PROFESJONALISTA
Firma Szkoleniowo-Konsultingowa

Siedziba/biuro: ul. gen. F. Kleeberga 2; 85 – 791 Bydgoszcz
tel: /52/ 584 – 12 – 31; **fax:** /52/ 584 – 12 – 32 **e-mail:** biuro@profesjonalista.net.pl
NIP: 559–140–64–39 **Regon:** 093049465 **Konto:** PKO BP S.A. 30 1020 5040 0000 6302 0097 8692

Serdecznie zapraszamy Państwa pracowników na **wyjątkowo praktyczne** - **szkolenie on-line** poprowadzone przez **– wieloletniego praktyka PSZ** na temat:

Cyberbezpieczeństwo w PUP:

jak skutecznie chronić urząd przed cyfrowym atakiem.

Data szkolenia: – **18/09/2026** lub **23/11/2026**

CELE SZKOLENIA:

- **Nabycie praktycznych umiejętności** w zakresie procedur postępowania w przypadku wystąpienia incydentów bezpieczeństwa.
- **Ograniczenie podatności instytucji** na ataki wykorzystujące techniki manipulacji psychologicznej (socjotechnikę).
- Spełnienie wymogów prawnych dotyczących budowania świadomości bezpieczeństwa informacji.
- **Zminimalizowanie ryzyka** udanego cyberataku opartego na czynniku ludzkim.
- Nauka **prawidłowej reakcji na incydenty** bezpieczeństwa.

CZAS TRWANIA:	**4 - 5 godzin** / (*ostateczny czas szkolenia jest uzależniony m.in. od wielkości Grupy i toczącej się w trakcie szkolenia dyskusji*)
MIEJSCE:	**- własne miejsce pracy**/ dowolnie wybrane miejsce
FORMA:	- **szkolenie on-line/webinarium** - warsztaty praktyczne (rozwiązywanie bieżących problemów) - wykład / - elementy burzy mózgów - prezentacja (w materiałach szkolenia) - dyskusja panelowa (w miarę możliwości technicznych)
WYMAGANIA SPRZĘTOWE:	- łącze internetowe o wystarczającej przepustowości! - komputer / laptop / smartfon umożliwiający komunikację on-line; - oprogramowanie do komunikacji on-line (**platforma e-learning podana przez organizatora**)/ - kamera internetowa (opcjonalnie).

PROWADZĄCY ZAJĘCIA:

Pan **Grzegorz ŚWIDER – informatyk/programista – absolwent** Wyższej Szkoła Informatyki i Zarządzania w Rzeszowie na kierunku informatyka i ekonometria o specjalności systemy i sieci komputerowe; oraz kolejnej o specjalności informatyczne sieci globalne. Absolwent Uniwersytetu Rzeszowskiego; gdzie ukończył studia podyplomowe w zakresie – zarządzanie Funduszami Strukturalnymi. **Na co dzień pracownik PSZ**, dzięki czemu jest świetnie zorientowany w bieżących problemach pracowników Urzędów Pracy.

Na bieżąco i aktywnie uczestniczy w testach kolejnych wersji programów Syriusz / Płatnik – zwłaszcza w obszarze aktualizacji wielotysięcznych baz danych jakie posiadają jednostki PUP oraz wydajności prac serwerów SQL. Świetnie znający informatyczne oprogramowania i systemy, którymi posługują się jednostki PUP, od wielu lat zajmujący się również statystyką publiczną.

Wykładowca wspólnie z nami **realizuje rocznie dziesiątki szkoleń i konsultacji wewnętrznych w Urzędach Pracy** m.in. z zakresu efektywności, raportów ZUS U1-U7 oraz statystyki MRPiPS, a także programu PŁATNIK / Syriusz i **szkoleń w obszarze funkcjonalności platform elektornicznych: - praca.gov.pl / e-PUAP / PUE ZUS / e-Doręczenia.**

Plan/treść nauczania

1. Wprowadzenie i kluczowe pojęcia

- Specyfika danych w Powiatowym Urzędzie Pracy - *Rodzaje przetwarzanych danych wrażliwych: PESEL, historia zatrudnienia, stan majątkowy, dane medyczne (orzeczenia o niepełnosprawności*; d*ane osób bezrobotnych vs. dane wrażliwe przedsiębiorców (dotacje, KFS)*
- System informacyjny jednostki
- Cyberbezpieczeństwo a cyberzagrożenie - *definicje w kontekście administracji publicznej (triada CIA: Poufność, Integralność, Dostępność danych.*
- Proces, produkt i usługa ICT

