Szostek_digital i wspólnicy

Prof. UŚ Dariusz Szostek wraz z Partnerami zapraszają na

SPOTKANIA Z AI, CYBERBEZPIECZEŃSTWEM I PAPERLESS

Jak to wszystko wdrożyć zgodnie z prawem? Czyli co czeka **biznes**, **MŚP**, **administrację**, **służbę zdrowia** w świetle nadchodzących zmian legislacyjnych.

Jesteśmy świadkami kolejnej rewolucji technologicznej, tym razem opartej o algorytmy, w tym AI. Truizmem jest stwierdzenie, iż najbliższa dekada rozwoju gospodarki cyfrowej, ale co istotne także gospodarki tradycyjnej wymaga odpowiedniej implementacji do organizacji algorytmów, weryfikację już wykorzystywanych pod katem bezpieczeństwa i łańcucha dostaw, bezpieczne, odporne na ataki sposoby przechowywania danych, a także bezpieczne sposoby komunikowania się z wykorzystaniem bezpiecznych narzędzi oraz kanałów.

W chwili obecnej weszło lub wchodzi w życie szereg unijnych aktów prawnych w sposób istotny zmieniających a wielu przypadkach od nowa regulujących rynek i gospodarkę cyfrową. Wśród nich rozporządzenia **DSA**, **DSM** (dotyczące dużych platform internetowych), **AI Act**, ale nie mniej w zakresie wdrażania AI – Rozporządzenie Maszynowe (dla wielu przedsiębiorców nawet mające większe znaczenie niż AI Act). W zakresie bezpieczeństwa **DORA, MiCA, CRA** itd.

Wszystkie te akty odnoszą się bezpośrednio lub pośrednio do algorytmów, danych i bezpieczeństwa, ze szczególnym naciskiem na analizę ryzyka. To co do niedawna – wdrażanie w organizacji systemów informatycznych - podlegało wolnemu rynkowi i właściwie pełnej swobodzie, w świetle nowych przepisów, głównie dla bezpieczeństwa, w wielu przypadkach podlegać będzie co najmniej udokumentowanej analizie ryzyka, a także konieczności wprowadzenia nowych procesów w organizacji. Niestety zmiany te powiązane są z nowymi obowiązkami dla przedsiębiorców i koniecznością rozliczalności. **Dlaczego?**

SAMSUNG asseco Xtension™ GRUPA E www.grupae.pl Archicom ECHO GROUP Archicom COLLECTION

FITC Certum by asseco biocertiX CYFROWA POLSKA CyberDefence 24

https://szostek-digital.eu

W roku 2024 przeprowadzono na Polskę ponad **110 tys. ataków krytycznych** na infrastrukturę przedsiębiorców, administracji, służby zdrowia, uczelni itd. Polska zaraz po Ukrainie plasuje się na podium państw zagrożonych, inwigilowanych oraz atakowanych w cyberprzestrzeni. W dalszej kolejności atakowane są inne państwa UE i NATO. Unia Europejska dostrzegła problem cyberbezpieczeństwa Europy, w konsekwencji przyjęła pakiet zmian legislacyjnych w tym zakresie nakładając na **szereg nowych podmiotów,** w tym biznes (producentów min. żywności, leków, pojazdów, części do pojazdów), dostawców wody, energii, producentów urządzeń o podwójnym znaczeniu (w tym hardware) itd. **nowe obowiązki w zakresie cyberbezpieczeństwa.** Brak ich spełnienia, może skutkować **wyłączeniem z łańcucha dostaw**. Obowiązki te są zawarte w szeregu (wyżej wymienionych) aktów prawnych, nie tylko w NIS2.

Zostają także wprowadzone nowe, nieistniejące wcześniej narzędzia jak jednolita tożsamość cyfrowa w UE dla osób fizycznych jak i (nowość) osób prawnych (czego nie należy mylić z polskim mObywatelem), a także inne nowe kwalifikowane usługi zaufania. Zmienia się także podejście i rozumienie udostępniania danych osobowych.

Wiele podmiotów, w tym administracja wdraża narzędzia AI, często bez analizy ryzyka pod kątem nie tylko RODO ale także nowych przepisów dotyczących cyberbezpieczeństwa. W świetle nowych przepisów taka dowolność implementacji, w szczególności w odniesieniu do podmiotów ważnych lub krytycznych w znaczeniu dyrektywy NIS, jest niewłaściwe. I nie jest wystarczającym tłumaczeniem brak nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Jej brak **nie zwalnia z obowiązku** dostosowania działalności biznesowej, czy sposobu funkcjonowania administracji, do jednolitych wymogów cyberbezpieczeństwa. **Czas na przygotowanie** swojej organizacji do nadchodzących zmian, tym bardziej iż wymagają one długotrwałych działań, ciągłej analizy i dostosowywania się nie tylko do przepisów prawa ale i zmieniającej się technicznej i politycznej rzeczywistości.

