From: [redacted]
Sent: Thursday, November 11, 2021 11:05 AM
Subject: WNIOSEK KRIO I REALIZACJE ZADAŃ IOD W UG STRZELCE KRAJENSKIE I JEDNOSTKACH ORGANIZACYJNYCH

INFORMACJA PUBLICZNA?

Czy został wykonany coroczny audyt z Krajowych Ram Interoperacyjności? Czy Inspektor Ochrony Danych wykonał audyty? Jeśli nie to za co jest wypłacane wynagrodzenie dla IOD?

Przepis § 20 *rozporządzenia w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[1][1], zwanego dalej *rozporządzeniem*, określa ciążące na kierownictwie podmiotu publicznego obowiązki związane z systemem zarządzania bezpieczeństwem informacji. Jednym z nich jest wskazany w § 20 ust. 2 pkt 14 *rozporządzenia* obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

Kto kontroluje IOD? Czy jego praca poddawana jest kontroli zewnętrznego audytora?

Czy radni kontrolują umowy zawarte z IOD?

Prosimy o dane radnych

Czy dokumenty uzupełniane przez iod czy obowiązuje stara zasada : przesyłamy wzory a Ty radź sobie sam?

Czy był u Państwa przeprowadzony audyt KRIO? Kiedy, data, raport, sprawozdanie, kto przeprowadzał?

Prezes UODO w decyzji z 10 września 2019 r. (ZSPR.421.2.2019) wyjątkowo mocno podkreśla:

„kontrola dostępu i uwierzytelnianie to podstawowe środki bezpieczeństwa mające na celu ochronę przed nieautoryzowanym dostępem do systemu informatycznego wykorzystywanego do przetwarzania danych osobowych. Zapewnienie dostępu uprawnionym użytkownikom i zapobieganie nieuprawnionemu dostępowi do systemów i usług to jeden z wzorcowych elementów bezpieczeństwa".

Czy IOD zewnętrzny podjął działania realne w tym celu czy tylko opracował dokumenty, a realizację pozostawił innym osobom czy też faktycznie dokonał ich realizacji. Zgodnie ze stanowiskiem UODO za realne działania w zakresie bezpieczeństwa odpowiada także IOD.

Jakie realne, a nie teoretyczne działania IOD podjął w celu **wdrożenia dostępu do sieci i usług sieciowych**, w tym sposób autoryzacji użytkowników w sieci i środki wykorzystywane do realizacji dostępu do sieci (np. używanie VPN lub sieci bezprzewodowych), oraz uregulować sposób monitorowania korzystania z usług sieciowych (pkt 9.1.2 PN-EN ISO/IEC 27002).

Czy IOD nie zapomniał o konieczności zmiany domyślnych danych logowania w wykorzystywanych systemach i narzędziach (pkt 9.1.4 PN-EN ISO/IEC 27002; pkt 2.8 i 2.19 OWASP).

Czy IOD **kontroluje użycie programów narzędziowych** umożliwiających obejście zabezpieczeń systemów i aplikacji, m.in. ograniczyć możliwość instalacji takich narzędzi przez użytkowników (pkt 9.4.4 PN-EN ISO/IEC 27002).

Czy IOD kontroluje **dostęp do kodów źródłowych programów oraz związanych z nimi elementów**, takich jak projekty, specyfikacje, plany weryfikacji i badania poprawności (pkt 9.4.5 PN-EN ISO/IEC 27002).

Jakie działanie podjął IOD w celu **zadbania, aby systemy i aplikacje nie były podatne na ataki** SQL Injection, RFI, LFI, XML Injection, XML External Enity, XPath query, XSS, HTTP Parametr Pollution (pkt 5.10, 5.13, 5.14 i 5.15 OWASP).

