Jak zabezpieczyć sieć oraz systemy używane w urzędzie gminy i miasta? Jak kontrolować oprogramowanie zainstalowane na komputerach przenośnych wykorzystywanych do pracy zdalnej? Praktyczne wskazówki dotyczące zachowania polityki bezpieczeństwa z wykorzystaniem połączenia VPN

Wideoszkolenie PCC Poland adresowane do inspektorów ds. informatyzacji, informatyków i pracowników urzędów miast i gmin zajmujących się bezpieczeństwem systemów teleinformatycznych

Radzimy jakich zabezpieczeń użyć, aby uchronić urząd przed wyciekiem danych

Podczas wideoszkolenia zostaną omówione metody zabezpieczeń sieci i systemów teleinformatycznych wykorzystywanych w pracy urzędu. Prowadzący udzielą odpowiedzi na najczęściej zadawane pytania z zakresu wykorzystywania połączeń VPN, działania systemu elektronicznego zarządzania dokumentami oraz zachowania polityki bezpieczeństwa podczas pracy zdalnej

W programie m.in.:

- Kto ponosi odpowiedzialność w przypadku wycieku danych na komputerze prywatnym używanym do pracy zdalnej lub stacjonarnej w urzędzie gminy lub miasta?
- Jakie zabezpieczenia należy stosować, aby uchronić się przed wyciekiem danych?
- Omówienie procedur zachowania bezpieczeństwa teleinformatycznego w trakcie korzystania z komputerów przenośnych podczas pracy zdalnej
- Czy bezpieczne jest używanie pulpitu zdalnego podczas pracy w urzędzie?
- Jakie oprogramowanie może poprawić przepływ informacji między działami urzędu podczas pracy zdalnej?
- Jaki typ zapór sieciowych należy użyć dla poszczególnych urzędów w zależności od ich wielkości?
- W jaki sposób skonfigurować połączenie VPN?

Wzory pism, jakie otrzymają uczestnicy:

- Wzory umowy porozumienia poprawnego użytkowania komputerów przez pracowników urzędu
- Wzór umowy powierzenia przetwarzania danych osobowych z dostawcami usług zewnętrznych

Szczegółowy program szkolenia:

1. Polityka bezpieczeństwa – wyciek danych oraz logi w systemach teleinformatycznych

Zagrożenie wycieku danych w urzędzie

- Rodzaje danych przechowywanych w systemach teleinformatycznych
- Podstawowe zagadnienia związane z polityką bezpieczeństwa danych przydatne w pracy inspektora ds. informatyzacji lub informatyka
- Jakie zabezpieczenia należy stosować, aby uchronić się przed wyciekiem danych?
- Jakie procedury należy wdrożyć w sytuacji wycieku danych?

- Wdrożenie KRI
- Omówienie EZD – przeniosłam zagadnienie z innego miejsca
- Co powinna zawierać umowa powierzenia przetwarzania danych osobowych?
- Kto ponosi odpowiedzialność w przypadku wycieku danych podczas pracy zdalnej pracowników urzędu?
- Kto ponosi odpowiedzialność w przypadku wycieku danych na komputerze prywatnym używanym do pracy zdalnej lub stacjonarnej w urzędzie?
- Odpowiedzialność karna i cywilna w przypadku wycieku danych

Informacje o zdarzeniach i działaniach wykonywanych na systemie komputerowym

- Jakie logi gromadzić?
- Ile czasu należy przetrzymywać logi dotyczące sprzętu?
- W jaki sposób należy gromadzić logi systemów teleinformatycznych?
- Jakie informacje można uzyskać z logów?
- Jak chronić i zabezpieczać logi systemów teleinformatycznych?
- Jak wykorzystywać logi zgodnie z zasadami bezpieczeństwa teleinformatycznego i RODO?
- Przedstawienie możliwych sytuacji awaryjnych oraz sposoby rozwiązań w związku z logami
- Jak archiwizować backup copy?

