



**Doświadczenia Urzędu Miasta Stołecznego Warszawy
w realizacji audytów bezpieczeństwa informacji
oraz ochrony danych osobowych
w świetle zmieniającego się otoczenia prawnego**

Biuro Audytu Wewnętrznego Urzędu m.st. Warszawy



Wymagania KRI - § 20 ust. 2

- wielkim wyzwaniem organizacyjnym dla Urzędu m.st. Warszawy

- 14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, **nie rzadziej niż raz na rok.**



Miasto Stołeczne Warszawa

Podstawowym wyzwaniem
duża liczba audytowanych jednostek

Należy pamiętać, że:

Miasto Stołeczne Warszawa to:

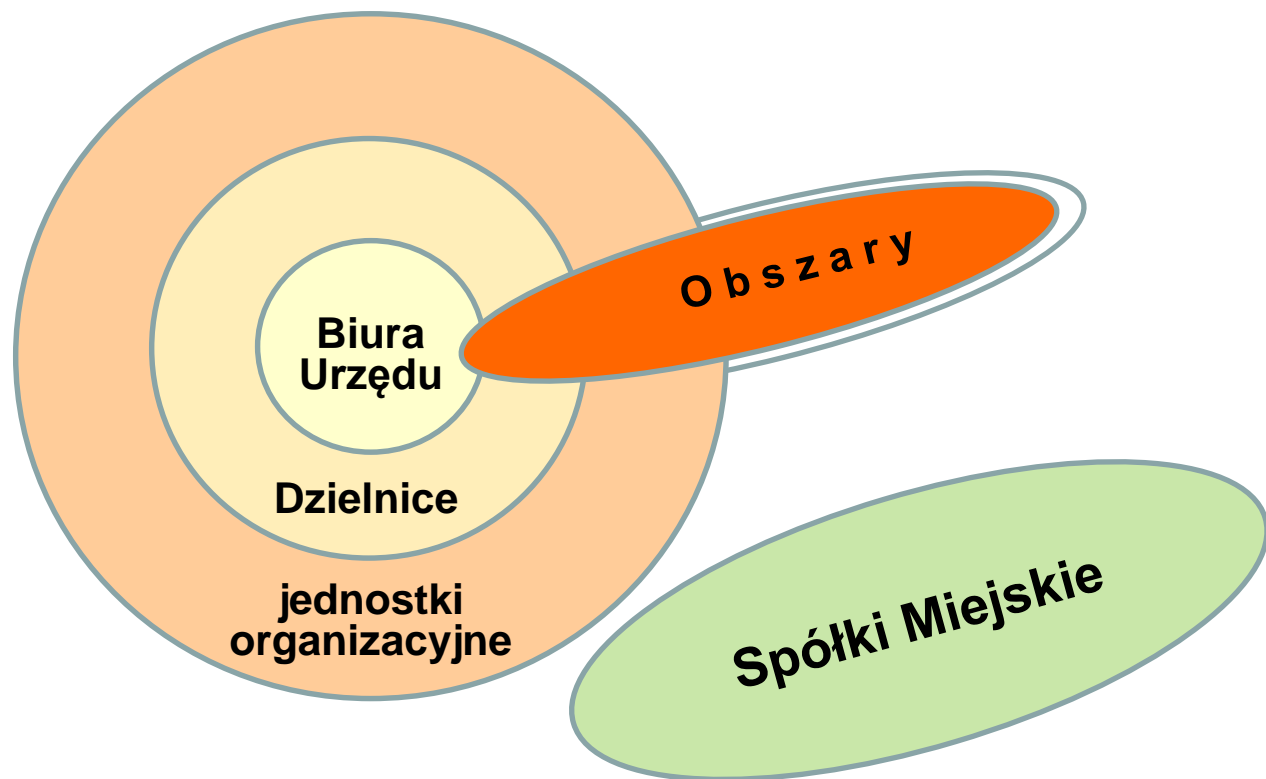
- **40** Biur Urzędu
- **18** Urzędów Dzielnic
- **ponad 1000** jednostek organizacyjnych i osób prawnych, które podlegają lub są nadzorowane przez Prezydenta m.st. Warszawy





Miasto Stołeczne Warszawa

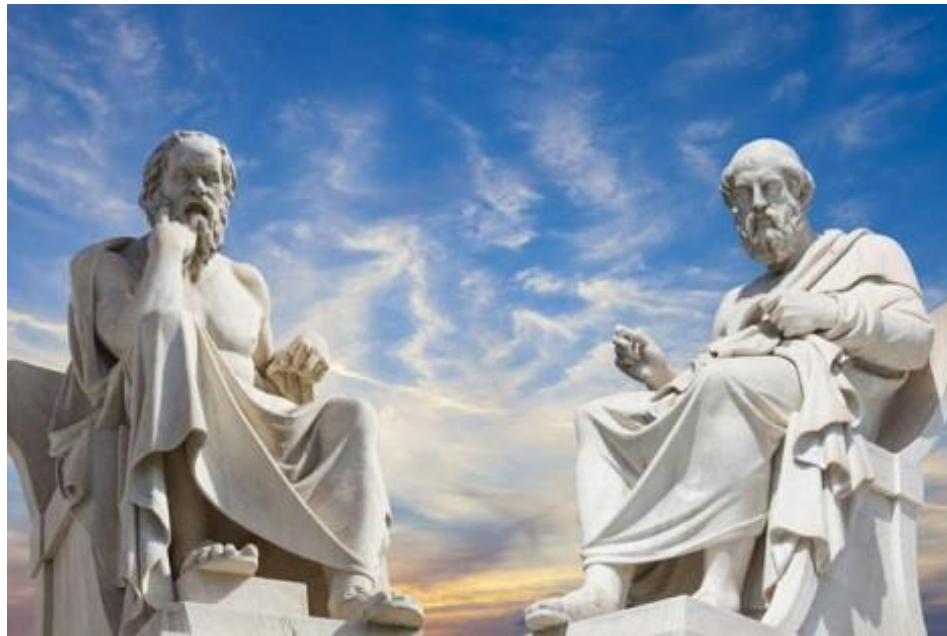
Podstawowym wyzwaniem
duża liczba audytowanych jednostek



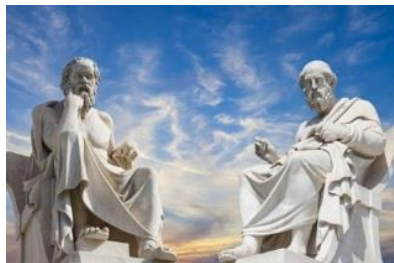
Miasto Stołeczne Warszawa

Potencjalne możliwości i wybór rozwiązania

Filozofia różnych dróg zapewnienia audytu w m.st. Warszawa



Fot. shutterstock.com



Poszukiwanie optymalnej drogi postępowania

Filozofie różnych dróg prowadzących do celu ...