Preambuła Wniosku:

Najwyższa Izba Kontroli w protokole pokontrolnym nr kap-4101-002-00/2014 - " (...) negatywnie ocenia działania burmistrzów i prezydentów, DYREKTORÓW , KIEROWNIKÓW w zakresie zarządzania bezpieczeństwem informacji w urzędach, o którym mowa w § 20 rozporządzenia KRI. NIK stwierdziła nieprawidłowości w tym obszarze w 21 z 24 (87,5%) skontrolowanych urzędów miast, z których sześć oceniła negatywnie. (...)"

Zadaniami KRIO zajmuje się IOD. Niedopuszczalną praktyką jest sytuacja, że IOD zleca wszystkie zadania ASI!. Czy IOD uczestniczy w prachac?

Lp.	*Zagadnienie*	*Tak*	*Nie*	*Uwagi*
Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.				
1.	Czy prowadzona jest ewidencja:			
	a) sprzętu informatycznego w ramach ewidencji majątkowej?CZY IOD KONTROLUJĘ EWIDENCJĘ			
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ			
	c) umów serwisowych?			
2.	Czy przypisano konkretnym osobom obowiązki w zakresie prowadzenia			

	powyższych ewidencji - w tym oprogramowania i nośników oprogramowania? *Jeśli TAK proszę o przedłożenie dokumentu.* *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
3.	Czy posiadam zinwentaryzowany sprzęt / oprogramowanie wraz z określeniem ważności danego komponentu dla całej jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
4.	Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych? IOD KONTROLUJĘ EWIDENCJĘ			
5.	Czy pracownicy mogą podłączać swój sprzęt (laptopy, telefony, tablety) do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
6.	Czy zapisuję każdy fakt podłączenia zewnętrznego sprzętu do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
7.	Czy monitoruję podłączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.				
1.	Czy znam najistotniejsze zagrożenia dla zinwentaryzowanych systemów IT? *Jeśli TAK proszę o ich wskazanie.*			
2.	Czy wiem, które systemy są krytyczne dla działania jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
3.	Czy mam pewność, że każdy krytyczny system jestem w stanie odtworzyć z kopii zapasowych w odpowiednim czasie? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			

4.	Czy mam opracowane plany działania w momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)?			
5.	Czy znam potencjalne zagrożenia dla systemów, które znajdują się w mojej infrastrukturze lub w infrastrukturze zewnętrznej (outsourcing)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
Podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji wraz z bezzwłoczną zmianą uprawnień, w przypadku zmiany zadań.				
1.	Czy wskazana/e jest/są w jednostce osoba/y odpowiedzialna/e za bezpieczeństwo IT w jednostce? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W* *Jeśli TAK proszę o przedłożenie dokumentu.*			
2.	Czy osoby te posiadają stosowne kompetencje? *Jeśli TAK proszę o potwierdzenie tego faktu.*			
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?			
4.	Czy uprawnienia, o których mowa w pkt 3 uprawniają jedynie do przetwarzania informacji w stopniu adekwatnym do realizowanych zadań? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?			
6.	Czy na bieżąco aktualizowane są uprawnienia do dostępu (np. w momencie zmiany zakresu obowiązków)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
7.	Czy prowadzona jest formalna listę zadań /obowiązków /uprawnień takich osób? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.				
	Należy zaznaczyć stosowane w jednostce rozwiązania.			

