Michał Dziarkowski,
Aleksandra Rząca,
Szymon Szkarłat

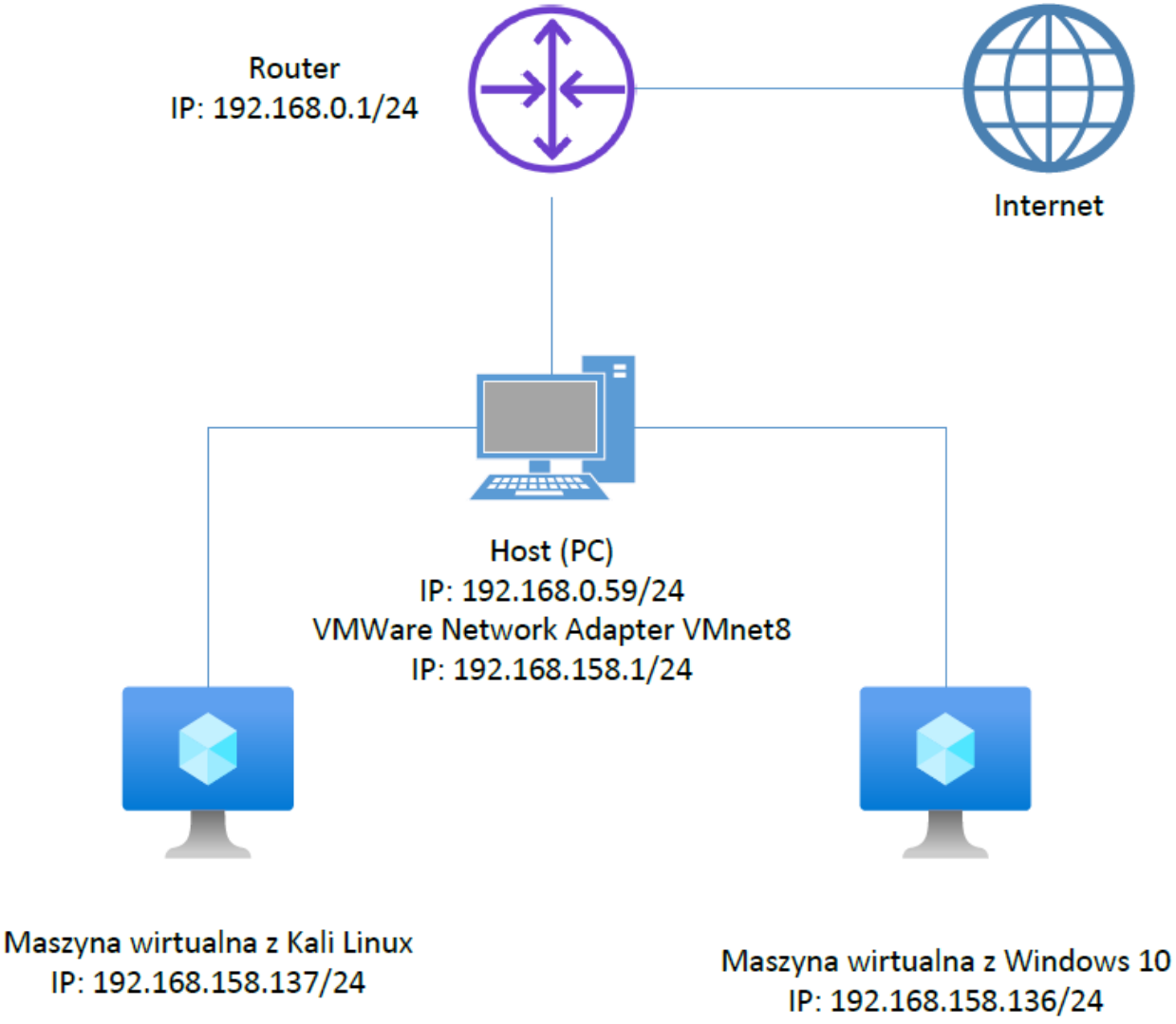
Testy Penetracyjne

Laboratorium 1

Spis treści

Rysunek techniczny środowiska wirtualizacyjnego 2
Program w Python 3
Kod źródłowy 3
Działanie programu 4
Opis scenariusza 5
Dokument planowania testu penetracyjnego 6
1. Cele testu penetracyjnego 6
2. Zakres testów 7
3. Harmonogram 8
4. Analiza ryzyka 10
5. Zasoby 11
Rules of Engagement 12
1. Obszar testowania 12
2. Metodologia testów 13
3. Podział czasu 13
4. Analiza i zarządzanie ryzykiem 14
5. Ograniczenia testów 15