W realizowanym rozwiązaniu organizacyjnym uwzględniono propozycje zgłoszone w grupie dyskusyjnej wskazując następujące kierunki:

- ✓ drogi tradycyjnej poprzez **audyty zapewniające**.
- ✓ ścieżki pomocniczej poprzez **audyty analityczne**

Wybór właściwej drogi zależy od wyników przeprowadzonej analizy ryzyka i rachunku kosztów.

Wyboru dokonał Prezydent m.st. Warszawy w uzgodnieniu osobą kierującą audytem.

Pierwsze działania organizacyjne

- Trochę historii

- **2008**: Pierwszy audyt bezpieczeństwa informacji w Urzędzie (w tym w Urzędach Dzielnic – wsparcie eksperta zewnętrznego),
- **2011-12**: audyty bezpieczeństwa informacji i ochrony danych osobowych zrealizowany własnymi zasobami osobowymi. Komórki audytu wspierane przez pracowników komórki IT oraz ochrony danych osobowych,
- **2013**: audyt bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie zrealizowany przez usługodawcę zewnętrznego,
- **2013**: audyt zapewniający bezpieczeństwo informacji i ochrony danych osobowych w wybranych jednostkach organizacyjnych m.st. Warszawy zrealizowany przez pracowników nowo utworzonej komórki w ramach audytu.
- **2013**: 1-szy audyt analityczny bezpieczeństwa informacji i ochrony danych osobowych w wybranych jednostkach organizacyjnych Miasta Stołecznego Warszawy (58 jednostek),
- Od **2015 roku** audyt zapewniający bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie i w wybranych jednostkach organizacyjnych Miasta Stołecznego Warszawy realizowany przez pracowników komórki audytu,
- Od **2017** audyt analityczny wszystkich jednostkach organizacyjnych Miasta Stołecznego Warszawy w zrealizowany przy wykorzystaniu systemu informatycznego.

Program zadania audytowego zapewniającego - wyciąg

1. Bezpieczeństwo informacji i ochrony danych osobowych na poziomie całej jednostki:

- a) Organizacja procesu zarządzania bezpieczeństwem informacji i ochrony danych osobowych,
- b) Działania prewencyjne w kierunku zapewnienia bezpieczeństwa informacji,
- c) System zarządzania uprawnieniami do przetwarzania danych osobowych,
- d) Zarządzanie zasobami informatycznymi,
- e) Identyfikacja i analiza ryzyka w kierunku utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do przeprowadzonej analizy; ocena skutków dla ochrony danych.

Program zadania audytowego zapewniającego - wyciąg

- f) Zarządzanie incydentami bezpieczeństwa informacji, naruszenia ochrony danych osobowych,
- g) Ochrona przed złośliwym oprogramowaniem,
- h) Bezpieczeństwo sieci informatycznej,
- i) Testowanie, nadzorowanie i monitorowanie bezpieczeństwa.

2. Bezpieczeństwo IT na poziomie wybranego systemu

- a) Dokumentacja techniczna systemu informatycznego,
- b) Zarządzanie kontami i uprawnieniami użytkowników systemu informatycznego,
- c) Zapewnienie ochrony przetwarzanych informacji przed nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,
- d) Rozliczalność działań podejmowanych w systemie informatycznym.

Program zadania audytowego zapewniającego - wyciąg

3. Ocena serwisów internetowych pod względem bezpieczeństwa oraz spełniania wymagań WCAG wskazanych w Rozporządzeniu KRI:

- a) Monitorowanie, testowanie i eliminowanie podatności serwisów internetowych,
- b) Delegowanie odpowiedzialności w procesie zarządzania informacjami zamieszczanymi,
- c) Dostosowanie serwisów internetowych do wymagań WCAG wskazanych w Rozporządzeniu KRI.

W realizacji audytów
wykorzystujemy ocenę dojrzałości organizacji
wg metodyki COBIT 4.1,
aby ustalić dostosowanie / spełnienie wymogów
Rozporządzenia KRI oraz RODO

Metodyka COBIT 4.1 6 stopni modelu dojrzałości organizacji

Poziom dojrzałości organizacji	Opis poszczególnych poziomów dojrzałości organizacji
0 - Nieistniejący	Całkowity brak rozpoznawalnych procesów. Organizacja nie dostrzegła nawet istnienia problemu, który wymaga rozwiązania.
1 - Wstępny/doraźny	Istnieją dowody na to, że organizacja dostrzegła problemy wraz z koniecznością ich rozwiązania. Nie są to jednak ustandaryzowane procesy. Zamiast nich, do rozwiązywania poszczególnych problemów stosuje się doraźne podejście. Ogólne podejście do zarządzania nie jest podejściem zorganizowanym.
2 - Powtarzalny lecz intuicyjny	Procesy zostały rozwinięte do poziomu, na którym różne osoby wykonujące to samo zadanie postępują zgodnie z podobnymi procedurami. Nie ma formalnych szkoleń, standardowe procedury nie zostały zakomunikowane, a podjęcie odpowiedzialności pozostawiono jednostkom. Występuje wysoki poziom zależności od wiedzy poszczególnych osób, dlatego prawdopodobne jest występowanie błędów.

Metodyka COBIT 4.1 6 stopni modelu dojrzałości organizacji

Poziom dojrzałości organizacji	Opis poszczególnych poziomów dojrzałości organizacji
3 - Zdefiniowane procesy	Istnieją ustandaryzowane i udokumentowane procedury, które zostały zakomunikowane poprzez szkolenie. Pracownicy są upoważnieni do ich stosowania. Jest jednak mało prawdopodobne, że odstępstwa od stosowania procedur zostaną wykryte. Procedury nie są zaawansowane, a są raczej formalizacją istniejących praktyk.
4 - Kontrolowany i mierzalny	Kierownictwo monitoruje i ocenia zgodność z procedurami, a także podejmuje odpowiednie czynności, gdy procesy nie działają efektywnie. Procesy są stale doskonalone i stanowią źródło dobrych praktyk. W ograniczony lub fragmentaryczny sposób wykorzystywane są rozwiązania zautomatyzowane oraz narzędzia.
5 - Zoptymalizowany	Procesy zostały dopracowane do poziomu dobrej praktyki w oparciu o efekty ciągłego doskonalenia i modelowanie dojrzałości w innych organizacjach. Technologia informatyczna jest wykorzystywana w zintegrowany sposób do automatyzacji toku pracy, zapewniając narzędzia służące poprawie jakości i wydajności oraz sprawiając, że jednostka szybko adaptuje się do zmieniających się warunków.