1.	Bieżące czynności monitorowania dostępu w tym logi (serwery, systemy, urządzenia sieciowe).			
2.	Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:			
a.	ochrona sieci na poziomie portów LAN			
b.	BIOS			
c.	centralny system kontroli dostępu logicznego do pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows			
d.	niezależne od domenowych systemy kontroli dostępu logicznego do kluczowych systemów informatycznych; *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
e.	system ochrony zewnętrznej klasy firewall			
f.	system ochrony zewnętrznego dostępu logicznego (urządzanie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;			
g.	stosowanie tokenów z hasłami jednorazowymi			
Podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE PRACĘ NA ODLEGŁOŚĆ CZY TYLKO PRZEDSTAWIA DOKUMENTY*				
1.	Czy wprowadzono regulacje wewnętrzne jednostki w zakresie zdalnego dostępu do zasobów informatycznych/pracy na odległość? *Jeśli TAK proszę o przedłożenie dokumentu.*			
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT? *Jeśli TAK proszę o udokumentowanie.*			
3.	Czy w pracy na odległość stosuję bezpieczne metody połączenia?			
4.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?			
5.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, są chronione przed utratą danych (np. w wyniku kradzieży)? *Jeśli TAK proszę wskazać, w jaki sposób.*			
Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*				
1.	Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w			

	umowach zawieranych z dostawcami sprzętu/ oprogramowania? *Jeśli TAK proszę o udokumentowanie.*			
2.	Czy posiadam krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości wgrania aktualizacji komponentów, na których bazuje dany system)?			
Zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. CZY IOD PRZEPROWADZIŁ ANALIZĘ RYZYKA I OCENĘ SKUTKÓW DLA PRZETWARZANIA DANYCH W URZĄDZENIACH MOBILNYCH?*				
1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? *Jeśli TAK proszę o przedłożenie.*			
2.	Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?			
3.	Czy istniej możliwość zdalnego, trwałego usunięcia danych z tego typu urządzenia?			
4.	Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?			
5.	Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?			
6.	Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?			
Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. ANALIZA RYZYKA W/W*				
1.	Czy realizuję bieżące aktualizacje zarówno na stacjach PC (system operacyjny / java / adobe reader / flash itp.), jak i serwerach?			
2.	Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?			
3.	Czy posiadam aktualne sygnatury dla systemu antywirusowego?			
4.	Czy mam przygotowaną procedurę odtworzenia danej stacji roboczej / serwera po wykryciu na nim wirusa?			
5.	Czy mam informacje o systemach, dla których aktualizacja nie powiodła się?			
6.	Czy wiem, które systemy IT są krytyczne dla prawidłowego działania jednostki?			
7.	Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?			
8.	Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za			

	pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?			
9.	Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?			
10.	Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?			
11	Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?			
12.	Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?			
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?			
14.	Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)			
Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.				
1.	Czy istnieją w jednostce procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?			
2.	Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?			

[redacted]

URZĄD MIASTA
GORZOWA WIELKOPOLSKIEGO

Urząd Miasta
ul. Sikorskiego 3-4
66-400 Gorzów Wlkp.

T: +48 95 735 55 00
F: +48 95 735 56 70
E: kancelaria@um.gorzow.pl
I: www.gorzow.pl

Gorzów Wielkopolski, dnia 10.12.2021 r.

WOR - III.1431.288.2021.KPa

[redacted]

Odpowiadając na złożony w dniu 11 listopada 2021 r. wniosek o udostępnienie informacji publicznej, poniżej przekazuję odpowiedzi na zadane pytania.

Czy został wykonany coroczny audyt z Krajowych Ram Interoperacyjności?

Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność poprzez miedzy innymi okresowe, czyli powtarzające się audyty wewnętrzne, realizowane nie rzadziej niż raz na rok.

Audyt za 2021 rok, o którym mowa powyżej zaplanowany jest do przeprowadzenia w pierwszych miesiącach 2022 roku.

Czy Inspektor Ochrony Danych wykonał audyty? Jeśli nie to za co jest wypłacane wynagrodzenie dla IOD?

Inspektor Ochrony Danych **nie jest Administratorem Bezpieczeństwa Informacji** – w zakresie jego obowiązków jest ochrona danych osobowych o których mowa w RODO. Przepisy określające wymóg związany z zapewnieniem okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji (wynikający z KRI) **nie wskazują konkretnych osób, które mogą wykonać audyt z KRI**.

