Infrastruktura IT, cyberbezpieczeństwo, oprogramowanie - najlepsze praktyki. Jakie są największe zagrożenia cyberbezpieczeństwa i jak im zapobiegać? Co warto wdrażać, w jakiej kolejności, co jest przereklamowane? Czy oprogramowanie i sprzęt bez wsparcia producenta należy natychmiast wycofać? Czy chmura w urzędzie to dobry pomysł, czy są przeszkody prawne? Czy da się tak zabezpieczyć system, aby użytkownicy nie musieli się przejmować cyberbezpieczeństwem?

Wideoszkolenie PCC Poland jest przeznaczone dla pracowników wydziałów informatyki w urzędach miast i gmin, którzy odpowiadają za obszary takie jak wdrażanie zabezpieczeń, backup danych i systemów, administrowanie serwerami, konfigurację i ochronę sieci, zarządzanie ewidencją użytkowników i sprzętu komputerowego oraz licencjami.

Co wprowadzi nowelizacja dyrektywy NIS2 i jak przygotować się na nadchodzące zmiany?

Podczas szkolenia, wykorzystując horyzontalne spojrzenie, praktyk wyjaśni w jaki sposób osiągnąć optymalne współdziałanie obszarów merytorycznych z obszarem informatyki w kontekście urzędów miast i gmin oraz jednostek samorządu terytorialnego. Szkolenie wyjaśni wpływ dyrektywy NIS2 oraz objaśni sposób przygotowania się do nadchodzących zmian. Uczestnicy nauczą się, jak wybrać i stosować narzędzia oraz oprogramowanie w celu zwiększenia bezpieczeństwa sieci oraz dowiedzą, jak zapewnić ciągłość działania systemów informatycznych. Dowiedzą się również jak działać prewencyjnie, aby zapobiec wyciekowi, utracie lub zaszyfrowaniu danych dla okupu. Ekspert omówi tematy związane z zarządzaniem licencjami oprogramowania, jak zapewnić legalność, prowadzić ewidencje oraz wybierać, tak aby były korzystne cenowo i dopasowane do potrzeb, zarówno w dużych, jak i mniejszych jednostkach sektora finansów publicznych.

W programie m.in.:

- Co zapisać w polityce bezpieczeństwa informacji, aby wykorzystać możliwości zabezpieczeń technicznych np. UTM?
- Jakie są obowiązki informatyka we wdrażaniu cyberbezpieczeczeństwa?
- Jak zarządzać licencjami oprogramowania, aby być legalnym i efektywnym kosztowo?
- Co trzeba zrobić, żeby stworzyć solidną konstrukcję sieci informatycznej w urzędzie?
- Coraz częściej urzędy odchodzą od swoich serwerów, kupują usługi w chmurze. Jak wygląda kwestia bezpieczeństwa takich usług?
- Urząd to nie firma zarobkowa, nie należy do obszaru biznesowego, więc nie wiadomo czy można podciągnąć tę jednostkę do grupy komercyjnej, czy w takim przypadku należy kupić licencję do konkretnych programów Open Source?
- Licencje Microsoft są niejasne, jak licencjonować pod produkty i wersje?

Szczegółowy program szkolenia:

1. Bezpieczeństwo w urzędzie – Jaki wpływ na funkcjonowanie urzędu miasta/gminy będzie

miało wprowadzenie dyrektywy NIS2? Dlaczego korzystając z publicznych chmur warto zastanowić się nad bezpieczeństwem dla urzędu?