2. Ramy prawne administracji publicznej

- Krajowe Ramy Interoperacyjności (KRI) - *Minimalne wymagania dla systemów teleinformatycznych w urzędzie*
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC)
- **Wdrażanie dyrektywy NIS2** w urzędach - *Sztywne terminy zgłaszania incydentów, obowiązkowe szkolenia, wdrożenie zarządzania ryzykiem*
- Podmioty kluczowe i ważne
- Nowe obowiązki administracji publicznej
- Ustawa o działaniach antyterrorystycznych - *Stopnie alarmowe CRP (ALFA, BRAVO, CHARLIE, DELTA-CRP) – co oznaczają dla zwykłego pracownika i jakie procedury należy wtedy uruchomić*
- Bezpieczeństwo informacji a RODO - *Kary finansowe i odpowiedzialność dyscyplinarna za wyciek danych interesantów*

3. Bezpieczeństwo systemów centralnych w Powiatowym Urzędzie Pracy

- Rola systemów centralnych (np. Syriusz Std) - *Bezpieczna praca w środowisku Syriusz Std, systemie Praca.gov.pl oraz centralnych rejestrach (ZUS, CRP KEP, PESEL, CEIDG)*
- Wymagania cyberbezpieczeństwa systemów rządowych - *Bezpieczne kanały komunikacji (tunele VPN, dedykowane certyfikaty klucza publicznego*
- Nadawanie i odbieranie dostępów - *zasada minimalnych uprawnień (pracownik widzi tylko to, co niezbędne do wykonania zadania); - procedura natychmiastowego odbierania dostępów w przypadku zwolnienia pracownika lub zmiany stanowiska*
- Odpowiedzialność jednostki za systemy centralne - *gdzie kończy się odpowiedzialność Ministerstwa, a gdzie zaczyna odpowiedzialność lokalnego PUP (bezpieczeństwo końcówki użytkownika).*
- Integracja zabezpieczeń lokalnych z centralnymi - *monitorowanie ruchu i logów systemowych na poziomie lokalnego urzędu*

4. Codzienne zagrożenia w pracy urzędnika (Socjotechnika)

- Phishing, spear-phishing i wieloskładnikowy złośliwy kod - *Ataki celowane na pracowników PUP (np. fałszywe CV od "kandydata do pracy" z załącznikiem .exe/.scr, maile od "Urzędu Skarbowego" lub "ZUS"). - Wieloskładnikowy złośliwy kod (Ransomware) – jak jedno kliknięcie może zablokować pracę całego urzędu*
- Bezpieczna korespondencja mailowa urzędu - *weryfikacja nadawcy (analiza nagłówków maila, pułapki w adresach e-mail np. *@gov-pl.cc)./ - zasady bezpiecznego przesyłania dokumentów (szyfrowanie załączników z hasłem przesyłanym innym kanałem).*

- Komunikatory służbowe a prywatne - *Zakaz przesyłania danych służbowych i osobowych przez Messenger, WhatsApp czy prywatne maile*
- Przesyłanie plików i zewnętrzne źródła - *Zagrożenie związane z "zagubionymi" pendrive'ami (ataki typu BadUSB). Blockowanie portów USB w urzędzie*
- Uwierzytelnianie w usługach zewnętrznych - *Higiena haseł: zasada unikalności, menedżery haseł, bezwzględny wymóg 2FA (Uwierzytelnianie Dwuskładnikowe).*
- Zagrożenia w publicznych sieciach Wi-Fi - *Dlaczego pracownik na delegacji nie może logować się do systemów PUP przez otwarte Wi-Fi (np. w pociągu, hotelu) bez aktywnego VPN.*

5. Nowe technologie i zaawansowane ryzyka

- **Sztuczna Inteligencja (AI)** jako źródło zagrożeń - *Generowanie idealnych językowo wiadomości phishingowych w języku polskim (koniec z błędami ortograficznymi jako znakiem rozpoznawczym oszustwa).*
- Deepfake, generatory głosu i vishing
- Dezinformacja ukierunkowana na administrację - *Kampanie fake news uderzające w lokalne urzędy*
- Media społecznościowe pracowników a wizerunek PUP - *Oversharing: co pracownik ujawnia na Facebooku/LinkedIn (np. zdjęcia z biura z widocznym monitorem, systemem Syrius lub dokumentami na biurku).*
- Bezpieczeństwo pracy zdalnej i hybrydowej - *Domownicy i osoby trzecie a wgląd w ekran służbowy. Bezpieczeństwo fizyczne laptopa służbowego.*

6. Zarządzanie bezpieczeństwem i incydentami w PUP

- Definicja i kategoryzacja incydentu - *Kiedy zgubienie pendrive'a, kliknięcie w podejrzany link czy brak dostępu do internetu staje się "incydentem bezpieczeństwa".*
- Procedura zgłaszania incydentów (wewnętrzna/zewnętrzna) - *Kogo zawiadomić najpierw (ASI, ABI/IOD, Informatyk urzędu)?/ - Jak i kiedy urząd musi zaraportować incydent do właściwego CSIRT (np. CSIRT NASK) – krytyczny czas 24/72 godziny*
- Obsługa i mitygacja skutków - *Pierwsza pomoc po cyberataku: odłączenie kabla sieciowego (LAN), zakaz wyłączania komputera (zabezpieczenie pamięci RAM dla celów dowodowych).*
- Wymagana dokumentacja według nowej ustawy KSC - *Prowadzenie wewnętrznego rejestru incydentów w PUP.*
- Obowiązki urzędników w wypadku awarii - *Procedura "Business Continuity" – jak obsługiwać bezrobotnych, gdy systemy IT nie działają (praca w trybie offline/papierowym).*