W urzędzie sprawdzają się w roli audytora z tego zakresu nie tylko inspektor ochrony danych ale również administrator systemów informatycznych czy pracownicy Wydziału audytu wewnętrznego, kontroli i analiz (z tej komórki wewnętrznej administrator również korzysta).

Kto kontroluje IOD? Czy jego praca poddawana jest kontroli zewnętrznego audytora?

Inspektor ochrony danych podlega bezpośrednio administratorowi i w związku z tym sposób wykonywania funkcji przez IOD podlega jego kontroli.

Praca Inspektora ochrony danych nie była poddawana kontroli zewnętrznego audytora.

Czy radni kontrolują umowy zawarte z IOD? Prosimy o dane radnych.

Radni nie kontrolują umów zawartych z IOD.

Dane radnych obecnej kadencji znajdują się w Biuletynie Informacji Publicznej Urzędu Miasta Gorzowa Wielkopolskiego pod adresem:

https://bip.wrota.lubuskie.pl/umgorzow/90/Sklad_Rady_Miasta/

Czy dokumenty uzupełniane przez IOD czy obowiązuje stara zasada: przesyłamy wzory a Ty radź sobie sam?

Pytanie postawione nieprecyzyjnie, nie wiadomo, o co konkretnie chodzi.

Czy IOD zewnętrzny podjął działania realne w tym celu czy tylko opracował dokumenty, a realizację pozostawił innym osobom czy też faktycznie dokonał ich realizacji. Zgodnie ze stanowiskiem UODO za realne działania w zakresie bezpieczeństwa odpowiada także IOD.

Urząd nie korzysta z usług zewnętrznego IOD.

Jakie realne, a nie teoretyczne działania IOD podjął w celu ***wdrożenia dostępu do sieci i usług sieciowych****, w tym sposób autoryzacji użytkowników w sieci i środki wykorzystywane do realizacji dostępu do sieci (np. używanie VPN lub sieci bezprzewodowych), oraz uregulować sposób monitorowania korzystania z usług sieciowych (pkt 9.1.2 PN-EN ISO/IEC 27002).*

Najbliższe kontrole z zakresu bezpieczeństwa systemów zaplanowane są w okresie grudzień / styczeń.

Czy IOD nie zapomniał o konieczności zmiany domyślnych danych logowania w wykorzystywanych systemach i narzędziach (pkt 9.1.4 PN-EN ISO/IEC 27002; pkt 2.8 i 2.19 OWASP).

Najbliższe kontrole z zakresu bezpieczeństwa systemów zaplanowane są w okresie grudzień / styczeń.

Czy IOD ***kontroluje użycie programów narzędziowych*** *umożliwiających obejście zabezpieczeń systemów i aplikacji, m.in. ograniczyć możliwość instalacji takich narzędzi przez użytkowników (pkt 9.4.4 PN-EN ISO/IEC 27002).*

Najbliższe kontrole z zakresu bezpieczeństwa systemów zaplanowane są w okresie grudzień / styczeń.

Czy IOD kontroluje ***dostęp do kodów źródłowych programów oraz związanych z nimi elementów****, takich jak projekty, specyfikacje, plany weryfikacji i badania poprawności (pkt 9.4.5 PN-EN ISO/IEC 27002).*

Najbliższe kontrole z zakresu bezpieczeństwa systemów zaplanowane są w okresie grudzień / styczeń.

Jakie działanie podjął IOD w celu ***zadbania, aby systemy i aplikacje nie były podatne na ataki*** *SQL Injection, RFI, LFI, XML Injection, XML External Enity, XPath query, XSS, HTTP Parametr Pollution (pkt 5.10, 5.13, 5.14 i 5.15 OWASP).*

Najbliższe kontrole z zakresu bezpieczeństwa systemów zaplanowane są w okresie grudzień / styczeń.

Zadaniami KRIO zajmuje się IOD. Niedopuszczalną praktyką jest sytuacja, że IOD zleca wszystkie zadania ASI! Czy IOD uczestniczy w pracach?