- Czy stosowanie się wyłącznie do zasad określonych w KRI jest wystarczające, żeby zabezpieczyć urząd?
- Każdy urząd indywidualnie interpretuje zasady bezpieczeństwa i KRI. Jakie są dobre praktyki w zabezpieczeniu urzędu?
- Czy wejście regulacji o możliwości poddaniu dostawców sprzętu i oprogramowania procedurze sprawdzającej pod kątem zagrożenia, zminimalizuje niebezpieczeństwo w urzędach? Dlaczego?
- Co trzeba zrobić, żeby stworzyć solidną konstrukcję sieci informatycznej w urzędzie?
- Jakich narzędzi i jakiego oprogramowania użyć do udoskonalenia systemu pod kątem bezpieczeństwa?
- Czy zastosowanie UTM jest konieczne w urzędzie? Dlaczego?
- Czy warto korzystać z outsourcingu, jeżeli chodzi o zarządzanie siecią i systemami? Dlaczego? Jakie są wady i zalety?
- Jakie są wady korzystania z chmury w urzędzie? Do jakich niebezpiecznych sytuacji może dojść, jaką kontrolę nad danymi ma informatyk, jeśli korzysta z publicznej chmury?
- Jak zarządzać maszynami wirtualnymi w chmurze i jakie to niesie zagrożenia?
- Jak odzyskać dane z chmury w przypadku utracenia danych/zaszyfrowania?
- Sposoby reakcji na włam - jak się zachować, gdy dochodzi do incydentu? Czy należy wyłączać serwery?
- Czy są urządzenia, na których można zrezygnować ze wsparcia producenta, jeżeli jest to wymagające finansowo?
- Do jakiego momentu jest wsparcie producenta? Czy po pewnym czasie wsparcie wygasa?
- Jakie korzyści płyną z posiadania sprzętu ze wsparciem technicznym? Dlaczego to jest ważne (szczególnie chodzi o sprzęt wrażliwy, np. serwery)?
- Wykorzystywanie prywatnego sprzętu (laptopów, komputerów stacjonarnych) do wykonywania obowiązków i procedur urzędu - czy jest to w ogóle możliwe? Czy istnieje jakieś ryzyko?
- Dlaczego korzystanie z oprogramowania antywirusowego z maksymalnymi możliwościami bezpieczeństwa jest ważne?
- Czy urząd jako instytucja publiczna ma obowiązek posiadania antywirusa?
- Czy wbudowane zabezpieczenia Windows'a są wystarczające dla urzędu?
- Antywirus komercyjny a wbudowane zabezpieczenia Windows, jakie są różnice, wady i zalety?
- Jak efektywnie zarządzać zabezpieczeniami Windows'a, wiedząc, że to jest tak obszerna architektura?
- Jak wykorzystać VPN'a w urzędzie? Jakie korzyści z tego płyną?
- Jakie korzyści płyną z korzystania z routera z firewallem z technologią UTM?
- Dlaczego należy zadbać o wymianę oprogramowania systemu, jeżeli korzysta się z wersji bez wsparcia technicznego? Jaki wpływ to ma na bezpieczeństwo? Łatanie luk?
- Czy instalowanie oprogramowania przez urzędników jest możliwe? Czy istnieje jakieś ryzyko?
- Kto jest odpowiedzialny za ustalenie, czy dane oprogramowanie jest zdatne do zainstalowania na systemach urzędowych?

2. Dostępy i uprawnienia nadawane pracownikom urzędu miasta/gminy. Na jakiej zasadzie ograniczać dostęp do konkretnych stron?

- Jak informatyk w urzędzie może zabezpieczyć się przed odpowiedzialnością za niezgodnie/nielegalnie zainstalowane oprogramowanie?

- Jak przebiega analiza oprogramowania pod kątem wirusów i niebezpieczeństw? Na co należy zwrócić uwagę?
- Kto jest odpowiedzialny za aktualizację systemów i oprogramowania?
- Jakie korzyści płyną z limitowania dostępu do poszczególnych stron urzędnikom?
- W jaki sposób ograniczać dostęp do konkretnych stron?
- Kto ustala, jakie witryny są dostępne dla urzędników?
- Jakie są korzyści z używania narzędzi, które uniemożliwiają zamieszczania konkretnych treści, np. w wiadomościach email?
- Jak nadawane są dostępy i uprawnienia? Kto je nadaje?
- Kto jest osobą decyzyjną przy wydawaniu dostępu i uprawnień w systemach?
- Kto jest odpowiedzialny za monitorowanie dostępów? Czy jest taki obowiązek?
- Jak często należy sprawdzać, czy odpowiednie osoby posiadają uprawnienia? Z jaką częstotliwością robić czystki?
- Jakie są narzędzia wspierające bieżące analizowanie incydentów?
- Jak zapanować nad tym co jest zainstalowane na danym urządzeniu i kto za to odpowiada w przypadku dużej liczby maszyn?
- Jakie są dostępne narzędzia do ustalania polityki druków oraz ograniczania wstawiania konkretnych treści?
- Jakie korzyści płyną z wykorzystania systemów DLP?
- Kiedy i jakie urządzenia podlegają procesowi szyfrowania dysków?
- Czy każdy sprzęt mobilny, wynoszony poza urząd, musi być zaszyfrowany? Jakie są na to sposoby?
- Jakie narzędzia do szyfrowania dysków są efektywne?
- Jakimi sposobami zadbać o bezpieczeństwo danych na urządzeniach przenośnych?
- Dlaczego warto zainwestować w oprogramowanie do szyfrowania dysków, niż korzystanie z darmowych alternatyw?
- Oprogramowanie open source a bezpieczeństwo - czy można bezpiecznie z takowego korzystać, jeżeli obracamy danymi wrażliwymi?
- Jak zarządzać systemami w przypadku dużej ilości, np. 100 sztuk komputerów stacjonarnych?
- Dlaczego posiadanie Active Directory w dużym urzędzie to “must-have”? Czy są jakieś alternatywy do AD?

