

Warszawa, dnia 03 lutego 2020 r.

Zarząd Banku Spółdzielczego

Szanowni Państwo,

Związek Rewizyjny Banków Spółdzielczych im. F. Stefczyka w ramach statutowej działalności wskazuje na **konieczność podnoszenia kwalifikacji pracowników Banku**. Wraz z ekspertami Servus Comp zapraszamy na specjalistyczne szkolenie dla banków spółdzielczych:

PREMIUM BANK – ZASADY PRZESTRZEGANIA CYBERBEZPIECZEŃSTWA W STUKTURACH BANKU SPÓŁDZIELCZEGO

Czas trwania szkolenia: **1 DZIEŃ**

Opis szkolenia:

Cyberbezpieczeństwo to fundament funkcjonowania całej infrastruktury Banku. Niesie ze sobą zagrożenia cyberprzestępczością, cyberterroryzmem i cyberwojną. Szkolenie skupia się między innymi na:

- omówieniu aspektów związanych z ochroną przeciwko potencjalnej działalności cyberprzestępczej czyli cyberatakami
- zabezpieczeniu poufnych danych - w tym danych osobowych, środków finansowych, ciągłości pracy Banku
- bezpieczeństwie fizycznym zapewniającym ochronę przed zagrożeniami dla zasobów i informacji wrażliwej
- prezentowaniu narzędzi wyprzedzających, zalecanych przy kontrolach IPS, np. protokół 802.1x, które eliminują niebezpieczeństwo nieautoryzowanych urządzeń wyludzających dane bankowe
- oraz wiele innych aspektach związanych z cyberbezpieczeństwem w bankowości spółdzielczej

Zajęcia prowadzone są w formie wykładu z omówieniem i analizą konkretnych przypadków, tzw. case study. Celem studium przypadku jest pokazanie koncepcji wartych skopiowania, jak i potencjalnych błędów, których należy unikać.

Adresaci szkolenia:

- Inspektorzy Ochrony Danych (IOD)
- Administratorzy Systemów Informatycznych (ASI)
- Pracownicy odpowiedzialni za funkcjonowanie infrastruktury informatycznej
- Pracownicy zainteresowani kwestiami cyberbezpieczeństwa

Cele i korzyści szkolenia:

- Zwiększenie świadomości i wiedzy związanej z tematyką cyberbezpieczeństwa
- WYROBIENIE nawyku odpowiedzialnego i bezpiecznego korzystania z cyberprzestrzeni w miejscu pracy

- Zapoznanie się z podstawowymi pojęciami związanymi z kwestiami cyberbezpieczeństwa
- Świadome wdrażanie zasad cyberbezpieczeństwa w strukturach banku
- Usystematyzowanie posiadanej i poszerzonej wiedzy przez Uczestników szkolenia

Program szkolenia:

9.30 – 10.00 **Rejestracja Uczestników**

10.00 – 11.00 **Wprowadzenie**

- Powitanie i przedstawienie się
- Wprowadzenie, ustawa o cyberbezpieczeństwie

Bezpieczeństwo fizyczne

- Omówienie kwestii związanych z wymogami bezpieczeństwa fizycznego w Bankach Spółdzielczych z uwzględnieniem specyfiki branży oraz przepisów branżowych

11.00 – 11.15 **Przerwa kawowa**

11.15 – 12.15 **Program bezpieczeństwa i dokumentacja**

- Tworzenie i prowadzenie dokumentacji zgodnie z regułami
- Edukowanie użytkowników końcowych
- Reagowanie na incydenty

12.15 – 13.15 **Przerwa na lunch**

13.15 – 14.15 **Bezpieczeństwo urządzeń**

- Infrastruktura serwerowa (MS Windows/ Linux)
- Punkty końcowe
- Odtwarzanie awaryjne

14.15 – 14.30 **Przerwa kawowa**

14.30 – 15.00 **Infrastruktura**

- Infrastruktura sieciowa
- Segmentacja logiczna i fizyczna

15.00 – 16.00 **Bezpieczeństwo systemowe**

- Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe
- Zarządzanie lukami w zabezpieczeniach
- Rozwój oprogramowania
- Systemy IDS i IPS
- Rejestrowanie i monitorowanie, okresowe kontrole

16.0 – 16.10 **Podsumowanie i zakończenie**

Prowadzący szkolenie:

MACIEJ GROMEK

Systemowy Inżynier IT, ekspert technologiczny specjalizujący się w audytach dotyczących bezpieczeństwa fizycznego, cyberbezpieczeństwa, audytach podatności środowiska infrastruktury IT, testach penetracyjnych. Specjalnością jest analityka infrastruktury na styku proceduralnym i technologicznym.