2. Praca zdalna

- Przekazywanie sprzętu komputerowego do pracy zdalnej i praca na prywatnym sprzęcie komputerowym
- Czy można przekazać sprzęt komputerowy oraz oprogramowanie dla pracowników urzędu?
- Na jakich warunkach można przekazać sprzęt komputerowy oraz oprogramowanie dla pracowników urzędu?
- Omówienie procedur zachowania bezpieczeństwa teleinformatycznego w trakcie korzystania z komputerów przenośnych podczas pracy zdalnej
- Jak bezpiecznie korzystać z przeglądarek internetowych?
- Zarządzanie hasłami – tworzenie bezpiecznych haseł
- Jak zabezpieczyć dane podczas pracy zdalnej w urzędzie?
- Jak kontrolować oprogramowanie zainstalowane na komputerach przenośnych wykorzystywanych do pracy zdalnej w urzędzie?
- Metody zabezpieczeń komputerów służbowych przed nieprawidłowym użytkowaniem przez pracowników urzędu gminy lub miasta (wykorzystywanie komputerów w celach prywatnych, ściąganie nielegalnego oprogramowania, naruszanie praw autorskich)
- Czy pracownicy urzędu mogą pracować zdalnie i stacjonarnie na prywatnych komputerach po wcześniejszym sprawdzeniu legalności programowania?
- Kto odpowiada za oprogramowanie na komputerze prywatnym używanym do pracy zdalnej lub stacjonarnej w urzędzie?
- Czy można kontrolować komputery prywatne używane do pracy zdalnej w urzędzie pod kątem ściągania nielegalnego oprogramowania oraz naruszania praw autorskich?

Jak pracować zespołowo podczas pracy zdalnej?

- Omówienie programów oraz narzędzi do pracy zdalnej. W jaki sposób wykorzystać te programy oraz narzędzia? Darmowe rozwiązania
- W jaki sposób korzystać z pulpitu zdalnego?

- Czy bezpieczne jest używanie pulpitu zdalnego?
- Jakie zagrożenia niesie używanie pulpitu zdalnego?
- W jaki sposób pracować zespołowo w chmurze z perspektywy pracy w urzędzie?
- Porównanie rozwiązań do pracy grupowej oferowanych przez Google oraz Microsoft. Jakie są darmowe oraz płatne rozwiązania?
- Przenoszenie danych do chmury – usługa OneDrive i Office 365, porównanie kosztów licencji
- Jakie oprogramowanie może poprawić przepływ informacji między działami urzędu podczas pracy zdalnej?
- W jaki sposób tworzyć formularze przez ePUAP? W jaki sposób tworzyć formularze na podstawie repozytorium dokumentów?
- Omówienie działania komunikatorów Teams oraz Zoom. Zestawienie ich z innymi opcjami dostępnymi na rynku

3. Jak zabezpieczyć sieć oraz systemy używane w urzędzie?

Zapora sieciowa – czy jest koniecznym zabezpieczeniem w urzędzie?

- Omówienie zagadnienia zapory sieciowej
- Rodzaje i typy zapór sieciowych
- Porównanie zapór sieciowych oraz ich działania
- Jaki typ zapór sieciowych należy użyć dla poszczególnych urzędów w zależności od ich wielkości?
- Jak używać zapory sieciowej?
- Jak działa zapora sieciowa typu UTM?
- Z czego składa się zapora sieciowa typu UTM?
- Przed czym chroni zapora sieciowa UTM?
- Jakie techniki oraz weryfikacje stosować w przypadku zapory sieciowej UTM?
- Jakie możliwości dostarcza zapora sieciowa UTM?
- W jaki sposób wykorzystać zaporę sieciową UTM w pracy urzędu?

Jak bezpiecznie połączyć użytkowników podczas pracy zdalnej?

- W jaki sposób zabezpieczyć połączenie VPN?
- Jaką darmową sieć VPN wybrać?
- Plusy i minusy darmowej sieci VPN
- W jaki sposób skonfigurować połączenie VPN?
- Czy połączenie VPN pozwala na prace na jednym systemie oraz bazie?
- Które połączenie VPN jest najbardziej opłacalne dla poszczególnych urzędów w zależności od ich wielkości?

Prowadzący:

Przemysław Cienkowski - Kierownik Referatu Zarządzania Dokumentacją i Bezpieczeństwa Informacji w Urzędzie Miasta Piotrkowa Trybunalskiego. Koordynator zespołu wdrażającego system elektronicznego zarządzania dokumentacją (EZD) w Urzędzie Miasta, Pełnomocnik Prezydenta Miasta ds. Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwa Informacji, Audytor ISO/IEC 27001:2013. Absolwent Uniwersytetu Łódzkiego.

Jacek Lara - Kierownik Referatu Informatyki Urzędu Miasta Piotrkowa Trybunalskiego. Koordynator wdrożeń systemów informatycznych użytkowanych w Urzędzie Miasta i Jednostkach Organizacyjnych Miasta w tym systemu klasy EZD. Nadzoruje i koordynuje system bezpieczeństwa teleinformatycznego Urzędu Miasta. Absolwent Politechniki Łódzkiej.