3. Licencje, zarządzanie i ewidencja - Jakie są dostępne narzędzia do prowadzenia ewidencji kluczy i licencji?

- Jak ułatwić zarządzanie licencjami bez korzystania z dedykowanego oprogramowania, jeżeli mamy do czynienia z dużą liczbą licencji?
- Jakie są programy, które sczytują licencje i automatyzują ewidencje?
- Jakie są typy i rodzaje licencji, które są używane w urzędach miast i gmin?
- Jaka jest odpowiedzialność informatyka za zarządzanie licencjami?
- Kto w urzędzie ponosi konsekwencje w razie nieprawidłowości z zakresu licencji?
- Jak poprawnie ewidencjonować licencje?
- Jakie są dostępne narzędzia do prowadzenia ewidencji kluczy i licencji?
- Czy posiadając licencję Windows’a w formie wielokrotnego klucza jest łatwiej zarządzać systemami? W jaki sposób i dlaczego?
- Czy kupowanie licencji Windows w formie wielokrotnego klucza (MAK) jest finansowo opłacalne?
- Jakie narzędzia wspierają inwentaryzację urządzeń?
- Czy cena licencji oprogramowania (np. programu do szyfrowania dysków) przekłada się na jego

jakość?
- Jakie są dostępne rozszerzenia pakietów Microsoft? Jakie wybrać, aby odpowiadały one urzędowi, a nie były wymagające finansowo?
- Czy zakupienie licencji Office w pakiecie jest korzystniejsze niż przypisywanie indywidualnych licencji do poszczególnych urządzeń?
- Czy kupowanie sprzętu (np. laptopów) z już nadanym kluczem produktu jest korzystne finansowo? Czy jest bezpieczne?
- Co w sytuacji, gdy zakupiony sprzęt z nadaną licencją pochodzi z niewiadomego źródła?
- Licencja Office z odzysku, jak to wygląda prawnie?
- Kiedy można przenieść licencję Office na inne urządzenie?
- Którą licencję CAL wybrać? Licencję na użytkownika czy na urządzenie?
- PRZYKŁAD: W urzędzie jest stanowisko 3-zmianowe. 3 osoby korzystają z jednego urządzenia w innym czasie. Czy w takiej sytuacji należy kupić licencję CAL na urządzenie, a nie na użytkowników - kupi się tylko jedną licencję, a nie aż trzy (na każdego użytkownika)? Czy jednak powinna być na każdego użytkownika oddzielna licencja?
- W jakich sytuacjach należy wybrać licencję CAL na urządzenie, a w jakich na użytkownika w przypadku posiadania innego sprzętu niż tylko komputery?
- Licencje Microsoft są niejasne, jak licencjonować pod produkty i wersje?
- Jak wybrać odpowiednie licencje Windows Server? Licencja na liczbę rdzeni, nie gniazd procesora.
- Jak licencjonować produkty Oracle do maszyn ‘tower-owych?
- Urząd to nie firma zarobkowa, nie należy do obszaru biznesowego, więc nie wiadomo, czy można podciągnąć tę jednostkę do grupy komercyjnej, czy w takim przypadku należy kupić licencję do konkretnych programów Open Source?
- Jak, dlaczego i których pracowników urzędu należy edukować na temat licencji i zakresu funkcji, jakie oferują?
- Jakie kroki należy podjąć w sytuacji, gdy informatyk, który był odpowiedzialny za zarządzanie i ewidencję licencji, zmarł i nikt nie ma dostępu do oprogramowania/plików?