Co oceniamy?

Oceniane obszary i podobszary – Poziom dojrzałości jednostki w skali 0-5		Jednostka 1	Jednostka 2	Jednostka 3	Jednostka 4	Jednostka 5	Jednostka 6
Bezpieczeństwo informacji i ochrony danych osobowych na poziomie całej jednostki	a) Organizacja procesu zarządzania bezpieczeństwem informacji i ochrony danych osobowych	2	2	1	1	2	1
	b) Działania prewencyjne w kierunku zapewnienia bezpieczeństwa informacji	1	2	0	0	1	0
	c) System nadawania upoważnień do przetwarzania danych osobowych	2	3	1	1	3	2
	d) Zarządzanie zasobami informatycznymi	1	1	0	1	2	1
	e) Identyfikacja i analiza ryzyka w kierunku utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko stosownie do przeprowadzonej analizy	2	1	1	1	2	0
	f) Zarządzanie incydentami bezpieczeństwa informacji	3	1	0	1	1	1
	g) Ochrona przed złośliwym oprogramowaniem	4	1	0	1	1	1
	h) Bezpieczeństwo sieci informatycznej	4	1	1	0	2	2
	i) Testowanie, nadzorowanie i monitorowanie bezpieczeństwa	2	1	2	0	2	1
Bezpieczeństwo IT na poziomie wybranego systemu	a) Dokumentacja techniczna systemu informatycznego	4	1	0	1	2	1
	b) Zarządzanie kontami i uprawnieniami użytkowników systemu informatycznego	4	3	0	1	1	1
	c) Zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami	3		0	1	1	0
Ocena bezpieczeństwa serwisów internetowych oraz spełniania wymagań WCAG 2.0	a) Monitorowanie, testowanie i eliminowanie podatności serwisów internetowych w tym BIP	1	0	0	0	0	0
	b) Delegowanie odpowiedzialności w procesie zarządzania informacjami zamieszczanymi w BIP	3	1	1	1	2	1
	c) Dostosowanie serwisów internetowych do wymagań WCAG 2.0 wskazanych w Rozporządzeniu KRI	1	0	0	0	1	0

Audyt zapewniający

Ocena dojrzałości

oraz rzeczywiste badanie systemów informatycznych

Dlaczego badając obszar bezpieczeństwa informacji zagłębiamy się w badania systemów informatycznych?

W dokumentach jak w pentagonie,



realizacja jak w przedszkolu.

Audyt zapewniający

Co badamy poza dokumentacją?

- Stan aktualizacji stacji roboczych i serwerów pod kątem oprogramowania systemowego i niesystemowego – realizowane za pomocą skanera podatności

GFI LanGuard

Dashboard Scan Remediate Activity Monitor Reports Configuration Utilities

Launch a New Scan

Scan Target: localhost Profile: Full Scan

Credentials: Currently logged on user Username: Password: Key file: Scan

Scan Results Overview

Scan target: localhost

- 192.168.1.3 [004910014013-0] (Windows 7 x64)
- Vulnerability Assessment
 - High Security Vulnerabilities (12)
 - Medium Security Vulnerabilities (5)
 - Low Security Vulnerabilities (5)
 - Potential Vulnerabilities (2)
 - Missing Service Packs and Update Rollu...
 - Missing Security Updates (6)
- Network & Software Audit
 - System patching status
 - Ports
 - Hardware
 - Software
- System Information
 - Shares (4)
 - Password Policy
 - Security Audit Policy (Off)
 - Registry
 - NetBIOS Names (3)
 - Computer
 - Groups (15)
 - Users (5)
 - Logged On Users (9)
 - Sessions (5)
 - Services (87)

Scan Results Details

192.168.1.3 [004910014013-0] (Windows 7 x64)

Vulnerability level:

The average vulnerability level for this scanning session is: **High**

Top 5 issues to address:

- 2019-Apr-4493435 2019-04 Cumulative Security Update for Internet Explorer 11 for Windows 7 for x64-based systems (KB4493435)
- 2019-03 Update for Windows 7 for x64-based Systems (KB4490128)
- Security Update for Microsoft Excel 2010 (KB4462230) 32-Bit Edition
- Security Update for Microsoft Office 2010 (KB4464520) 32-Bit Edition
- 2019-Apr-4493448 2019-04 Security Only Quality Update for Windows 7 for x64-based Systems (KB4493448)

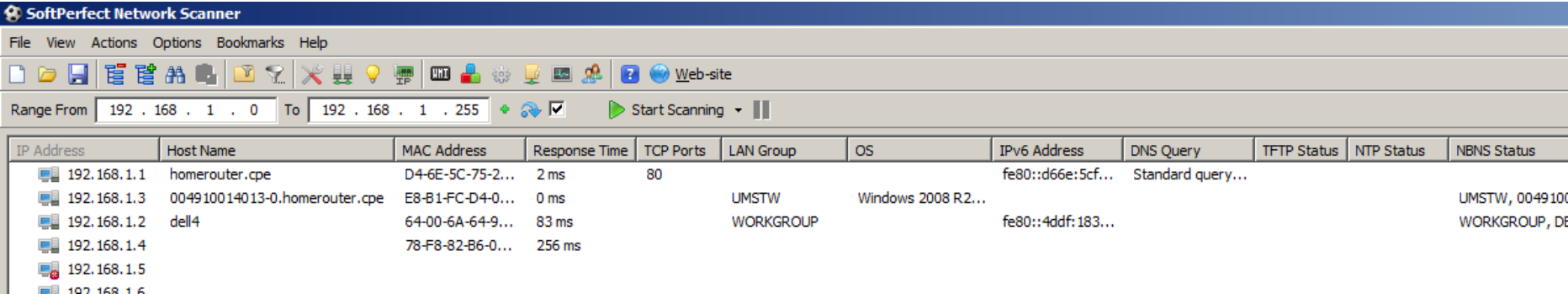
Results statistics:

- Missing software updates:
- Other vulnerabilities:
- Potential vulnerabilities:
- Installed applications:
- Open ports:

Audyt zapewniający

Co badamy poza dokumentacją?

