Warszawa dn. 9 stycznia 2023

Sekkura Sp. z o. o.
KRS 0000493718
01-445 Warszawa
ul. Erazma CIOŁKA 13/114
NIP: 5272708879
Nr rejestru działalności regulowanej RD-23/2017

SZKOLENIE Z ZAKRESU BEZPIECZEŃSTWA INFORMACYJNEGO

WPROWADZENIE

Żyjemy w erze „zmiany władzy", gdzie czynnik pieniądza i siły militarnej traci na znaczeniu, a zyskuje informacja. Informacja Stała się zasobem kluczowym zarówno dla podmiotów państwowych, gospodarczych i zwykłych ludzi. Z tego powodu negatywne zjawiska na tym obszarze istotnie nasiliły się w ciągu ostatnich dwóch dekad. Pojęcia takie jak fake news i wojna informacyjna weszły na stałe do naszych słowników, stanowią realne zagrożenie zarówno dla podmiotów państwowych, jak i zwykłych użytkowników. Wyciek informacji, dezinformacja, plotka, trolling często decydują o być albo nie być ludzkich karier, a niekiedy o losach całych przedsiębiorstw.

W ramach kursu zapobiegania wyżej wymienionym zjawiskom na poziomie osobistym i przedsiębiorstwa proponujemy:

- warsztaty wyszukiwania informacji (kto, co i ile może się dowiedzieć z Internetu o Tobie i/lub Twoim przedsiębiorstwie/instytucji);
- naukę praktycznego rozpoznawania i analizy fake news oraz deep fakes;
- uświadomienie zagrożeń związanych z wyciekami informacji, wskazanie głównych dróg ich wycieków oraz sposobów ujawniania przez cyberprzestępców i konkurencję;
- przegląd praktycznych, łatwych do przyswojenia i wdrożenia porad w zapewnienia sobie i przedsiębiorstwu bezpieczeństwa informacyjnego w Internecie.

Szkolenie prowadzimy w dwóch wersjach:

- wersji dedykowanej dla **kadry zarządzającej** ogniskując się na zagadnieniach o charakterze strategicznym;
- wersji dedykowanej dla **pracowników szczebla operacyjnego** z naciskiem na wdrożenie kompetencji praktycznych wykrywania i analizy dezinformacji, wyszukiwania informacji oraz neutralizowania zagrożeń informacyjnych.

Zakres szkolenia w wersji dla kadry zarządzającej:

1. Kto, co i jak wiele może się o nas lub naszej firmie dowiedzieć – perspektywa historyczna

Środki i metody inwigilacji elektronicznej (typologia stanów bezpieczeństwa informacyjnego/typologia ryzyk utraty informacji; studia przypadków utraty informacji – szpiegostwo przemysłowe, szpiegostwo polityczne; przestępczość pospolita; typowe miejsca i sposoby inwigilacji; urządzenia i oprogramowanie szpiegowskie).

Czas trwania: 1 x 45 minut, wykład i warsztat.

2. Wycieki danych. Jak to wygląda od strony cyberprzestępców?

Historia Raidforums i Breached.to. Wstawka etnograficzna o polskich cyberprzestępcach (prezentacja jednego z najdłużej funkcjonujących polskich forów cyberprzestępczych). WikiLeaks i jego copycats. Cryptome – tuba CIA? Ujawnione raje podatkowe – Offshore Leaks. Następcy WikiLeaks – Distributed Denial of Secrets.

Czas trwania: 1 x 30 minut, wykład i warsztat.

3. Jak żyć w świecie postprawdy, czyli Fake News Detection

Zagadnienia pojęciowe (disinformation/misinformation, fake news, sockpuppet, strawman, sybill attack, troll, fact checking i inne). Aspekt instytucjonalny – ręczna, ekspercka walidacja faktów. Od Snopes do Bellingcat. Politifact i FactCheck. Polskie i inne wybrane portale fact-checkingowe. Portale tematyczne. Mapa Reporters Lab. Uczenie maszynowe i oddolna weryfikacja dezinformacji. Metodyka wykrywania fake news (propozycje autorskie, zarys).

Czas trwania: 1 x 60 minut, wykład i warsztat.

4. Deep Fakes – o krok od utraty wiary w rzeczywistość

Historia, istota i typologia (jako zjawisko techniczne i kulturowe) deep fakes. Jak zdemaskować deep fakes – autorska analiza (sztuczne inteligencje *versus* wetware). Addendum praktyczne: wykrywanie deep fakes ze wsparciem AI.

