	Sprawdzenie wdrożonego mechanizmu kopii zapasowych.	
	Sprawdzenie wdrożonego systemu logowania zdarzeń.	
	Sprawdzenie zabezpieczenia systemu w fazie boot.	
	Sprawdzenie wykorzystywanego sposobu zarządzania systemem.	
	Sprawdzenia systemów: Windows Server, Linux.	
	Inwentaryzacja otwartych portów oraz ich wpływ na potencjalne zagrożenia.	
Audyt bazy danych SQL	Sprawdzenie wdrożenia podstawowych zasad utwardzenia (hardening) bazy (np.: dostępność domyślnych użytkowników tzw. guest, partycjonowanie bazy, składowanie logów, logowanie nietypowych zdarzeń, dostępność wybranych niebezpiecznych procedur i funkcji składowanych).	
	Sprawdzenie komunikacji z klientem bazodanowym - wykorzystanie mechanizmów kryptograficznych (logowanie się klienta oraz transfer danych).	
	Recenzja architektury bazy (wykorzystane mechanizmy autoryzacji oraz uwierzytelniania; segmentacja uprawnień, wykorzystanie widoków; wykorzystanie procedur składowanych).	
	Weryfikacja sposobu wykonywania kopii zapasowych.	
	Analiza sposobu udostępnienia RDBMS na poziomie sieciowym.	
	Analiz baz: SQL Server, Oracle, MySQL, PostgreSQL	
Audyt sieci LAN	Analiza topologii sieci	
	Weryfikacja podziału LAN na strefy sieciowe (w tym wykorzystanie firewalli oraz VLAN/PVLAN)	
	Wykazanie podatności w wybranych podsieciach	
	Weryfikacja dostępnych mechanizmów uwierzytelniania dostępnych sieci	
	Weryfikacja mechanizmów ochronnych w warstwie 2 i 3 modelu OSI	
	Weryfikacja dostępu do Internetu z LAN	
	Weryfikacja zasad utrzymania sieci	
Audyt styku sieci lokalnej z Internetem	Weryfikacja zasad utrzymania sieci	
	Próba wybranych ataków typu DoS	
	Analiza topologii brzegu sieci	
	Testy szczelności systemów firewall	
Audyt urządzeń sieciowych	Skanowanie aktywnych hostów w wybranej podsieci	
	Skanowanie portów TCP/UDP	
	Próba ominięcia firewall z wykorzystaniem min. fragmentacji IP	
	Określenie ścieżki sieciowej do urządzeń	
	Próba detekcji typu oraz wersji usług sieciowych	
	Próba detekcji typu i wersji oprogramowania	
	Określenie i zlokalizowanie znanych podatności w oprogramowaniu	
	Próba komunikacji w obrębie protokołu ICMP wraz z generowaniem pakietów o dużym rozmiarze.	

Dodatkowe wytyczne

W ramach pracy Wykonawca opracuje wnioski audytowe oraz rekomendacje dalszych działań i koniecznych zmian odnoszących się do zapewnienia zgodności działania zbudowanych aplikacji z wymaganiami normy PN-ISO/IEC 27001:2014 i najlepszymi praktykami w dziedzinie zarządzania np. ITIL. Wnioski te będą stanowiły część końcowego raportu z audytu.

Skanowanie podatności na komputerach i serwerach powinno odbywać się bez instalacji jakiegokolwiek oprogramowania na urządzeniach badanych. Przeprowadzenie testów nie może zaburzyć bieżącej działalności pracy ZTM w Poznaniu (ataki destrukcyjne).

Wykonawca zobowiązany będzie do przedstawienia szczegółowego raportu z wykonanych prac. Raport zawierać musi informacje o przebiegu badania, znalezionych błędach oraz zalecenia po audytowe. Raporty końcowe zawierające podsumowanie wykonanych prac, dostarczane są Zamawiającemu po zakończeniu każdego audytu każdego obszaru. Raporty obejmować muszą przynajmniej informacje wymienione poniżej:

a) poziom krytyczności błędu według zaproponowanej przez Wykonawcą i uzgodnionej z Zamawiającym klasyfikacją,
b) prawdopodobieństwo znalezienia/wykorzystania podatności przez atakującego – tzw. Likehood, probability,
c) wpływ na system (lub inne systemy) – tzw. impact,
d) szczegółowy sposób wykrycia i charakterystyka ataku (z uwzględnieniem zasad powtarzalności dla każdego przypadku). Informacje powinny być na tyle szczegółowe, aby była możliwa reprodukcja danego błędu,
e) możliwości zabezpieczenia się przed podatnością i uwagi prowadzące do uniknięcia tego typu problemów w przyszłości,
f) załączniki dokumentujące wystąpienie błędu (np. zrzuty ekranu, przykładowe pakiety atakujące lub świadczące o podatności, pliki zawierające zapis ruchu sieciowego w formacie libpcap itp.).

Wykonawca jest zobligowany do opracowania następujących definicji:

a) kryterium wpływu na systemu (impact),
b) prawdopodobieństwo wykorzystania podatności przez atakującego (likelihood),
c) poziom krytyczności

oraz przedstawienia Zamawiającemu do akceptacji sposobu prezentacji wyników audytu. Zamawiający oczekuje, że dla wykrytych błędów o wpływie na system: średni lub krytyczny i równoczesnym prawdopodobieństwie: średni lub wysoki zostaną opracowane przez Wykonawcę szczegółowe rekomendacje zmian. Struktura raportu powinna odpowiadać merytorycznemu podziałowi prac na obszary i aplikacje.

Wykonawca, z dniem podpisania protokołu odbioru raportu, przenosi na Zamawiającego autorskie prawa majątkowe do raportu na polach eksploatacji, obejmujących:

a) odtwarzanie,
b) utrwalanie i trwałe zwielokrotnianie całości lub części utworu, wszystkimi znanymi w chwili zawierania Umowy technikami, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową,
c) przekazywanie,
d) przechowywanie,
e) wyświetlanie,
f) wprowadzanie do pamięci komputera wraz z prawem do dokonywania modyfikacji,
g) tłumaczenie,
h) przystosowywanie,
i) zmiany układu lub jakiekolwiek inne zmiany,