- Usługi uruchomione w wewnętrznych sieciach komputerowych, udostępnione udziały sieciowe, urządzenia sieciowe – realizowane za pomocą automatycznych skanerów



SoftPerfect Network Scanner

File View Actions Options Bookmarks Help

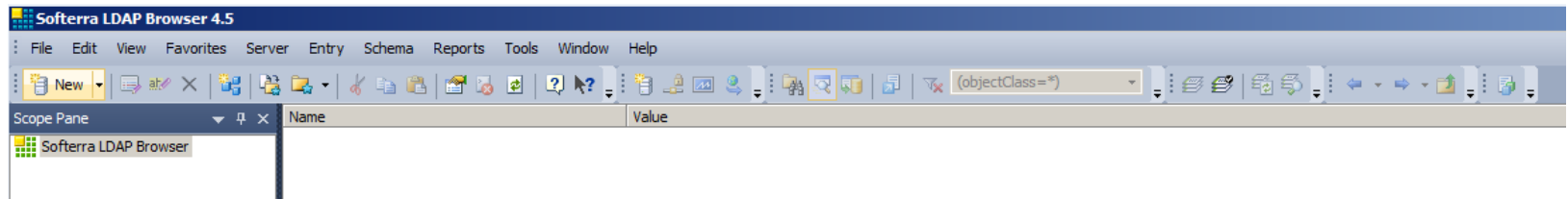
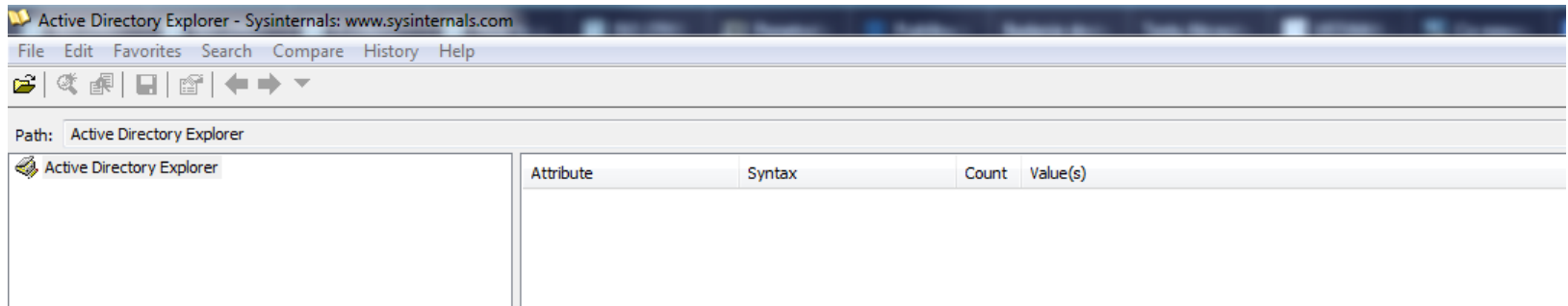
Range From 192 . 168 . 1 . 0 To 192 . 168 . 1 . 255 Start Scanning

IP Address	Host Name	MAC Address	Response Time	TCP Ports	LAN Group	OS	IPv6 Address	DNS Query	TFTP Status	NTP Status	NBNS Status
192.168.1.1	homerouter.cpe	D4-6E-5C-75-2...	2 ms	80			fe80::d66e:5cf...	Standard query...			
192.168.1.3	004910014013-0.homerouter.cpe	E8-B1-FC-D4-0...	0 ms		UMSTW	Windows 2008 R2...					UMSTW, 0049100
192.168.1.2	dell4	64-00-6A-64-9...	83 ms		WORKGROUP		fe80::4ddf:183...				WORKGROUP, DE
192.168.1.4		78-F8-82-B6-0...	256 ms								
192.168.1.5											
107.168.1.6											

Audyt zapewniający

Co badamy poza dokumentacją?

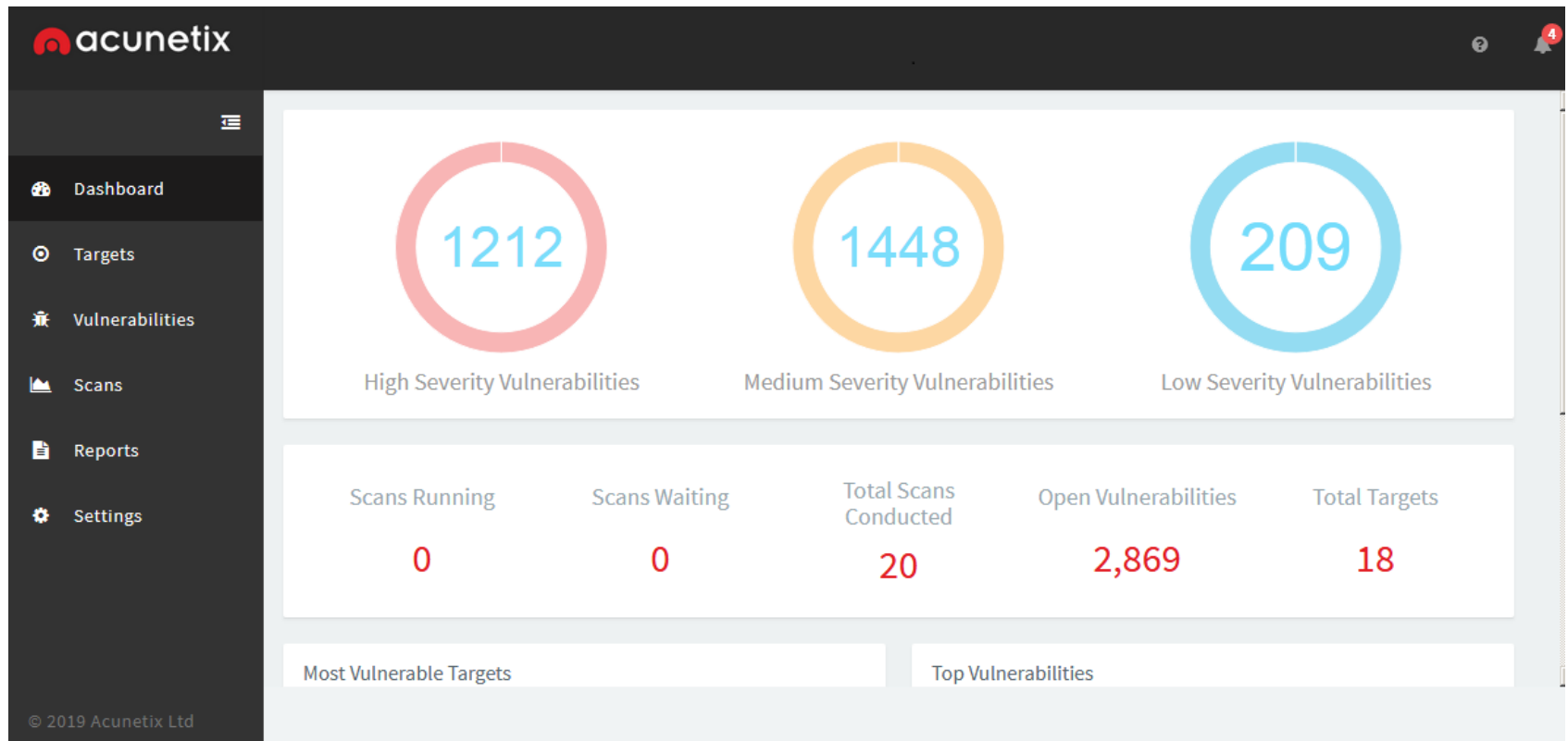
- Ustawienia polityk usługi katalogowej Active Directory



Audyt zapewniający

Co badamy poza dokumentacją?