W urzędzie w realizacji zadań wynikających z rozporządzenia z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych współuczestniczą w swoim zakresie Administrator Systemu Informatycznego, którym jest *Dyrektor Wydziału Zarządzania Systemami Informatycznymi,* jak również Inspektor Ochrony Danych.

Lp.	*Zagadnienie*	*Tak*	*Nie*	*Uwagi*
Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.				
1.	Czy prowadzona jest ewidencja:			
	a) sprzętu informatycznego w ramach ewidencji majątkowej? CZY IOD KONTROLUJĘ EWIDENCJĘ	X		Kontrola planowana w okresie grudzień / styczeń
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ	X		Kontrola planowana w okresie grudzień / styczeń
	c) umów serwisowych?	X		
2.	Czy przypisano konkretnym osobom obowiązki w zakresie prowadzenia powyższych ewidencji - w tym oprogramowania i nośników oprogramowania? *Jeśli TAK proszę o przedłożenie dokumentu. CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		X	Kontrola planowana w okresie grudzień / styczeń
3.	Czy posiadam zinwentaryzowany sprzęt / oprogramowanie wraz z określeniem ważności danego komponentu dla całej jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		Kontrola planowana w okresie grudzień / styczeń
4.	Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych? IOD KONTROLUJĘ EWIDENCJĘ		X	
5.	Czy pracownicy mogą podłączać swój sprzęt (laptopy, telefony, tablety) do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		X	Kontrola planowana w okresie grudzień / styczeń

6.	Czy zapisuję każdy fakt podłączenia zewnętrznego sprzętu do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		Kontrola planowana w okresie grudzień / styczeń
7.	Czy monitoruję podłączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		Kontrola planowana w okresie grudzień / styczeń
Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.				
1.	Czy znam najistotniejsze zagrożenia dla zinwentaryzowanych systemów IT? *Jeśli TAK proszę o ich wskazanie.*	X		W ocenie odpowiadającego niedopuszczalne jest wskazywanie podmiotom zagrożeń i podatności systemów IT.
2.	Czy wiem, które systemy są krytyczne dla działania jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		Kontrola planowana w okresie grudzień / styczeń
3.	Czy mam pewność, że każdy krytyczny system jestem w stanie odtworzyć z kopii zapasowych w odpowiednim czasie? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		Kontrola planowana w okresie grudzień / styczeń
4.	Czy mam opracowane plany działania w momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)?	X		
5.	Czy znam potencjalne zagrożenia dla systemów, które znajdują się w mojej infrastrukturze lub w infrastrukturze zewnętrznej (outsourcing)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		Kontrola planowana w okresie grudzień / styczeń
Podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji wraz z bezzwłoczną zmianą uprawnień, w przypadku zmiany zadań.				
1.	Czy wskazana/e jest/są w jednostce osoba/y odpowiedzialna/e za bezpieczeństwo IT w jednostce? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W* *Jeśli TAK proszę o przedłożenie dokumentu.*	X		Kontrola planowana w okresie grudzień / styczeń
2.	Czy osoby te posiadają stosowne kompetencje? *Jeśli TAK proszę o potwierdzenie tego faktu.*	X		Zatrudniane są wyłącznie osoby posiadające niezbędne kwalifikacje
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?	X		
4.	Czy uprawnienia, o których mowa w pkt 3 uprawniają jedynie do przetwarzania informacji w stopniu	X		Kontrola planowana w okresie grudzień / styczeń

