

„Cyberbezpieczeństwo w firmie”

Poziom podstawowy z elementami średniozaawansowanymi

19/11/2026

DARR S.A. - ul. Szczawieńska 2, Szczawno-Zdrój 58-310

PROGRAM SZKOLENIA (SKRÓCONY)

08:00 – 08:15	Rejestracja uczestników
08:15 - 09:30	- Wprowadzenie: dlaczego Cyberbezpieczeństwa dotyczy każdego pracownika? - Podstawowe pojęcia i sposób działania cyberprzestępców - Phishing i jego odmiany - Oszustwa wymierzone w sekretariaty i asystentów zarządu
09:30 – 09:45	Przerwa kawowa
09:45 – 11:00	- Socjotechnika w biurze i przez telefon - Hasła i bezpieczne logowanie - Bezpieczna praca z pocztą elektroniczną i dokumentami - Bezpieczeństwo stanowiska pracy i urządzeń biurowych
11:00 – 11:30	Przerwa obiadowa
11:30 – 12:45	- Praca zdalna, hybrydowa i w podróży - Ochrona danych osobowych i informacji poufnych - Media społecznościowe i cyfrowy ślad pracownika - Sztuczna inteligencja w pracy biurowej – szanse i zagrożenia
12:45 – 13:00	Przerwa kawowa
13:00 – 14:15	- Ransomware i infekcje złośliwym oprogramowaniem - Reagowanie na incydent – co robić, a czego unikać? - Podsumowanie
14:15 – 15:00	Podsumowanie, pytania

PROGRAM SZKOLENIA (PEŁNY)

08:00 – 08:15	Rejestracja uczestników
08:15 - 09:30	1. Wprowadzenie: dlaczego cyberbezpieczeństwo dotyczy każdego pracownika? - Aktualny obraz zagrożeń w Polsce na podstawie raportów CERT Polska - Typowe incydenty w małych, średnich i dużych firmach – studia przypadków z Polski i regionu - Człowiek jako pierwsza linia obrony organizacji - Skutki incydentu: straty finansowe, przestoje, utrata reputacji, odpowiedzialność prawna 2. Podstawowe pojęcia i sposób działania cyberprzestępców - Poufność, integralność i dostępność informacji w codziennej pracy - Kim są atakujący i jakie mają motywacje - Etapy typowego ataku: od rozpoznania do kradzieży danych lub pieniędzy - Najczęstsze rodzaje złośliwego oprogramowania w prostym ujęciu 3. Phishing i jego odmiany - Rozpoznawanie fałszywych wiadomości e-mail: nadawca, domena, linki, presja czasu - Smishing (SMS), vishing (telefon), quishing (kody QR) i fałszywe komunikatory - Phishing ukierunkowany (spear phishing) i ataki na kadrę zarządzającą (whaling) - Fałszywe powiadomienia: kurierzy, banki, urzędy, platformy chmurowe - Ćwiczenie: analiza prawdziwych przykładów wiadomości 4. Oszustwa wymierzone w sekretariaty i asystentów zarządu - Oszustwo „na prezesa” (CEO fraud) i przejęcie korespondencji biznesowej (BEC) - Podmiana numeru rachunku na fakturze i fałszywe zmiany danych kontrahenta - Podsywanie się pod zarząd, księgowość, dostawców i klientów - Deepfake głosowy i wideo – nowe oblicze oszustw telefonicznych - Procedura weryfikacji niezależnym kanałem (oddzwonienie na znany numer)
09:30 – 09:45	Przerwa kawowa
09:45 – 11:00	5. Socjotechnika w biurze i przez telefon - Najczęstsze techniki manipulacji: autorytet, pilność, życzliwość, strach - Fałszywy „serwisant IT”, kurier, audytor lub nowy pracownik - Wejście „na doczepkę” i bezpieczna obsługa gości w recepcji - Jak grzecznie, ale stanowczo odmówić udzielenia informacji 6. Hasła i bezpieczne logowanie - Zasady tworzenia silnych haseł i fraz hasłowych - Menedżer haseł jako codzienne narzędzie pracy - Uwierzytelnianie wieloskładnikowe (MFA): aplikacje, klucze sprzętowe, klucze dostępu (passkeys) - Ataki polegające na „zasypywaniu” prośbami o zatwierdzenie logowania - Sprawdzanie, czy dane logowania nie wyciekły 7. Bezpieczna praca z pocztą elektroniczną i dokumentami - Załączniki wysokiego ryzyka: makra, archiwa, pliki wykonywalne, nietypowe formaty - Bezpieczne otwieranie linków i plików udostępnianych w chmurze - Błędnie zaadresowane wiadomości i pułapki autouzupełniania adresów - Bezpieczne przysyłanie dokumentów poufnych: szyfrowanie, hasła, kanały firmowe 8. Bezpieczeństwo stanowiska pracy i urządzeń biurowych - Blokada ekranu, zasada czystego biurka i czystego ekranu - Aktualizacje systemu i aplikacji – dlaczego nie warto ich odkładać - Nośniki USB, nieznane urządzenia i ładowarki - Drukarki i urządzenia wielofunkcyjne jako źródło wycieku danych
11:00 – 11:30	Przerwa obiadowa