7. Rola kadry kierowniczej i podsumowanie

- Odpowiedzialność prawna i finansowa kierownictwa - *Osobista odpowiedzialność Dyrektora PUP za brak wdrożenia wymogów NIS2 (w tym kary finansowe nakładane bezpośrednio na kierowników jednostek).*
- Budowanie kultury cyberbezpieczeństwa w PUP - *Jak liderzy mogą promować zgłaszanie błędów zamiast karania za przypadkowe kliknięcie w phishing*
- Finansowanie zabezpieczeń i audyty - *Pozyskiwanie środków na cyberbezpieczeństwo w samorządzie (np. programy rządowe, fundusze celowe).*

8. Panel dyskusyjny, pytania i odpowiedzi

Powyższy program nauczania spełnia wszystkie wymogi, o których mowa w Rozporządzeniu Ministra Edukacji i Nauki z 2023r.; w sprawie kształcenia ustawicznego w formach pozaszkolnych.

Koszt szkolenia: - cena za uczestnictwo **1 słuchacza** w szkoleniu on-line/webinarium wynosi – **600,00zł netto/brutto (stawka VAT - zwolnienie na podstawie oświadczenia)**.

W celu zgłoszenia udziału w szkoleniu należy **wypełnić formularz zgłoszeniowy** i przesłać go poprzez e-mail na adres biuro@profesjonalista.net.pl ew. faksem na numer (52) 584-12-32. Po otrzymaniu Państwa zgłoszenia dokonamy potwierdzenia przyjęcia Rezerwacji na szkolenie.

***

Następnie najpóźniej na dzień przed datą wyznaczonego szkolenia (*i po potwierdzeniu zebrania grupy minimalnej na szkolenie*) – podamy dane niezbędne do zalogowania na platformie e-learningowej oraz pozostałe parametry techniczne konieczne do uczestnictwa w spotkaniu.

Dodatkowe informacje organizacyjne można uzyskać pod numerem **(52) 584 – 12 – 31**

Prosimy o dokonywanie zgłoszeń - najpóźniej na 2 dni przed planowanym szkoleniem

Organizator zastrzega sobie **możliwość odwołania lub przesunięcia szkolenia on-line/webinarium** w sytuacji, gdy nie zostanie osiągnięty minimalny limit grupy lub z powodu niedyspozycji wykładowcy. Informacje o zmianach w terminie szkolenia zostanie przesłana najpóźniej na dzień przed planowanym rozpoczęciem szkolenia.

Webinarium to szkolenie wykorzystujące transmisję audio-wideo w czasie rzeczywistym za pośrednictwem Internetu. Webinar jest zaplanowany na konkretny termin i odbywa się w ustalonych godzinach. Uczestnicy na żywo widzą i słyszą trenera, w każdej chwili można zadawać pytania ekspertowi na czacie bądź rozmawiać z innymi uczestnikami.

Osoby, które zapiszą się na webinarium, dzień przed otrzymają w mailu link do webinarium. W dzień szkolenia o ustalonej godzinie uczestnik klika w link i łączy się online z innymi uczestnikami oraz wykładowcą. Wyświetlane materiały szkoleniowe i prezentacje są widoczne w trakcie spotkania. Istnieje także możliwość aktywnego uczestnictwa w szkoleniu w tym celu należy mieć słuchawki z mikrofonem ew. kamerę internetową. Wykładowca przekazuje uczestnikom wybrane zagadnienia na prezentacji i omawia wszystkie kwestie merytoryczne. Podczas szkolenia prowadzący ma możliwość angażowania uczestników. Dzięki temu jest ono interaktywne. Po szkoleniu następuje sesja pytań i odpowiedzi, podczas której można wyjaśnić wszystkie wątpliwości związane z omawianym tematem. Każdy uczestnik po szkoleniu otrzyma materiały w wersji elektronicznej na e-mail.

Uwaga - trenerzy nie wyrażają zgody na jakąkolwiek formę utrwalania, powielania, udostępniania lub nagrywania przebiegu szkolenia oraz materiałów szkoleniowych. Treść szkolenia i materiały szkoleniowe objęte są prawami autorskimi.

Uczestników prosimy o **podawanie własnych adresów e-mail i bezpośrednich numerów telefonu** na wypadek ew. problemów technicznych zaistniałych w trakcie spotkania.