Dlatego serdecznie zapraszamy wraz z naszymi Partnerami: Samsung, Asseco, FlyOnTheCloud, Grupą E, Związek Cyfrowa Polska, Archicom, Xtension, biocertiX oraz patronem medialnym CyberDefence24 na cykl nieodpłatnych spotkań w całej Polsce przybliżającej problematykę i przygotowujących do nowych wyzwań.

DO KOGO SKIEROWANE SĄ SPOTKANIA?

Przedsiębiorcy, którzy będą podlegali pod UKSC, ze szczególnym uwzględnieniem MŚP, prezydenci, burmistrzowie i sekretarze gmin, dyrektorzy szpitali, dyrektorzy IT uczelni wyższych.

KTO POPROWADZI SPOTKANIA?

Każde spotkanie poprowadzą prof. UŚ Dariusz Szostek i dr inż Rafał Prabucki wraz z przedstawicielami Partnerów oraz z udziałem Gości Specjalnych - osobowości ze świata biznesu, nauki lub administracji. Informacje na temat Gości Specjalnych, którzy pojawią się w poszczególnych miastach będziemy przekazywać Państwu na bieżąco.

prof. UŚ, dr hab. Dariusz Szostek - Profesor Wydziału Prawa i Administracji Uniwersytetu Śląskiego, radca prawny Specjalista z zakresu paperless, kwalifikowanych usług zaufanych, tożsamości cyfrowej, cyfrowego obiegu dokumentów, algorytmizacji procesów, implementacji w organizacji algorytmów w tym AI w zgodności z wymogami cyberbezpieczeństwa, tokenizacji procesów w tym wykorzystanie blockchain oraz smart contract, implementacji prawa w algorytmy (inżynieria prawa), cywilista. Realizator projektów Horizon 2020 związanych z innowacjami w przemyśle – SHOP4CF i MAS4AI.

Współtwórca m.in: koncepcji i legislacji eSądu w Lublinie – elektronicznego postępowania upominawczego; koncepcji i legislacji elektronicznego potwierdzenia odbioru, powszechnie stosowanego na Poczcie Polskiej (tablety na których potwierdza się odbiór pism); koncepcji i wdrożenia podpisu biometrycznego na tabletach min. biocertiX (wspólnego projektu Samsunga, Asseco i Xtension), koncepcji i wdrożenia oprogramowania Ius Case w wydawnictwie C.H. Beck Założyciel i dyrektor Centrum naukowego - CYBER SCIENCE - Śląskiego Centrum Inżynierii Prawa, Technologii i Kompetencji Cyfrowych, zrzeszającego Uniwersytet Śląski, Politechnikę Śląską, Uniwersytet Ekonomiczny w Katowicach, Instytut EMAG sieci Łukasiewicza i NASK. Działacz w zakresie zarządzania Internetem, członek rady programowej IGF Poland Ekspert kadencji 2020-2024 Obserwatorium Parlamentu Europejskiego ds. Sztucznej inteligencji.

SAMSUNG asseco Xtension™ GRUPA E www.grupae.pl Archicom ECHO GROUP Archicom COLLECTION

FITC Certum by asseco biocertiX CYFROWA POLSKA CyberDefence 24

Przewodniczący Zespołu ds. Cyberbezpieczeństwa Konferencji Rektorów Akademickich Szkół Polskich. W 2025 r. powołany przez wicepremiera K. Gawkowskiego na członka Rady Naukowej Instytutu Łączności Autor licznych książek i opracowań w zakresie prawa nowych technologii – „Legal tech. Czyli jak bezpiecznie korzystać z narzędzi informatycznych w organizacji, w tym w kancelarii oraz dziale prawnym". Inicjator serii metodyk związanych z technologią i prawem w wydawnictwie C.H. Beck. Członek licznych projektów w zakresie cyfryzacji.
Popularyzator wiedzy w zakresie Blockchain – członek Blockhaton EUiPO oraz autor między innymi Blockchain i Prawo (w wersji angielskiej Blockchain and law wyd. Nomos).
Współtwórca i partner w latach 2014-2024 kancelarii Szostek_Bar i Partnerzy, w latach 2017-2019 współpracownik PwC Legal, w latach 2019-2021 współpracownik Kancelarii Maruta-Wachta.
Odpowiedzialny za szereg wdrożeń paperless w organizacjach (m.in. w bankach).
Wykładowca akademicki – profesor na WPIA UŚ, ale także wykładowca studiów podyplomowych z zakresu nowych technologii, AI czy też cyberbezpieczeństwa na: Akademii Koźmińskiego, Polskiej Akademii Nauk, Politechnice Śląskiej (Zarządzanie cyberbezpieczeństwem).

dr inż Rafał Prabucki - doktor nauk prawnych i inżynier. Auditor wiodący ISO/IEC 27001, BCMS ISO 22301 oraz ISO/IEC 42001/2023. Posiadacz tytułu Certified in Cybersecurity (CC) wydanym przez (ISC)². Adiunkt na Uniwersytecie Śląskim.
Członek CYBER SCIENCE i SABI. Założyciel LegalHackers Katowice.
Asystent w zakończonych projektach dotyczących wykorzystania nowych technologii w przemyśle: MAS4AI na Uniwersytecie Śląskim i SHOP4CF na Uniwersytecie Opolskim. Alumn stypendiów w Polsce, Hiszpani i Niemczech.