4. Czynnik ludzki - najsłabsze ogniwo w organizacji

- Nieważne jak dobrze zabezpieczony jest system, człowiek to najsłabsze ogniwo, w jaki sposób uświadamiać urzędników o zagrożeniach?
- W jaki sposób nauczyć urzędników jak rozróżniać niebezpieczeństwo?
- Jak rozróżniać niebezpieczne e-maile?
- Na jakie sposoby potrafią działać osoby, które chcą stworzyć zagrożenie dla urzędu? Przykłady wadliwych maili.

5. Backup – dlaczego kopia zapasowa jest tak ważna? Jak się zabezpieczyć przed utratą danych?

- Jak często należy tworzyć kopię zapasową indywidualnych maszyn?
- Z jaką częstotliwością powinno się tworzyć kopie zapasowe całych serwerów?
- Dlaczego częstotliwość robienia kopii zapasowych zależy od kontekstu i specyfiki systemu?
- Jak ustalić częstotliwość robienia kopii zapasowych na podstawie wielkości urzędu i ilości przechowywanych danych? Jakie są przesłanki?
- Co jest największym problemem przy tworzeniu kopii zapasowych?
- Jakie są zalety zabezpieczenia dysków w formie napędu taśmowego?
- Wykonywanie kopii zapasowych a ich skuteczność, co robić, żeby mieć pewność, że kopie faktycznie

zostały wykonane?
- Dlaczego warto przeprowadzać testy możliwości odtworzenia kopii? Jak często powinniśmy je stosować?
- Na ile przydatna jest kopia zapasowa w wersji offline? Czy powinno się taką robić?
- Jakie korzyści płyną z posiadania serwera NAS z dyskami w konwencji RAID?

6. Domeny - problematyczne sytuacje

- Co w sytuacji, gdy osoba, na którą była wykupiona domena, odchodzi od organizacji? Jakie kroki podjąć, żeby odzyskać domenę?
- Przykład: Zastępca burmistrza wykupił domenę na siebie, odszedł z pracy. Co zrobić w takiej sytuacji? Jak przeprowadzić cesję na przekazanie domeny na gminę? Czy jest możliwe, żeby domena instytucji państwowej była zakupiona na osobę prywatną, np. domeny zakupione kilkadziesiąt lat temu?
- Jak należy postąpić i jakie kroki podjąć w sytuacji, gdy jest spór z osobą, na którą jest zarejestrowana domena, a nie należy już do organizacji?
- Jakie działania należy podjąć w sytuacji, gdy osoba na którą jest zarejestrowana domena umiera?
- Coraz częściej firmy jak i urzędy odchodzą od swoich serwerów, kupują usługi w chmurze. Jak wygląda kwestia bezpieczeństwa takich usług?
- Który program najlepiej się sprawdza do centralnego zarządzania domeną i użytkownikami?
- Dlaczego warto mieć usługi domenowe i serwerowe w oddzielnych firmach?
- Jakie są zalety kupienia domeny niezależnej, nieprzypisanej do żadnej firmy?

7. Audyt – dlaczego nie należy pomijać audytu zewnętrznego i jakie korzyści płyną z przeprowadzenia takiego audytu? Na co zwracać uwagę przy audycie szerokopasmowym?