Rysunek techniczny środowiska wirtualizacyjnego



Program w Python

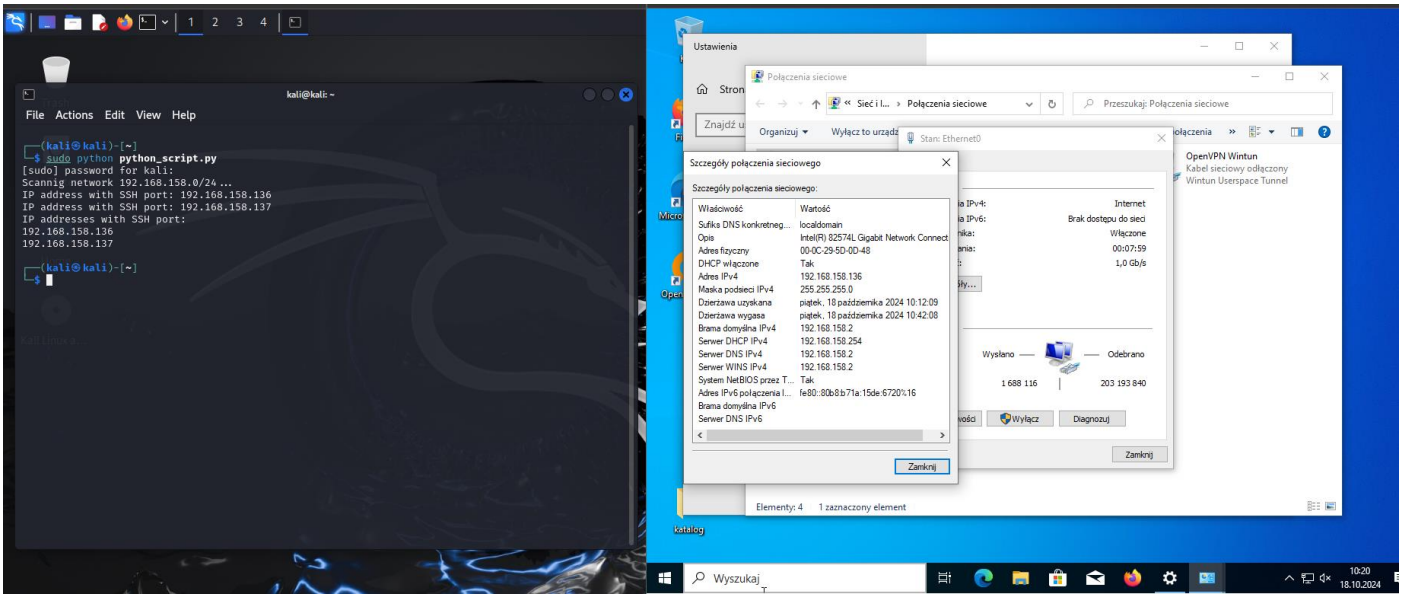
Kod źródłowy

Kod źródłowy programu umieszczamy poniżej w postaci zrzutu ekranu, ale również dołączamy go jak osobny plik w naszym raporcie do laboratorium 1.

```python
import socket


def is_port_open(ip, port):
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(1)

    try:
        sock.connect((ip, port))
        sock.close()
        return True

    except:
        return False


def find_ssh_open_hosts(subnet):
    open_hosts = []
    port = 22

    for i in range(1, 254):
        ip = f"{subnet}.{i}"
        if is_port_open(ip, port):
            print(f"IP address with SSH port: {ip}")
            open_hosts.append(ip)

    return open_hosts


if __name__ == "__main__":
    subnet = "192.168.158"
    print(f"Scannig network {subnet}.0/24 ... ")
    open_hosts = find_ssh_open_hosts(subnet)

    if open_hosts:
        print("IP addresses with SSH port:")
        for host in open_hosts:
            print(host)
    else:
        print("No IP address with SSH port found")

```

Działanie programu

Program jest uruchamiany na maszynie wirtualnej z systemem Kali Linux. Adres IP na maszynie z systemem Linux to 192.168.158.137/24, natomiast na maszynie z Windows 10 ustawiony jest adres IP: 192.168.158.136/24. Na Windows 10 jest otwarty port SSH (nr portu 22), co potwierdza, poniższy zrzut ekranu.



