Podsumowanie dyskusji

Podczas prowadzonej dyskusji, której tematem przewodnim był „Doświadczenia i wyzwania po pierwszych audytach KSC - dyskusja o potrzebie zmian i usprawnień" omówione zostały następujące kwestie:

1. Testy techniczne, a audyt KSC - wymaganie, czy zbędny element?

    a. Uczestnicy dyskusji wskazali, iż analiza techniczna powinna być elementem składowym audytu KSC, gdyż bez niej trudno dokonać pełnej weryfikacji i oceny skuteczności istniejącego systemu bezpieczeństwa.
    b. Na obecnym etapie wdrożenia i audytu KSC uczestnicy bardziej koncentrowali się na weryfikacji zgodności organizacyjnej, w tym dokumentacji, jednak widzą potrzebę zmian i ujęcia aspektów technicznych w kolejnych latach.
    c. Sama ocena zabezpieczeń organizacyjnych, w tym dokumentacji systemu bezpieczeństwa – na zasadzie weryfikacji zgodności nie jest wystarczająca do wydania opinii oraz dostarczania wiarygodnej informacji o ryzykach, na jakie narażony jest operator usługi kluczowej.
    d. Nie opłaca się korzystać z „tanich" i niskowykwalifikowanych audytorów, gdyż jakość dostarczanej przez nich pracy może okazać się bezwartościowa.
    e. Zespół audytorski powinien posiadać odpowiednie kwalifikacje techniczne oraz doświadczenie do oceny architektury bezpieczeństwa oraz przeprowadzenia testów technicznych (testy konfiguracji, testy podatności, testy penetracyjne), wraz z poprawną interpretacją uzyskanych wyników (raportów) wygenerowanych przez narzędzia do prowadzenia skanów.
    f. Zakres testów powinien być dostosowany do możliwości i potrzeb organizacji, jako minimum wskazano ocenę architektury bezpieczeństwa oraz testy podatności. W dalszych krokach o ile istnieją możliwości finansowe, po konsultacji z firmą zewnętrzną warto rozszerzyć zakres testów o najbardziej ryzykowne obszary i tam dokonać weryfikacji konfiguracji oraz przeprowadzić testy penetracyjne (też w uzgodniony sposób: white box, grey box, black box).
    g. Wskazano, iż testy nie powinny dotyczyć jedynie niewielkiego i ograniczonego wycinka systemu, a uwzględniać sposób działania potencjalnego atakującego, który będzie starał się wykorzystywać słabe luki w systemie bezpieczeństwa i atakować najbardziej podatne elementy, aby uzyskać dostęp do swojego głównego celu ataku. Bardzo rzadko zdarza się, aby atakujący bezpośrednio atakował najbardziej zabezpieczone elementy organizacji.
    h. Testy penetracyjne powinny być realizowane w odniesieniu do przyjętych standardów i dobrych praktyk tj. OWASP TOP TEN lub OWASP ASVS.
    i. Testy na poziomie zupełnie podstawowym (testy podatności) mogą być realizowane wewnętrznie, w szczególności w jednostkach nie dysponujących wystarczającym budżetem. Można do tego wykorzystać darmowe narzędzia tj. NMAP, czy OpenVAS. Jednak testy przeprowadzone przez zewnętrznego eksperta i wysokich kwalifikacjach dostarczają dodatkową wartość i mogą wskazać znacznie większy zakres słabości badanych systemów.

2. Połączenie audytu online i audytu on-site - słabości i mocne strony.
    a. Wskazano, iż audyt online posiada wiele mocnych stron, do których należy zaliczyć:
        i. łatwość prowadzenia wywiadów 1 na 1, bez ograniczeń czasowych wynikających z ograniczonego czasu audytu na miejscu;
        ii. możliwość udostępnienia ekranu przez audytowanego i przejścia przez poszczególne komponenty systemu i jego konfiguracji;
        iii. możliwość zdalnego uzyskania dokumentacji;
        iv. znacznie lepsza efektywność pracy audytora;
    b. Do słabych stron audyty online należy zaliczyć:
        i. problemy z komunikacją w spotkaniach grupowych;
        ii. problemy z instalacją narzędzi lub konfiguracją urządzeń do prowadzenia testów technicznych;
        iii. problemy z oceną zabezpieczeń fizycznych i środowiskowych;
        iv. brak możliwości pozyskania części najwrażliwszej dokumentacji;

v. często brak możliwości uzyskania zdalnego oglądu kluczowych elementów infrastruktury.