Prowadzący wykłady na Uczelniach w Polsce, Litwie i we Francji. Kierownik studiów podyplomowych "Tokenizacja i automatyzacja procesów w gospodarce cyfrowej" na Uniwersytecie Śląskim.
Autor książek i komentarzy, uczestnik Hackathonów i konkursów na innowacje – finalista w Młodzi i Innowacyjni dla PGNiG w 2017 roku oraz drugie miejsce w #hack4law w edycji z 2024 roku.

AGENDA

Spotkanie z gościem specjalnym (za każdym razem będzie to lokalna osobowość)

1. Wprowadzenie. Zmiany legislacyjne dotyczące rynku cyfrowego w Europie i ich implementacja do krajowego porządku prawnego a cyberbezpieczeństwo.

- Dyrektywa NIS 2 i jej implementacja w UKSC
- Rozporządzenie DORA (Digital, Operational Resilience Act) a obowiązki przedsiębiorców
- Rozporządzenie Cyber Resilience Act (CRA) jako element cyberbezpieczeństwa
- Rozporządzenie Digital Service Act
- Rozporządzenie Machinery Regulation
- AI Act – czyli jak wdrażać narzędzia AI w zgodzie z regulacjami cyberbezpieczeństwa

Wykład Partnera: SAMSUNG - Tomasz Chomicki & XTENSION, Michał Kacprowicz – Cyberbezpieczeństwo rozwiązań mobilnych – strategia i przyszłość. Być nie tylko paperLess ale też CyberBezPieczny! (15 min.)

2. Jednolita tożsamość cyfrowa, kwalifikowane atrybuty, nowe podejście do danych osobowych, EU Wallet, kwalifikowane doręczenia, kwalifikowany rejestr elektroniczny i kwalifikowane repozytorium elektroniczne oraz inne kwalifikowane usługi zaufane jako istotny element cyberbezpieczeństwa. eIDAS w praktyce.

Wykład partnera: FOTC - Agata Pieńkosz i Paweł Kotuliński - Google Workspace i Google Cloud - bezpieczeństwo bez kompromisów.

3. Cyberbezpieczeństwo w praktyce:

- Jak przygotować organizację na nowe wymagania – krok po kroku.
- Wymagania UKSC:

- Podmiot kluczowy a podmiot ważny.
- Analiza ryzyka, łańcuch dostaw, zmiany procesowe organizacji.
- Wdrożenie narzędzi do oceny ryzyka, takich jak ISO 31000, NIST CSF.
- Mapowanie procesów biznesowych w celu identyfikacji potencjalnych punktów ryzyka.
- Ustalanie priorytetów w oparciu o krytyczność systemów dla działalności firmy.
- Przeprowadzanie audytów dostawców pod kątem zgodności z wymogami bezpieczeństwa.
- Zawieranie umów SLA (Service Level Agreements) obejmujących odpowiedzialność za bezpieczeństwo.

AGENDA C.D.

- Monitoring aktywności dostawców w czasie rzeczywistym.
- Opracowanie planu wdrożeniowego dla nowych wymagań UKSC.
- Prowadzenie regularnych szkoleń dla pracowników, uwzględniających zmiany w procesach.
- Stworzenie interdyscyplinarnych zespołów ds. zarządzania zmianą.
- Odpowiedzialność kierownictwa za cyberbezpieczeństwo.
- Wyznaczenie CISO (Chief Information Security Officer) lub dedykowane osoby odpowiedzialnej za bezpieczeństwo informacji.
- Regularne raportowanie zarządowi i radzie nadzorczej na temat stanu bezpieczeństwa i incydentów.
- Integracja zarządzania cyberbezpieczeństwem z ogólną strategią biznesową.
- Ustanowienie polityk bezpieczeństwa, które są częścią kultury organizacyjnej.

Wykład partnera: Grupa E - Tomasz Orłowski - Jak kompleksowo i praktycznie podejść do wdrożenia cyberbezpieczeństwa zgodnego z NIS2?"

4. Bezpieczna komunikacja – jak ja wprowadzić?

HARMONOGRAM

28 maja – WARSZAWA
3 czerwca – KATOWICE (podczas AIChallenger)
termin wkrótce – GDAŃSK
termin wkrótce – RZESZÓW
termin wkrótce – KRAKÓW
termin wkrótce – ŁÓDŹ
termin wkrótce – WROCŁAW
termin wkrótce – KIELCE
termin wkrótce – POZNAŃ
termin wkrótce – OPOLE

ZAPISZ SIĘ

KONTAKT

Jeżeli mają Państwo pytania dotyczące spotkań, prosimy o kontakt z Aleksandrą Jarzebską aleksandra.jarzebska@szostek-digital.eu lub Janem Szostkiem jan.szostek@szostek-digital.eu