Opis scenariusza

Scenariusz 1

Opis:
SmartBank to duża instytucja finansowa oferująca szeroki wachlarz usług bankowości online oraz mobilnej dla klientów indywidualnych i korporacyjnych. SmartBank obsługuje transakcje płatnicze, kredyty, inwestycje oraz inne usługi finansowe dostępne za pośrednictwem aplikacji mobilnej, platformy webowej i oddziałów stacjonarnych. Kluczową rolę w działalności SmartBank odgrywają bezpieczne systemy IT, które przetwarzają ogromne ilości danych osobowych i finansowych.

Infrastruktura IT:

- **Aplikacja mobilna i webowa:** Platforma umożliwiająca klientom zarządzanie kontami, przeprowadzanie płatności, otwieranie kont oszczędnościowych oraz inwestycji.
- **Baza danych:** Serwery przechowujące dane klientów (dane osobowe, historie transakcji) oraz wrażliwe informacje finansowe.
- **Sieć wewnętrzna:** Sieć korporacyjna umożliwiająca pracownikom dostęp do systemów bankowych, CRM oraz systemu obsługi klienta.
- **Chmura prywatna:** Wirtualna infrastruktura obsługująca kluczowe aplikacje i usługi bankowe, hostowana na prywatnym środowisku chmurowym.

Główny cel:
Ocena, czy dane klientów są właściwie zabezpieczone, a systemy IT nie są narażone na ataki hakerskie. Identyfikacja potencjalnych luk w zabezpieczeniach przed atakami typu phishing oraz sprawdzenie, czy polityki dostępu w sieci wewnętrznej SmartBanku są odpowiednio skonfigurowane.

[pozostała część taka jak w instrukcji do Laboratorium]

Dokument planowania testu penetracyjnego

1. Cele testu penetracyjnego

- Ocena bezpieczeństwa aplikacji mobilnej i aplikacji webowej, pod względem kontroli dostępu, w tym błędów w mechanizmach uwierzytelniania i autoryzacji.
- Przeprowadzenie testów bezpieczeństwa infrastruktury sieciowej wewnętrznej, z uwzględnieniem bezpieczeństwa punktów dostępowych, segmentacji sieci i sieciowej zapory ogniowej.
- Analiza mechanizmów bezpieczeństwa infrastruktury wirtualnej z uwzględnieniem systemu IAM, możliwości audytowych i zgodności z lokalnymi prawami.
- Sporządzenie szczegółowego raportu z wynikami testu oraz rekomendacjami dotyczącymi zabezpieczeń.

2. Zakres testów

Testy penetracyjne obejmą trzy główne obszary działania:

Aplikacja mobilna i webowa:

- Przeprowadzenie szczegółowych testów na ataki aplikacyjne, to jest:
    - SQL Injection: Sprawdzenie, czy aplikacje w sposób właściwy przeprowadzają procedurę walidacji danych wejściowych, które podczas korzystania z aplikacji wprowadza użytkownik. Ponadto weryfikacja sposobu realizacji zapytań do bazy danych.
    - Cross-Site Request Forgery (CSRF): Sprawdzenie czy aplikacja webowa jest podatna na realizację fałszywych, nieautoryzowanych akcji (żądań).
    - Cross-Site Scripting (XSS): Sprawdzenie, czy aplikacja webowa pozwala na wstrzyknięcie, dołączenie skryptów bądź kawałków kodu, które mogą zostać wykonane w przeglądarkach użytkowników.
    - Broken Access Control: Testowanie, czy mechanizmy kontroli dostępu zostały zaimplementowane w sposób odpowiedni, tzn. osoby bez konkretnych uprawnień nie mają dostępu do danych wrażliwych czy danych osobowych klientów.
- Testy uwierzytelniania i zarządzania sesjami, aby upewnić się, że dane logowania klientów są odpowiednio chronione.
- Testy na ataki brute-force przeciwko mechanizmom uwierzytelniania, sprawdzenie czy aplikacje posiadają odpowiednie mechanizmy zabezpieczające przed tego typu atakiem.

