CIS-WAZ.2720.18.2018

Warszawa, dnia 6 lipca 2018 r.

Dotyczy: *zapytania ofertowego CIS-WAG.2720.18.2018 28 czerwca 2018 r. Opracowanie planu testów bezpieczeństwa API BDL, ich wykonanie oraz przygotowanie raportu z testów i zasad bezpieczeństwa testowanego systemu" na potrzeby realizacji projektu „Otwarte dane – dostęp, standard, edukacja".*

W dniu 5 lipca 2018 r. do Zamawiającego wpłynęły następujące pytania:

Pytanie 1

Ile i jakie (typ, wersja) systemy operacyjne, bazy danych, serwery i inne komponenty (jeśli są) będą objęte audytem konfiguracji/hardeningiem?

Odpowiedź 1

Sewer aplikacyjny : Windows Server 2012 R2, IIS wersja 8.5, NetCore 2.1.1
Sewer bazodanowy : MS SQL Server 2012 Enterprise Edition SP4 / Windows Server 2008 R2 Enterprise

Pytanie 2

Czy Zamawiający ma jakieś preferencje dotyczące metodyki wykorzystanej podczas audytu konfiguracji czy może to być np. CIS benchmark (https://www.cisecurity.org)?

Odpowiedź 2

Tak

Pytanie 3

Czy Zamawiający udostępni wykonawcy konta do audytowanych elementów infrastruktury (np. systemów operacyjnych, baz danych) - o uprawnieniach, które umożliwią wykonanie audytu konfiguracji przy wsparciu narzędzi automatycznych tj. Nesssus?

Odpowiedź 3

Tak

Pytanie 4

Czy dobrze rozumiemy, że system API BDL to API (application programming interface)?

Odpowiedź 4

Tak

Pytanie 5

Jeśli tak jakiego jakiego typu jest to API - REST/SOAP, jeśli nie to jaki to system webaplikacja, gruby klient?

Odpowiedź 5

REST, brak SOAP.

Pytanie 6

Ile metod/funkcji system udostępnia użytkownikom?

Odpowiedź 6

33 metody (get)

Pytanie 7

Ile jest mniej więcej parametrów wejściowych/wyjściowych w każdej metodzie/funkcji systemu?

Odpowiedź 7

Max 9 parametrów

Pytanie 8

Czy moglibyśmy otrzymać przykładowe komunikaty?

Odpowiedź 8

Przykłady :
Lista tematów najwyższego poziomu (fragment):

```
<subjectList xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <totalRecords>31</totalRecords>
        <page>0</page>
        <pageSize>10</pageSize>
        <links>
                <firstPage>/api/v1/subjects?format=xml&page=0&pageSize=10</firstPage>
                <self>/api/v1/subjects?format=xml&page=0&pageSize=10</self>
                <nextPage>/api/v1/subjects?format=xml&page=1&pageSize=10</nextPage>
                <lastPage>/api/v1/subjects?format=xml&page=3&pageSize=10</lastPage>
        </links>
        <results>
                <subject>
                        <id>K15</id>
                        <name>CENY</name>
                        <hasVariables>false</hasVariables>
                        <children>
                        <id>G186</id>
                        <id>G189</id>
                        <id>G405</id>
                        <id>G188</id>
                        <id>G187</id>
                        </children>
                </subject>
                <subject>
                        <id>K43</id>
                        <name>FINANSE PRZEDSIĘBIORSTW</name>
                        <hasVariables>false</hasVariables>
                        <children>
                        <id>G418</id>
                        <id>G576</id>
                        </children>
```

```
            </subject>
            [...]
        </results>
</subjectList>
```

Lista tematów najwyższego poziomu w formacie JSON:

```
{
 "totalRecords":31,
 "page":0,
 "pageSize":10,
 "links":{
  "firstPage":"/api/v1/subjects?format=json&page=0&pageSize=10",
  "self":"/api/v1/subjects?format=json&page=0&pageSize=10",
  "nextPage":"/api/v1/subjects?format=json&page=1&pageSize=10",
  "lastPage":"/api/v1/subjects?format=json&page=3&pageSize=10"
 },
 "results":[
 {
  "id":"K15",
  "name":"CENY",
  "hasVariables":false,
  "children":["G186","G189","G405","G187","G188"]
 },
 {
  "id":"K43",
  "name":"FINANSE PRZEDSIĘBIORSTW",
  "hasVariables":false,
  "children":["G576","G418"]
 },
 [...]
 ]
}
```