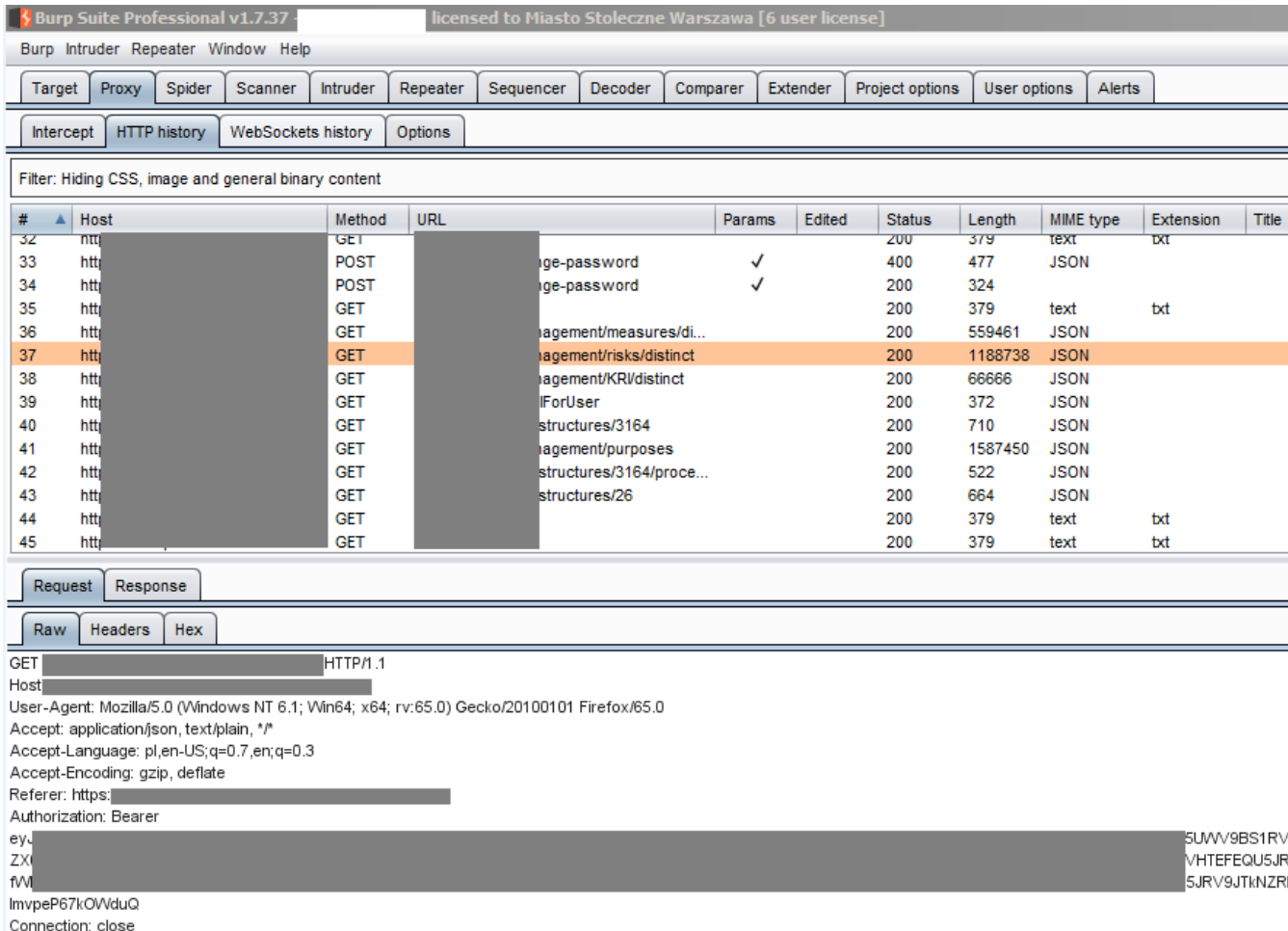
- Testy bezpieczeństwa serwisów internetowych – automatyczny skaner podatności



Audyt zapewniający

Co badamy poza dokumentacją?

- Testy bezpieczeństwa serwisów internetowych - testy manualne



Burp Suite Professional v1.7.37 licensed to Miasto Stołeczne Warszawa [6 user license]

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
32	htt	GET				200	379	text	txt	
33	htt	POST		age-password	✓	400	477	JSON		
34	htt	POST		age-password	✓	200	324			
35	htt	GET				200	379	text	txt	
36	htt	GET		agement/measures/di...		200	559461	JSON		
37	htt	GET		agement/risks/distinct		200	1188738	JSON		
38	htt	GET		agement/KRV/distinct		200	66666	JSON		
39	htt	GET		lForUser		200	372	JSON		
40	htt	GET		tructures/3164		200	710	JSON		
41	htt	GET		agement/purposes		200	1587450	JSON		
42	htt	GET		tructures/3164/proce...		200	522	JSON		
43	htt	GET		tructures/26		200	664	JSON		
44	htt	GET				200	379	text	txt	
45	htt	GET				200	379	text	txt	

Request Response

Raw Headers Hex

GET [redacted] HTTP/1.1

Host: [redacted]

User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:65.0) Gecko/20100101 Firefox/65.0

Accept: application/json, text/plain, *

Accept-Language: pl,en-US;q=0.7,en;q=0.3

Accept-Encoding: gzip, deflate

Referer: https://[redacted]

Authorization: Bearer

eyJ... [redacted] SUWW9BS1RV

ZXN... [redacted] VHTFEQU5JR'

fW... [redacted] SJRV9JTKNZRE

ImvpeP67kOWduQ

Connection: close

Audyt zapewniający

Co badamy poza dokumentacją?