	adekwatnym do realizowanych zadań? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*			
5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?	X		
6.	Czy na bieżąco aktualizowane są uprawnienia do dostępu (np. w momencie zmiany zakresu obowiązków)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		Kontrola planowana w okresie grudzień / styczeń
7.	Czy prowadzona jest formalna listę zadań /obowiązków /uprawnień takich osób? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		X	
Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami.				
	Należy zaznaczyć stosowane w jednostce rozwiązania.			
1.	Bieżące czynności monitorowania dostępu w tym logi (serwery, systemy, urządzenia sieciowe).	X		
2.	Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:	X		
a.	ochrona sieci na poziomie portów LAN	X		
b.	BIOS	X		
c.	centralny system kontroli dostępu logicznego do pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows	X		
d.	niezależne od domenowych systemy kontroli dostępu logicznego do kluczowych systemów informatycznych; *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		Kontrola planowana w okresie grudzień / styczeń
e.	system ochrony zewnętrznej klasy firewall	X		
f.	system ochrony zewnętrznego dostępu logicznego (urządzanie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;	X		
g.	stosowanie tokenów z hasłami jednorazowymi		X	
Podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE PRACĘ NA ODLEGŁOŚĆ CZY TYLKO PRZEDSTAWIA DOKUMENTY*				
1.	Czy wprowadzono regulacje wewnętrzne jednostki w zakresie zdalnego dostępu do zasobów informatycznych/pracy na odległość? *Jeśli TAK proszę o przedłożenie dokumentu.*	X		Polityka ochrony danych osobowych rozdział VII, Część II § 13
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT? *Jeśli TAK proszę o udokumentowanie.*	X		Dostęp jest włączany doraźnie, wyłącznie na czas prowadzenia prac
3.	Czy w pracy na odległość stosuję bezpieczne metody połączenia?	X		vpn
4.	Czy systemy (np. laptopy), które mają zdalny dostęp do	X		

	infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?			
5.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, są chronione przed utratą danych (np. w wyniku kradzieży)? *Jeśli TAK proszę wskazać, w jaki sposób.*	X		Szyfrowanie dysku, hasła
Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*				
1.	Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w umowach zawieranych z dostawcami sprzętu/ oprogramowania? *Jeśli TAK proszę o udokumentowanie.*	X		Polityka ochrony danych osobowych rozdział, VII § 16. Każda umowa zawiera zastrzeżenie dotyczące przetwarzanie danych osobowych.
2.	Czy posiadam krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości wgrania aktualizacji komponentów, na których bazuje dany system)?		X	
Zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. CZY IOD PRZEPROWADZIŁ ANALIZĘ RYZYKA I OCENĘ SKUTKÓW DLA PRZETWARZANIA DANYCH W URZĄDZENIACH MOBILNYCH?*				
1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? *Jeśli TAK proszę o przedłożenie.*		X	Polityka ochrony danych osobowych Część II rozdział VII § 18, 19. Dostęp do niezarejestrowanych nośników przenośnych jest zablokowany.
2.	Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?	X		
3.	Czy istniej możliwość zdalnego, trwałego usunięcia danych z tego typu urządzenia?	X		
4.	Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?		X	
5.	Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?			
6.	Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?		X	
Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. ANALIZA RYZYKA W/W*				
1.	Czy realizuję bieżące aktualizacje zarówno na stacjach PC (system operacyjny / java / adobe reader / flash itp.), jak i serwerach?	X		
2.	Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?	X		
3.	Czy posiadam aktualne sygnatury dla systemu antywirusowego?	X		
4.	Czy mam przygotowaną procedurę odtworzenia danej	X		

	stacji roboczej / serwera po wykryciu na nim wirusa?			
5.	Czy mam informacje o systemach, dla których aktualizacja nie powiodła się?	X		
6.	Czy wiem, które systemy IT są krytyczne dla prawidłowego działania jednostki?	X		
7.	Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?	X		
8.	Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?		X	
9.	Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?	X		
10.	Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?	X		
11	Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?	X		
12.	Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?	X		
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?	X		
14.	Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)	X		
Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.				
1.	Czy istnieją w jednostce procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?	X		
2.	Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?	X		

z up. PREZYDENTA MIASTA

Eugeniusz Kurzawski

Sekretarz Miasta