- Kto wykonuje audyt wewnętrzny?
- Jak często sprawdzać, czy długości haseł i same hasła użytkowników są poprawne i z jaką częstotliwością zmieniane?
- Czy informatyk ma obowiązek monitorować, kiedy hasła wygasają i czy odświeżanie haseł jest ustawione?
- Z jaką częstotliwością należy przeprowadzać audyt wewnętrzny?
- Jak często powinien się odbywać audyt zewnętrzny, prowadzony przez osoby niezwiązane z urzędem?
- Jakie są różnice pomiędzy audytem wewnętrznym a audytem zewnętrznym?
- Która forma audytu jest dokładniejsza?
- Czy audyt zewnętrzny jest obowiązkowy? Czy są sankcje za uchybienie terminu?
- Jakie są sankcje za nie przeprowadzenie audytu zleconego przez Ministerstwo Cyfryzacji?
- Dlaczego warto robić audyt sprzętu komputerowego? Czy warto zlecić taki audyt firmie zewnętrznej?

8. Praca zdalna w urzędzie

- W jaki sposób informatycy wykonują swoje obowiązki w sytuacji, gdy nie pracują stacjonarnie?
- Z jakich narzędzi korzystają informatycy w przypadku konieczności użycia pulpitu zdalnego?
- Z jakich narzędzi mogą korzystać informatycy, aby nie musieć każdorazowo prosić o dostęp do komputera użytkownika?
- Oprogramowanie płatne a darmowe z obszaru zdalnej kontroli pulpitu, czym się różnią? Czy w przypadku płatnych programów jest więcej dostępnych funkcjonalności?
- Jak przygotować sprzęt dla urzędnika pod kątem bezpieczeństwa w przypadku pracy zdalnej?

- Jak bezpiecznie korzystać ze zdalnych pulpitów?

Prowadzący:

Michał Rabka - posiada **ponad dwudziestoletnie doświadczenie w zakresie cyfryzacji jednostek samorządu terytorialnego**. Obecnie **pełni funkcję Naczelnika Wydziału Informatyki w Urzędzie Miasta Dąbrowa Górnicza**, oraz sprawuje nadzór nad sprawami związanymi z cyberbezpieczeństwem jako Koordynator ds. Cyberbezpieczeństwa. Dodatkowo, działa jako Pełnomocnik Prezydenta Miasta ds. Transformacji Cyfrowej.

Przez pierwszą połowę swojej kariery zawodowej, zdobywał doświadczenie praktyczne na stanowiskach technicznych, administrując infrastrukturą IT, bezpieczeństwem oraz wdrażając oprogramowanie. Przez kolejne 10 lat, jako Naczelnik Wydziału Informatyki, kierował realizacją dużych i złożonych projektów z zakresu budowy sieci szerokopasmowych, centrów przetwarzania danych, wdrażania aplikacji dziedzinowych oraz usług cyfrowych.

Był odpowiedzialny za realizację wielomilionowego projektu, dofinansowanego z funduszy UE, o nazwie "Budowa miejskiej sieci światłowodowej w Zagłębiu Dąbrowskim - Dąbrowa Górnicza". Sieć dostarcza usługi dla 71 jednostek miejskich, jest wyposażona w skuteczny centralny węzeł bezpieczeństwa. Odpowiadał również za projekt Wdrożenia Wspólnej obsługi informatycznej jednostek miejskich oraz wsparcie IT wdrożenia Centrum Usług Wspólnych jednostek oświatowych.

Jako Koordynator ds. cyberbezpieczeństwa od 2019 roku, pełni kluczową rolę w utrzymaniu wysokich standardów bezpieczeństwa w gminie. Posiada wiedzę i umiejętności pozwalające prowadzić audyty cyberbezpieczeństwa. Uczestniczył w opracowaniu oraz wdrożył wypracowane zasady polityki bezpieczeństwa informacji, łącząc aspekty cyberbezpieczeństwa oraz prawne wynikające z przepisów prawa w tym w szczególności z RODO.

Posiada solidne zaplecze teoretyczne. Ukończył Politechnikę Śląską w zakresie sieci komputerowych i baz danych, Szkołę Główną Handlową w Warszawie w zakresie Zarządzania IT, Uniwersytet Ekonomicznym w Katowicach w zakresie Audytu informatycznego oraz Zarządzania Projektami, Politechnikę Warszawską w zakresie Zarządzanie IT w administracji publicznej. Posiada tytuł MBA. Obecnie głównym obszarem zainteresowania są systemy zaawansowanej analizy danych ze szczególnym uwzględnieniem AI oraz praktycznego wykorzystania algorytmów sieci neuronowych.