- Pliki potencjalnie objęte prawami autorskimi
- Pliki potencjalnie szkodliwe, crack-i,
- Licencje na zainstalowane oprogramowanie
- Zintegrowane zapory sieciowe – czy skonfigurowane, czy zarządzane
- Systemy bezpieczeństwa – czy aktualne definicje
- Logi z systemów
- WCAG

Audyt zapewniający


Dlaczego wychodzimy poza badanie dokumentacji

- kierownictwo komórek audytowanych dostaje informacje o faktycznym stanie bezpieczeństwa, a nie tylko tym wynikającym z istnienia dokumentacji
- zwykle wiele czynności nie jest udokumentowanych (brak czasu, wygoda, bycie niezastąpionym)
- brak Systemu Zarządzania Bezpieczeństwem Informacji – działania informatyków są często podejmowane zwyczajowo
- działania komórek IT są trudne do kontrolowania bez wiedzy informatycznej
- nadzór i rozliczanie wewnętrznych służb IT lub podmiotów zewnętrznych świadczących opiekę informatyczną jest nierzadko dla kierowników audytowanych komórek zadaniem trudnym
- organizacja uczy się realizując zadania

Audyty analityczne i zapewniające

Wspólne elementy ...


Księga procedur:

 URZĄD MIASTA STOLECZNEGO WARSZAWY Biuro Audytu Wewnętrznego ul. Wspólna, Składowa 100-101 Warszawa, tel. 22 443 28 71, 22 443 28 71, 24 44 44 30 71, 24 44 44 30 71 Kontakt: MSto, Kuchnia, Kuchnia, Kuchnia, Kuchnia, Kuchnia	
KSIĘGA PROCEDUR BIURA AUDYTU WEWNĘTRZNEGO URZĘDU M.ST. WARSZAWY	
STANDARD 2040 ZASADY I PROCEDURY	
MIĘDZYNARODOWE STANDARDY PRAKTYKI ZAWODOWEJ AUDYTU WEWNĘTRZNEGO	
AKCEPTOWAŁ	ZATWIERDZIŁ
DYREKTOR BIURA AUDYTU WEWNĘTRZNEGO AUDYTOR GENERALNY <i>Bożena Stoma</i>	PREZYDENT MIASTA STOLECZNEGO WARSZAWY <i>Hanna Gronkiewicz-Waltz</i>
29.06.2018 Data podpis	Data podpis
Przygotowano w Wydziale Wsparcia Merytorycznego	

Audyty analityczne i zapewniające

Wspólne elementy ...

Program zadania:

 URZĄD MIASTA STOLECZNEGO WARSZAWY
Biuro Audytu Wewnętrznego
ul. Hojciecha Górskiego 7, 00-033 Warszawa, tel. 22 443 30 70, 22 443 30 71, faks 22 443 30 72
Sekretariat BAW@um.warszawa.pl, www.um.warszawa.pl

AW-BST.1720.33.2018

Program audytu analitycznego

pn.: „Ocena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych w kontekście zmieniającego się otoczenia prawnego”

Liczba stron: 7

Zatwierdzam

DYREKTOR
BIURA AUDYTU WEWNĘTRZNEGO
AUDYTOR GENERALNY
Bożena Stom

OCENA
WYDOLNIAJĄCYCH SIĘ
SYSTEMÓW I ICH
W BUDNIE AUDYTU
WENĘTRZNEGO
Dorota Rydz
Dorota Rydz, Dyrektor

Warszawa, dnia ... listopada 2018 r

Audyt analityczny

Mocne strony

Przykładowe mocne strony:

1. Audyt analityczny jest ukierunkowany na jednoczesne badanie licznych grup jednostek samorządu terytorialnego (JST). Podstawą badania są odpowiedzi w tym samym czasie, na takie same pytania zawarte w kwestionariuszu.
2. Relatywnie „krótki” czas zadania audytowego w formie audytu analitycznego, niemożliwy do uzyskania w formie audytu zapewnającego, przy tak dużej zróżnicowanej populacji.
3. Przejrzysta prezentacja wyników audytu.


Audyt analityczny

Problemy i ryzyka

- niezrozumienie pytań, spowodowane m.in. niedostatecznymi kompetencjami merytorycznymi lub niezrozumieniem językowym,
- brak obecności badającego w procesie przeprowadzania badania, który mógłby wyjaśnić wątpliwości na bieżąco,
- zafałszowanie udzielanych odpowiedzi, które mogą być spowodowane chęcią osiągnięcia lepszych wyników ankiety, według subiektywnego zrozumienia jej przez wypełniającego lub niską motywacją badanego do udzielenia rzetelnych odpowiedzi na zadane pytania,
- niepełne dostosowanie pytań do szczegółowej specyfiki jednostek przy użyciu wystandaryzowanego narzędzia informatycznego,
- problemy techniczne z funkcjonowaniem narzędzia informatycznego, zarówno w warstwie sprzętowej jak i programowej,
- brak kontroli nad czynnikami zewnętrznymi, które mogą rozpraszać osobę wypełniającą podczas badania,
- brak możliwości weryfikacji autentyczności osób wypełniających ankietę.

Audyt analityczny

Kwestionariusz audytowy

Kwestionariusz audytu w zakresie oceny bezpieczeństwa informacji	
	Temat zadania audytowego:
	Ocena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych w kontekście zmieniającego się otoczenia prawnego
Nr zadania:	AW-BST.1720.33.2018

1. Część A - Dane o jednostce

1.1 Pełna nazwa jednostki:	
1.2 Skrócona nazwa jednostki:	
1.3 Adres do korespondencji:	
1.4 Adres poczty elektronicznej sekretariatu badanej jednostki:	
1.5 Imię i nazwisko osoby wypełniającej "Kwestionariusz", email i telefon kontaktowy:	
1.6 Stanowisko (funkcja)	Kierownik jednostki / Inspektor Ochrony Danych / Kierownik komórki organizacyjnej / Pracownik wykonujący zadania IT/ Inna osoba

2. Część B – Badanie audytowe

Lp.	Pytanie	Odpowiedź (Słownik)
2.1	Czy jednostka przetwarza zwykle ^{VI} kategorie danych osobowych? <i>(Dawniej nazywane zwykłymi danymi osobowymi - podział przed obowiązkiem stosowania RODO obejmował dane zwykle i wrażliwe)</i>	Tak / Nie
2.2	Czy jednostka przetwarza szczególnie ^{VI} kategorie danych? <i>(Obejmują większość dawnych danych wrażliwych, sensytywnych, prawie cały art. 27 poprzedniej ustawy o ochronie danych osobowych z 1997 roku oraz dodatkowe dane biometryczne i ...)</i>	Tak / Nie
2.3	Czy jednostka przetwarza dane dotyczące wyroków skazujących i czynów zabronionych?	Tak / Nie
2.4	Czy jednostka przetwarza dane dzieci (do 18 roku życia)?	Tak / Nie
2.5	Czy jednostka przetwarza powierzone dane osobowe?	Tak / Nie
2.6	Ile podmiotów powierza dane osobowe jednostce?	[Liczba]
2.7	Ile umów powierzenia danych osobowych z tych jednostek jest obecnie aktywnych?	[Liczba]
2.8	Czy jednostka powierza przetwarzanie danych osobowych poza jednostkę?	Tak / Nie
2.9	Ilu podmiotom jednostka powierza dane osobowe?	[Liczba]
2.10	Ile umów powierzenia danych osobowych jednostki, innym podmiotom jest obecnie aktywnych?	[Liczba]