Infrastruktura sieciowa:

- Skanowanie sieci wewnętrznej w celu zidentyfikowania możliwych potencjalnych punktów wejścia do sieci wewnętrznej i ruchu lateralnego (enumeracja aktywnych hostów, otwartych portów oraz usług).
- Testy odporności na ataki phishingowe oraz przetestowanie, czy użytkownicy systemów są odpowiednio przeszkoleniu lub czy posiadają wystarczającą wiedzę w zakresie rozpoznawania tego typu ataków, w tym celu:
    - Wysłanie odpowiednich maili phishingowych na konta pocztowe powiązane z kontami danego użytkownika.
    - Wysłanie wiadomości SMS na numer telefonu, który jest powiązany z kontem danego użytkownika.
    - Zbiorcze podsumowanie tego etapu testów penetracyjnych
- Audyt konfiguracji zapory ogniowej oraz innych urządzeń sieciowych, do których jest dostęp podczas testów, oraz atak siłowy na hasła do urządzeń sieciowych.

Chmura prywatna:

- Sprawdzenie, czy konfiguracja środowiska chmurowego jest zgodna z najlepszymi praktykami bezpieczeństwa, w tym celu:
    - Zweryfikowanie aktualności stosowanego oprogramowania.
    - Sprawdzenie, czy konfiguracja nie zawiera błędów mogących narazić działanie systemu na brak odporności na ataki, a w konsekwencji na wyciek danych.
- Audyt bezpieczeństwa dostępu do chmury prywatnej (poprzez mechanizmy np. MFA czy IAM) oraz zarządzania danymi w chmurze, w szczególności z myślą o zgodności z RODO.

3. Harmonogram

Faza 1 – Planowanie (Dzień 1):

- Spotkanie z zespołem IT SmartBanku w celu potwierdzenia zakresu testów penetracyjnych oraz podpisania dokumentów SoW (Statement of Work) oraz klauzuli RODO.
- Ustalenie dozwolonych narzędzi, zakresu wiedzy zespołu przeprowadzającego tety nt. aplikacji, sieci i chmury, oraz harmonogramu przeprowadzanych testów, w tym terminów raportowania wyników cząstkowych.

Faza 2 – Zbieranie danych (Dzień 2-3):

- Przeprowadzenie pasywnego rekonesansu, w tym: rozpoznania aplikacji webowej oraz aplikacji mobilnej, a także zleconego obszaru infrastruktury sieciowej.
- Użycie specjalnych skanerów, umożliwiających wykrycie znanych luk bezpieczeństwa w aplikacjach webowej oraz mobilnej (w tym celu użycie narzędzi m.in.: Checkmarx ZAP oraz BurpSuite).
- Użycie odpowiednich narzędzi do skanowania, celem wstępnego wykrycia otwartych portów, usług czy hostów, w tym celu wykorzystanie Nmap oraz programu Wireshark.

Faza 3 – Skanowanie podatności i testowanie (Dzień 4-7)

- Wykonywanie testów aplikacji webowej pod kątem przedstawionych w celach podatności (SQL Injection, CSRF, XSS, Broken Access Control).
- Przeprowadzenie ataku siłowego na usługi na otwartych portach, sprawdzenie konfiguracji urządzeń sieciowych, w tym zapór ogniowych.
- Audyt konfiguracji kontroli dostępu chmury prywatnej, zakresu logowania wykonywanych akcji, oraz sposobu przechowywania tych logów. Ocena sposobu zarządzania danymi w chmurze pod względem poufności.

Faza 4 – Testy odporności na ataki phishingowe (Dzień 8-10)

- Rozesłanie maili oraz wiadomości SMS do niektórych użytkowników, celem sprawdzenia ich reakcji na otrzymane wiadomości oraz akcji, jakie będą w związku z otrzymany wiadomościami podejmować.
- Przeanalizowanie danych zebranych podczas tego etapu. Akcja ta pozwoli sprawdzić, czy użytkownicy systemów posiadają odpowiednią świadomość oraz mają niezbędną wiedzę z zakresu odporności na ataki phishingowe.