11:30 – 12:45	9. Praca zdalna, hybrydowa i w podróży - Publiczne sieci Wi-Fi, hotspoty i połączenie VPN - Ochrona przed podglądaniem i podsłuchem w miejscach publicznych - Urządzenia służbowe a prywatne – zasady korzystania - Bezpieczeństwo smartfona: blokada, aplikacje, uprawnienia, kopie zapasowe 10. Ochrona danych osobowych i informacji poufnych - RODO w codziennej pracy biura – najważniejsze obowiązki pracownika - Klasyfikacja informacji: publiczne, wewnętrzne, poufne - Bezpieczne przechowywanie, udostępnianie i niszczenie dokumentów papierowych i cyfrowych - Czym jest naruszenie ochrony danych i dlaczego liczy się czas zgłoszenia 11. Media społecznościowe i cyfrowy ślad pracownika - Jakie informacje o firmie i współpracownikach wykorzystują przestępcy? - Bezpieczne publikowanie: zdjęcia z biura, wydarzenia firmowe, podróże służbowe - Fałszywe profile, rekruterzy i oferty współpracy na portalach zawodowych - Ustawienia prywatności w najpopularniejszych serwisach 12. Sztuczna inteligencja w pracy biurowej – szanse i zagrożenia - Jakich danych nie wolno wprowadzać do publicznych narzędzi AI? - Wiadomości phishingowe generowane przez AI – brak błędów to już nie wyznacznik - Fałszywe nagrania, zdjęcia i głosy – jak zachować czujność - Firmowe zasady korzystania z narzędzi AI
12:45 – 13:00	Przerwa kawowa
13:00 – 14:15	13. Ransomware i infekcje złośliwym oprogramowaniem - Jak dochodzi do zaszyfrowania danych w firmie? - Objawy, które powinny zaniepokoić pracownika - Rola kopii zapasowych i dlaczego nie płaci się okupu - Pierwsze minuty po zauważeniu infekcji 14. Reagowanie na incydent – co robić, a czego unikać? - Jak i komu zgłosić incydent w firmie: dział IT, przełożony, inspektor ochrony danych? - Czego nie robić: usuwanie śladów, samodzielne „naprawianie”, ukrywanie błędu? - Zgłaszanie zewnętrzne: CERT Polska (incydent.cert.pl), przekazywanie podejrzanych SMS-ów na numer 8080, Policja - Kultura zgłaszania błędów bez obwiniania 15. Podsumowanie - Quiz sprawdzający wiedzę i omówienie odpowiedzi - Symulacja: rozpoznaj oszustwo w skrzynce pocztowej sekretariatu - Osobista lista kontrolna „10 nawyków bezpiecznego pracownika” - Sesja pytań i odpowiedzi, wskazanie materiałów do dalszej nauki
14:15 – 15:00	Podsumowanie, pytania