Audyt analityczny

Uzgodnienie

Ankieta: 2018 RODO V.2 Uzgodnienie informacji o wstępnych wynikach zadania audytowego AW-BST.1720.33.2018
Płacówka: [redacted]
Zapisana dn: 2019-01-28 wypełniający: [redacted] e_mail: [redacted] identyfikator odpowiedzi: [redacted]

Wypełniony formularz należy wydrukować, podpisać przez kierownika jednostki i niezwłocznie przesłać do Biura Audytu Wewnętrznego (00-033 Warszawa ul. Wojciecha Górnego 7).

INFORMACJA O WSTĘPNYCH WYNIKACH AUDYTU ANALITYCZNEGO

Temat audytu analitycznego: Domena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych w kontekście zmieniającego się otoczenia prawnego.

Numer zadania audytowego: AW-BST.1720.33.2018

Jednostka audytowana: [redacted]

Jednostka audytowana - (potwierdzenie nazwy jednostki): [redacted]

PODSUMOWANIE:

Wstępna ocena: Na bazie informacji otrzymanych z jednostki ocenia się badany obszar pozytywnie z zastrzeżeniami, które w wyniku wdrożenia wskazanych rekomendacji powinny usprawnić badany obszar.

Rekomendacja 1:

- 1a) Podjęcie działań w kierunku sporządzenia i zawarcia umów powierzenia danych osobowych zawierających zapisy zgodne z wymogami RODO,
- 1b) Podjęcie działań w kierunku aneksowania istniejących umów powierzenia danych osobowych z uwzględnieniem zapisów wymaganych w RODO.

Audyt analityczny

Uzgodnienie

(1.) Treść pytania ankietowego (2.07)	(2.07) Ile umów powierzenia danych osobowych z tych jednostek jest obecnie aktywnych?
(1.) Udzielona odpowiedź (2.07)	0
(1.) Treść pytania ankietowego (2.08)	(2.08) Czy jednostka powierza przetwarzanie danych osobowych poza jednostką?
(1.) Udzielona odpowiedź (2.08)	TAK
(1.) Treść pytania ankietowego (2.09)	(2.09) Ilu podmiotom jednostka powierza dane osobowe?
(1.) Udzielona odpowiedź (2.09)	5
(1.) Treść pytania ankietowego (2.10)	(2.10) Ile umów powierzenia danych osobowych jednostki, innym podmiotom jest obecnie aktywnych?
(1.) Udzielona odpowiedź (2.10)	1
(1a.) Termin wdrożenia rekomendacji	2019-05-30
(1a.) Uzgodnienie ustalenia i rekomendacji *	Uzgodniono <input type="radio"/>
	Uzgodniono z uwagami <input type="radio"/>
	Nieuzgodniono - proponowany zapis <input checked="" type="radio"/>
(1a.) Proponowany zapis	W formularz wkradł się błąd pisarski - podmioty powierzający 1, a nie 15. Do 30 maja 2019 roku uporządkujemy tą kwestię.

Audyt analityczny

Sprawozdanie

USTALENIE STANU FAKTYCZNEGO:	
Rekomendacja 1.	
(1.) Identyfikowany problem	Nie we wszystkich jednostkach stosuje się umowy powierzenia danych osobowych zgodne z zapisami RODO, Nie we wszystkich jednostkach wpisuje się umowy do CRU.
(1.) Identyfikowane ryzyko	Niezgodność z przepisami, kary finansowe, utrata reputacji
(1.) Adresat rekomendacji	Kierownik audytowanej jednostki w porozumieniu z jednostką nadzorującą.
Rekomendacja 1a. Podjęcie działań w kierunku sporządzenia i zawarcia umów powierzenia danych osobowych zawierających zapisy zgodne z wymogami RODO.	
(1.) Treść pytania ankietowego (2.05)	(2.05) Czy jednostka przetwarza powierzone dane osobowe?
(1.) Udzielona odpowiedź (2.05)	TAK
(1.) Treść pytania ankietowego (2.06)	(2.06) Ile podmiotów powierza dane osobowe jednostce?
(1.) Udzielona odpowiedź (2.06)	15

Audyt analityczny

Sprawozdanie

OSOBA UPOWAŻNIONA PRZEZ KIEROWNIKA JEDNOSTKI DO UZGODNIENIA INFORMACJI O WSTĘPNYCH WYNIKACH AUDYTU ANALITYCZNEGO	
Imię i nazwisko wypełniającego: *	<input type="text"/>
Stanowisko wypełniającego: *	<input type="text"/>
e-mail: *	<input type="text"/>
Telefon kontaktowy:	<input type="text"/>
Imię i nazwisko Kierownika jednostki:	<input type="text"/>
Data uzgodnienia treści informacji wstępnej z Kierownikiem jednostki:	(rrrr-mm-dd) <input type="text" value="2019-03-07"/>
Potwierdzam odczytanie Sprawozdania z audytu analitycznego 2018	
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
Podpis i pieczęć Kierownika jednostki	<input type="text"/>

Audyt analityczny przeprowadzili pracownicy Biura Audytu Wewnętrznego Urzędu m. st. Warszawy

Audyt analityczny

Informacja zbiorcza



URZĄD MIASTA STOŁECZNEGO WARSZAWY
Biuro Audytu Wewnętrznego

ul. Wojciecha Górskiego 7, 00-033 Warszawa, tel. 22 443 30 70, 22 443 30 71, faks 22 443 30 72
Sekretariat.BAW@um.warszawa.pl, www.um.warszawa.pl

AW-BST.1720.33.2018

Informacja zbiorcza z audytu analitycznego

pn.: „Ocena bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych
w kontekście zmieniającego się otoczenia prawnego”

zrealizowanego w 1005 jednostkach organizacyjnych m.st. Warszawy

Przez użyte skróty należy rozumieć:

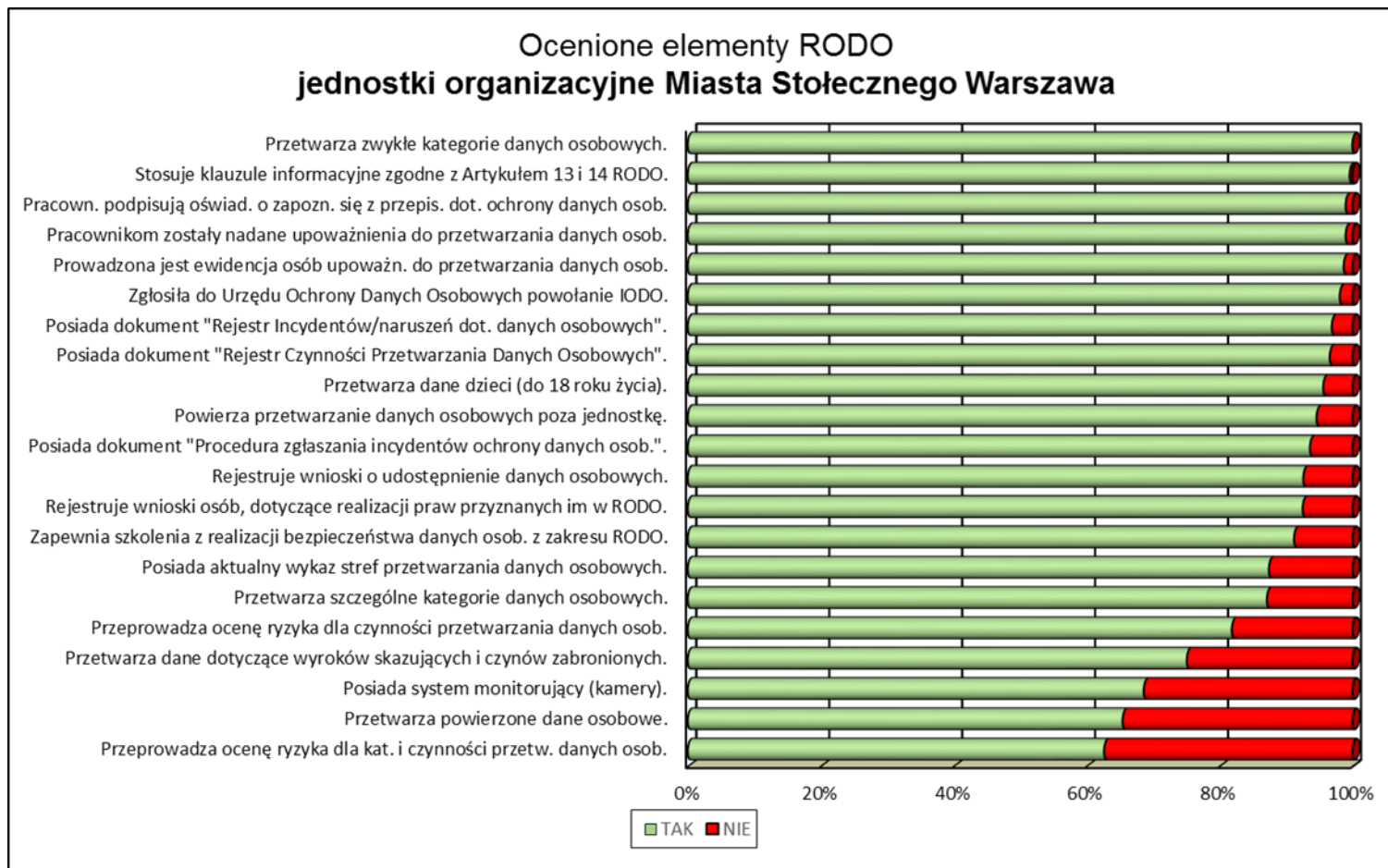
1. Rozporządzenie RODO, potocznie RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., ~~poz.~~ 1000 ze zm.)
3. IOD - Inspektor Ochrony Danych
4. UODO - Urząd Ochrony Danych Osobowych
5. CRU - Centralny Rejestr Umów
6. RCP - Rejestr Czynności Przetwarzania
7. RKCP - Rejestr Kategorii Czynności Przetwarzania

Liczba stron: 18

Warszawa, dnia ... marca 2019 r.

Audyt analityczny

Informacja zbiorcza



Audyt analityczny

Informacja zbiorcza

Nazwa Obszaru	Liczba audytowanych jednostek	Liczba rekomendacji nr:												
		1 a)	1 b)	2 a)	2 b)	2 c)	2 d)	2 e)	3 a)	3 b)	4 a)	4 b)	5	6
Edukacja	804	101	43	11	24	43	22	36	4	7	133	151	70	11
Kultura	70	8	3	1	4	7	3	7	3	7	18	15	8	1
Pomoc Społeczna	66	13	3	0	1	5	3	5	1	2	11	15	8	2
Sport i Rekreacja	18	1	1	0	2	3	0	2	1	1	3	2	3	1
Ochrona Zdrowia	17	2	0	0	0	2	0	1	1	0	0	1	1	0
Gospodarowanie Nieruchomościami Miasta	14	1	0	0	1	1	0	1	0	0	1	1	2	1
Aktywność Obywatelska	1	0	0	0	0	0	0	0	0	0	1	1	0	0
Architektura i Urbanistyka	1	0	0	0	0	0	0	0	0	0	1	0	0	0
Bezpieczeństwo i Porządek Publiczny	1	1	1	0	0	0	0	0	0	0	0	0	0	0
Finanse Publiczne	2	0	0	0	0	0	0	0	0	0	0	0	0	0
Funkcjonowanie Organów Władzy	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Gospodarowanie Środowiskiem	4	0	0	0	0	0	0	0	0	0	0	0	0	0
Transport, Komunikacja i Drogownictwo	3	0	0	0	0	0	0	0	0	0	1	1	0	0
Usługi Komunalne	3	1	0	0	0	0	0	0	0	0	0	1	0	0
Razem:	1005	128	51	12	32	61	28	52	10	17	169	188	92	16

Audyt zapewniający i analityczny

Korzyści z połączenia audytu zapewniającego i analitycznego

- Audyt analityczny to możliwość wykorzystania analizy do przeglądu wstępnego do audytu zapewniającego
- Ocena obszaru na podstawie licznej populacji jednostek audytowanych
- Analiza trendu zmian w poszczególnych obszarach
- Upowszechnienie wiedzy o wymaganiach względem KRI i RODO
- Zwiększenie wiarygodności informacji przekazywanych przez audytowanych w kwestionariuszach z audytu analitycznego
- Obniżenie kosztów audytu
- Podejście systemowe do procesów bezpieczeństwa informacji u audytowanych

Dziękujemy

Prelegenci z Biura Audytu Wewnętrznego Urzędu m.st. Warszawy:

Dorota Rytel-Wyrzykowska (drytel@um.warszawa.pl)

Mariusz Urban (mariusz.urban@um.warszawa.pl)