Faza 5 – Eksploatacja i raportowanie (Dzień 11-13)

- Próba wykorzystania wykrytych podatności w kontrolowany, niezakłócający normalnego funkcjonowania usług dla klientów, sposób.
- Dokumentowanie na bieżąco wyników, a także zbieranie odpowiednich danych do raportu końcowego.

Faza 6 – Przygotowanie raportu i omówienie wyników (Dzień 14-15)

- Przygotowanie szczegółowego i wyczerpującego raportu z przeprowadzonych testów penetracyjnych z rekomendacjami naprawczymi, które zaleca się, aby wdrożyć do przetestowanych systemów.
- Spotkanie z zarządem banku, dyrektorem IT oraz zespołem bezpieczeństwa SmartBanku, aby omówić wyniki testów i przekazać zalecane poprawki dotyczące bezpieczeństwa aplikacji webowej, mobilnej oraz całego systemu, który został poddany testom.

4. Analiza ryzyka

Testy penetracyjne niosą ze sobą pewne ryzyko, które musi być odpowiednio zarządzane:

1) Ryzyko naruszenia normalnego funkcjonowania działania systemu:
   - Testy przeprowadzane w nieodpowiednich godzinach mogą doprowadzić do tymczasowego naruszenia normalnego funkcjonowania aplikacji webowej czy mobilnej.
   - Mitygacja: Testy mogące naruszyć wydolność systemów zostaną przeprowadzone w godzinach najmniejszego ich obciążenia, a wrażliwe i krytyczne operacje będą realizowane wyłącznie w konsultacji i za zgodą zespołu bezpieczeństwa SmartBanku.

2) Ryzyko naruszenia poufności danych klientów:
   - Istnieje ryzyko, że dane klientów mogą zostać niecelowo ujawnione, podczas przeprowadzania testów penetracyjnych aplikacji webowej czy mobilnej.
   - Mitygacja: Testy będą przeprowadzane w izolowanym środowisku stagingowym, wszelkie dane klientów będą zanonimizowane, a osoby odpowiedzialne za przeprowadzenie testu nie będą miały dostępu do danych klientów.

3) Ryzyko utraty danych produkcyjnych:
   - Istnieje ryzyko bezpowrotnej utarty krytycznych, wrażliwych danych produkcyjnych. Dane te mogą okazać się bardzo istotne i ważne z perspektywy zachowania ciągłości i normalnego funkcjonowania całości systemu czy usług dla klientów.
   - Mitygacja: Testy nie będą prowadzone na środowisku produkcyjnym. Natomiast będą się odbywać na specjalnie do tego przygotowanym środowisku stagingowym z odpowiednią kopią zapasową wszelkich dostępnych danych produkcyjnych.

4) Ryzyko nieprawidłowych czy niepełnych wyników:
   - Wyniki testów nie będą pokazywać pełnego obrazu podatności czy luk bezpieczeństwa systemu.
   - Mitygacja: Zastosowanie różnorodnych narzędzi do testowania (Nmap, BurpSuite, ZAP) i wykorzystanie wszelakich dostępnych sposobów, celem dostarczenia pełnego spektrum poglądu na podatności dostępne w systemach.

5. Zasoby

- Zespół pentesterów: 3 osoby
- Zespół SmartBank: Kontakt z dyrektorem ds. IT oraz zespołem bezpieczeństwa SmartBanku, celem weryfikowania oraz konsultacji podczas testów.

Rules of Engagement

1. Obszar testowania

Aplikacja mobilna i webowa:

- Testy będą obejmować ocenę bezpieczeństwa aplikacji mobilnej i webowej SmartBanku, ze szczególnym uwzględnieniem zidentyfikowania podatności zawartych w standardzie OWASP (SQL Injection, XSS, CSRF, Broken Access Control).
- Dodatkowe testy będą przeprowadzone w zakresie bezpieczeństwa uwierzytelniania, zarządzania sesjami oraz odporności mechanizmów uwierzytelniania na ataki brute-force.
- Celem jest identyfikacja potencjalnych luk umożliwiających uzyskanie nieautoryzowanego dostępu do danych klientów.