Szczegóły tematu o ID=K3 w formacie XML:

```
<subjectDetails xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <id>K3</id>
        <name>LUDNOŚĆ</name>
        <hasVariables>false</hasVariables>
        <children>
            <id>G564</id>
            <id>G535</id>
            <id>G8</id>
            <id>G7</id>
            <id>G10</id>
            <id>G557</id>
            <id>G534</id>
        </children>
        <lastUpdate>2018-01-30T14:06:07.053</lastUpdate>
        <description>
```

Bilanse liczby i struktury ludności w gminach imiennie opracowane w oparciu o wyniki Narodowych Spisów Powszechnych z uwzględnieniem zmian spowodowanych ruchem naturalnym (urodzenia i zgony), migracjami ludności (na pobyt stały i czasowy) oraz przemieszczeniami związanymi ze zmianami administracyjnymi. Dane o ludności w miejscowościach na podstawie rejestru PESEL. Dane o zarejestrowanych małżeństwach, urodzeniach i zgonach pochodzące ze sprawozdawczości urzędów stanu cywilnego. Dane o orzeczonych rozwodach i separacjach pochodzące ze sprawozdawczości sądów. Dane o migracjach wewnętrznych i zagranicznych na pobyt stały pochodzące z Ministerstwa Spraw Wewnętrznych. Prognoza ludności na podstawie badania GUS.

```
        </description>
```

</subjectDetails>
Szczegóły tematu o ID=K3 w formacie JSON:
{
"id":"K3",
"name":"LUDNOŚĆ",
"hasVariables":false,
"children":["G8","G564","G535","G7","G10","G534","G557"],
"lastUpdate":"2018-01-30T14:06:07.053",
"description":"Bilanse liczby i struktury ludności w gminach imiennie opracowane w oparciu o wyniki Narodowych Spisów Powszechnych z uwzględnieniem zmian spowodowanych ruchem naturalnym (urodzenia i zgony), migracjami ludności (na pobyt stały i czasowy) oraz przemieszczeniami związanymi ze zmianami administracyjnymi.\nDane o ludności w miejscowościach na podstawie rejestru PESEL.\nDane o zarejestrowanych małżeństwach, urodzeniach i zgonach pochodzące ze sprawozdawczości urzędów stanu cywilnego.\nDane o orzeczonych rozwodach i separacjach pochodzące ze sprawozdawczości sądów.\nDane o migracjach wewnętrznych i zagranicznych na pobyt stały pochodzące z Ministerstwa Spraw Wewnętrznych.\nPrognoza ludności na podstawie badania GUS."
}
Komunikat błędu o nieistniejącym zasobie w formacie XML:
<message>
<errors>
<error>
<errorResult>Zasób nie istnieje</errorResult>
<errorReason>Nie znaleziono zasobu o podanym identyfikatorze</errorReason>
<errorSolution>Proszę sprawdzić poprawność identyfikatora zasobu</errorSolution>
<errorCode>3</errorCode>
<errorHelp>/api/v1/help/code/3</errorHelp>
</error>
</errors>
</message>
Komunikat błędu o nieistniejącym zasobie w formacie JSON:
{
"errors": [
{
"errorResult": "Zasób nie istnieje",
"errorReason": "Nie znaleziono zasobu o podanym identyfikatorze",
"errorSolution": "Proszę sprawdzić poprawność identyfikatora zasobu",
"errorCode": 3,
"errorHelp": "/api/v1/help/code/3"
}
]
}

Pytanie 9

Czy system posiada autoryzację, jeśli tak to ile jest jej poziomów - typów kont w systemie?

Odpowiedź 9

Liczba żądań może być limitowana na klucz API, dostęp do zasobów jest pełny dla wszystkich – również dla użytkowników anonimowych . API jest tylko do odczytu.

Pytanie 10

Czy otrzymamy konta do testowanego systemu (testy grey box)?

Odpowiedź 10

Na potrzeby testów udostępniony będzie dostęp limitowany i nielimitowany.

Pytanie 11

Czy testy mają zastać wykonane na wszystkich typach kont?

Odpowiedź 11

Testy powinny być wykonane z użyciem klucza API i bez niego.

Pytanie 12

Czy testowany system ma jakieś powiązanie z publicznie dostępnym API Bank Danych Lokalnych dostępnym pod adresem https://mojepanstwo.pl/api/bdl?

Odpowiedź 12

Nie

Pytanie 13

Czy oferta może być złożona jedynie w postaci elektronicznej na adres wskazany w zapytaniu?

Odpowiedź 13

Tak

DYREKTOR
Stanisław Sielużycki