3. Mocne strony i słabości szablonu audytu KSC w odniesieniu do różnych sektorów i organizacji.
    a. Wskazano, iż szablon audytu KSC dostarcza bardzo dobrego fundamentu do oceny systemu bezpieczeństwa zgodnie z KSC, ujednolica podejście do raportowania, wskazuje zakres weryfikacji, którą powinien podjąć audytor.
    b. Jako elementy do poprawy wskazano wysokie wymagania wobec mniejszych jednostek, które na obecnym poziomie dojrzałości nie są w stanie ich osiągnąć.
    c. Dodatkowo szablon mógłby zostać uzupełniony o poszczególne wymagania (zabezpieczenia) wskazane w Załączniku A do normy ISO 27001, które należałoby zweryfikować i uzupełnić.
    d. Szablon mógłby zostać uzupełniony o specjalistyczne wymagania tj. normy bezpieczeństwa dotyczące ICS, czy zastosowanie rozwiązań chmurowych.
4. Podejście do oceny różnych organizacji np. duża organizacja z sektora finansowego oraz niewielki szpital.
    a. W toku dyskusji wskazano, iż wiele obecnych standardów bezpieczeństwa nie nadąża za zmieniającymi się zagrożeniami i podejściem do bezpieczeństwa tj. Zero Trust Architecture, wykorzystanie IoT, bardzo szybka migracja do środowisk chmurowych.
    b. Podniesiono kwestię koncentracji na ryzykach danej organizacji, a nie jedynie podejściu zgodnościowym. Podejście zgodnościowe z KSC powinno być jednym z elementów oceny, jednak bardzo ważne jest wskazanie ryzyk bezpieczeństwa, które dotyczą danego podmiotu.
    c. Wskazano, iż nie można w podobny sposób traktować i oceniać organizacji np. z sektora bankowego, o długiej historii funkcjonowania w ramach reżimu finansowego i rekomendacji D, w której dojrzałość systemu bezpieczeństwa jest na dość wysokim poziomie oraz niewielkiej organizacji z sektora ochrony zdrowia, która dopiero wdraża rozwiązania bezpieczeństwa.
    d. Stwierdzono, iż małe i duże organizacje są na przeciwnych krańcach skali i mają zwykle inne problemy:
        i. małe organizacje mają problemy z niewielkim budżetem na bezpieczeństwo, posiadają niskowykwalifikowaną kadrę i zasoby niezbędne do zapewnienia bezpieczeństwa, natomiast często mają dość niewielką i nieskomplikowaną infrastrukturę,
        ii. duże organizacje mogą sobie pozwolić na znacznie większe wydatki, zatrudnić lub wyszkolić wysokiej klasy specjalistów oraz zapewnić narzędzia wspierające bezpieczeństwo, natomiast ich problemem jest wielkość i skomplikowanie posiadanej infrastruktury i całego ekosystemu związanego z bezpieczeństwem.
    e. Wskazano najczęstsze słabości bezpieczeństwa w mniejszych jednostkach i jednostkach z sektora finansów publicznych:
        i. brak segmentacji sieci;
        ii. wykorzystywanie niewspieranych systemów, bez wdrożenia dodatkowych mechanizmów kompensacyjnych;
        iii. brak informacji o znanych podatnościach;
        iv. brak testów podatności;
        v. niewdrożone procesy zarządzania podatnościami i patchami;
        vi. brak zautomatyzowanego systemu nadawania, zmiany i odbierania uprawnień;
        vii. podejście zgodnościowe, a nie oparte na ryzyku.