Infrastruktura sieciowa:

- Przeprowadzona zostanie enumeracja sieci wewnętrznej, mająca na celu zidentyfikowanie otwartych portów i wystawionych usług, będących potencjalnym wektorem ataku.
- Testy sieci wewnętrznej obejmą skanowanie pod kątem podatności (np. niewłaściwie skonfigurowane urządzenia, słabe hasła dostępowe do urządzeń, przestarzałe wersje oprogramowania)
- Sprawdzona zostanie efektywność polityk bezpieczeństwa, zwłaszcza dotyczących szkolenia pracowników w zakresie rozpoznawania phishingu.

Chmura prywatna:

- Analiza konfiguracji środowiska chmurowego pod kątem zgodności z najlepszymi praktykami bezpieczeństwa.
- Audyt konfiguracji Identity and Access Managment, z uwzględnieniem zasady najniższego przywileju, dobrych praktyk ABAC/RBAC, oraz specyfikacji haseł i zasad ich rotowania.
- Ocena tworzenia i przechowywania logów, oraz poufnego zarządzania danymi w chmurze, w tym zgodności z regulacjami RODO.

2. Metodologia testów

Testy zostaną przeprowadzone zgodnie z najlepszymi praktykami i standardami branżowymi:

- **OWASP Top 10:** Testy aplikacji mobilnej i webowej będą oparte na najnowszych wytycznych OWASP.
- **NIST SP 800-115:** Testy penetracyjne infrastruktury sieciowej oraz chmurowej.
- **CIS Benchmarks:** Testy konfiguracji serwerów i urządzeń sieciowych zgodnie z wytycznymi CIS.
- **Socjotechnika:** Testy na odporność na ataki phishingowe oraz szkolenia pracowników z rozpoznawania zagrożeń.

3. Podział czasu

1. Faza przygotowawcza:

- Uzyskanie wymaganych autoryzacji, podpisanie SoW, podpisanie klauzuli RODO, uzgodnienie dostępów: 1 dzień.
- Konfiguracja środowiska testowego: 1 dzień.

2. Faza testowania:

- Aplikacja mobilna i webowa: 4 dni.
- Infrastruktura sieciowa: 3 dni.
- Chmura prywatna: 2 dni.

3. Faza raportowania:

- Przygotowanie raportu końcowego: 2 dni.
- Prezentacja wyników i rekomendacji zarządowi: 1 dzień.

Całkowity czas trwania: 14 dni roboczych.

4. Analiza i zarządzanie ryzykiem

Ryzyka:	**Mitygacje:**
Przerwy w działaniu aplikacji mobilnej/webowej – Średnie.	Testy zostaną przeprowadzone w godzinach najmniejszego ruchu lub w oknach serwisowych.
Utrata danych produkcyjnych – Niskie.	Testy nie będą przeprowadzane w środowisku produkcyjnym. Testowanie z wykorzystaniem środowiska staging z kopią zapasową danych.
Naruszenie zgodności z przepisami RODO – Średnie.	Testy będą zgodne z regulacjami RODO. Dane osobowe klientów będą anonimizowane.
Zakłócenie działania infrastruktury sieciowej – Niskie.	Testy sieciowe będą wykonywane poza godzinami szczytu lub w oknach serwisowych ustalonych z zespołem IT.

- Wszystkie testy będą prowadzone zgodnie z wytycznymi dotyczącymi zgodności z przepisami oraz klauzulą RODO.
- Codziennie odbędą się krótkie spotkania informacyjne z przedstawicielami zespołu bezpieczeństwa SmartBanku, aby informować o postępach prac i zgłaszanych problemach.
- Każde wykrycie krytycznej podatności będzie natychmiast raportowane zespołowi bezpieczeństwa SmartBanku lub bezpośrednio dyrektorowi ds. IT.
- Wyniki testów zostaną zabezpieczone i przekazane wyłącznie osobom do tego upoważnionym.

5. Ograniczenia testów

- Testy penetracyjne nie będą obejmować bezpośrednio systemów produkcyjnych (w zakresie wprowadzania zmian), aby nie zakłócać usług dla klientów ani nie zagrażać potencjalną utratą danych.
- Testy będą prowadzone na wyznaczonych środowiskach stagingowych lub kopiach systemów w określonych wersjach.
- **Wyłączenia:** systemy niezwiązane bezpośrednio z obsługą klientów oraz bankowością online (np. systemy kadrowe) nie będą testowane.