Czas trwania: 1 x 45 minut, wykład i warsztat.

5. Bezpieczeństwo informacyjne z minimalną domieszką informatyki

Wdrażanie zasady „going gray" w Internecie. Przydatne nawyki i gadżety OPSEC. Rozdzielanie aktywności i ról społecznych. Wirtualizacja.

Czas trwania: 1 x 45 minut, wykład i warsztat.

Zakres szkolenia w wersji dla pracowników operacyjnych:

1. Cyberuniverse Analysis Tool (CAT) – kombajn do wyszukiwania informacji

Wprowadzenie do autorskiej wyszukiwarki. Instalacja, konfiguracja, używanie. Zasady bezpieczeństwa. Omówienie struktury.

Czas trwania: 1 x 60 minut, wykład i warsztat.

2. Przegląd wybranych narzędzi eksploracji Internetu – wyszukiwarek internetowych

Wyszukiwarki globalne. Wyszukiwarki zogniskowane na prywatności użytkownika. Metawyszukiwarki i multiwyszukiwarki. Wyszukiwarki oferujące agregowanie treści. Wyszukiwarki i katalogi lokalne. Wyszukiwarki ludzi. Wyszukiwarki „szarej literatury" (*grey literature*) i wyszukiwarki naukowe. Internetowa maszyna do podróży w czasie (wstecz) – archive.org. Wyszukiwanie w chmurach i wiadrach (Clouds&Bucket Search).

Czas trwania: 1 x 60 minut, wykład i warsztat.

3. Wywiad gospodarczy w służbie OSINT [zajęcia wykładowe i warsztatowe]

Geneza i rozwój wywiadu gospodarczego. Paradygmat *competitive intelligence.* Addendum praktyczne: gdzie i jak szukać w globalnych i europejskich bazach podmiotów gospodarczych (CoRD, Open Corporates i inne).

Czas trwania: 1 x 60 minut, wykład i warsztat.

4. Jak znaleźć rodaka/rodaczkę (lub jego/jej firmę). Polskie źródła dla potrzeb białego wywiadu [zajęcia warsztatowe]

Sztuka wyszukiwania w rejestrach publicznych (KRS, CEiIDG, Rejestr.io, CRBR,

RWDZ i inne). Zbiory danych i usługi wywiadowni gospodarczych. Giełdy długów i rejestry licytacji komorniczych. Opinie o pracodawcach i ogłoszenia o pracę. Bazy zawartości polskich mediów. Nieruchomości – ogłoszenia, rentier.io, baza pustostanów. Rejestry genealogiczne oraz bazy osób zmarłych jako źródło informacji. Taktyki wyszukiwania.

Czas trwania: 2 x 60 minut, wykład i warsztat.

5. **Jak żyć w świecie postprawdy, czyli Fake News Detection [zajęcia wykładowe i praktyczne]**

Zagadnienia pojęciowe (disinformation/misinformation, fake news, sockpuppet, strawman, sybill attack, troll, fact checking i inne). Aspekt instytucjonalny – ręczna, ekspercka walidacja faktów. Od Snopes do Bellingcat. Politifact i FactCheck. Polskie i inne wybrane portale fact-checkingowe. Portale tematyczne. Mapa Reporters Lab. Uczenie maszynowe i oddolna weryfikacja dezinformacji. Wybrane inicjatywy edukacyjne.

Czas trwania: 1 x 60 minut, wykład i warsztat.

6. **Deep Fakes – o krok od utraty wiary w rzeczywistość**

Historia, istota i typologia (jako zjawisko techniczne i kulturowe) deep fakes. Jak zdemaskować deep fakes – autorska analiza (sztuczne inteligencje *versus* wetware). Addendum praktyczne: wykrywanie deep fakes ze wsparciem AI.

Czas trwania: 1 x 60 minut, wykład i warsztat.

7. **Bezpieczeństwo informacyjne z minimalną domieszką informatyki**

Wdrażanie zasady „going gray" w Internecie. Przydatne nawyki i gadżety

OPSEC. Rozdzielanie aktywności i ról społecznych. Wirtualizacja.

Czas trwania: 1 x 60 minut, wykład i warsztat.

Podsumowanie

L.P.	Zakres szkolenia	Czas trwania (minuty)	Cena netto
1.	dla kadry zarządzającej	225	Ustalana z klientem
2.	dla pracowników operacyjnych	480	Ustalana z klientem