Specjalizuje się w audytach technologii funkcjonujących w Bankach Spółdzielczych.

ANDRZEJ POPIOŁEK

Audytor Wiodący Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001. Wykładowca na studiach MBA dedykowanych dla Prezesów Banków Spółdzielczych.

Specjalizacja w zakresie polityki bezpieczeństwa w Bankach Spółdzielczych, Przedsiębiorstwach oraz Instytucjach Państwowych. Ścisła współpraca ze Związkiem Rewizyjnym Banków Spółdzielczych jako audytor rekomendacji D i audytu Bezpieczeństwa Informacji w Bankach Spółdzielczych, obecnie doradca.

Specjalista z zakresu audytów sprawdzających spełnienie wymagań KNF, KRI, RODO i in. w zakresie cyberbezpieczeństwa i wytycznych ustawowych. Specjalizacja w dostosowaniu procedur w Banku, Przedsiębiorstwie i Urzędzie do wymagań organów nadzorczych.

Wykładowca, szkoleniowiec, konsultant – <http://zadbajobezpieczenstwo.pl>

Pasja: winogradnik, znawca wina, degustator, podróżnik.

Koszt uczestnictwa w szkoleniu:

Koszt uczestnictwa w szkoleniu 1 osoby wynosi: 400 zł + 23% VAT.

Cena szkolenia obejmuje: koszty obiadu i przerwy kawowej.

Miejsce szkolenia:

Warszawa: Hotel Gromada, Pl. Powstańców Warszawy 2, 00-030 Warszawa;

Zgłoszenia:

Uprzejmie proszę o przesyłanie zgłoszeń (e-mail-em lub przez stronę internetową:

<http://zrbs.pl/uslugi/szkolenia/>) lub email: glogowska@zrbs.pl

**Z poważaniem
Prezes Zarządu
/-/ Piotr Huzior**

Zgłoszenie uczestnictwa w szkoleniu

„ZASADY PRZESTRZEGANIA CYBERBEZPIECZEŃSTWA W STUKTURACH BANKU SPÓŁDZIELCZEGO”

| | |
|------------------------------------|-----------------------|
| Nazwa i adres Banku Spółdzielczego | Nazwa Banku: |
| | Adres: |
| | NIP: |
| Telefon | |
| Email | |

| | |
|-----------------------------------|--|
| Delegatura | Temat: „ZASADY PRZESTRZEGANIA CYBERBEZPIECZEŃSTWA W STUKTURACH BANKU SPÓŁDZIELCZEGO ” |
| <input type="checkbox"/> Warszawa | 14.05.2020 |

Zgłaszamy udział następujących osób:

| L.p. | Nazwisko i imię uczestnika |
|------|----------------------------|
| | |
| | |

Wyrażam dobrowolną zgodę na otrzymywanie informacji handlowej drogą elektroniczną od Związku Rewizyjnego Banków Spółdzielczych z siedzibą w Warszawie (dalej - „ZRBS”) ul. Mokotowska 14, 00-561 Warszawa na wskazany w formularzu numer telefonu i adres e-mail oraz na używanie przez ZRBS telekomunikacyjnych urządzeń końcowych, których jestem użytkownikiem, dla celów marketingu bezpośredniego, zgodnie z art. 172 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 z późn. zm.).

Zgodnie z art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwane dalej „**RODO**”) ZRBS informuje, że:

- 1) administratorem danych osobowych podanych w formularzu rejestracyjnym jest Związek Rewizyjny Banków Spółdzielczych z siedzibą w Warszawie (dalej - „ZRBS”) ul. Mokotowska 14, 00-561 Warszawa; adres e-mail: sekretariat@zrbs.pl,
- 2) w ZRBS wyznaczony jest inspektor ochrony danych, z którym można skontaktować się poprzez e-mail: iod@zrbs.pl (z inspektorem danych osobowych można skontaktować się we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych);
- 3) dane osobowe podane w formularzu rejestracyjnym przetwarzane są w celach prawnie uzasadnionego interesu ZRBS, jako administratora danych, polegającego na obsłudze administracyjnej organizowanych szkoleń oraz w celach reklamowych, promocyjnych i marketingowych na potrzeby marketingu bezpośredniego własnych produktów i usług – na podstawie art. 6 ust. 1 lit. f) RODO;
- 4) dane osobowe podane w formularzu rejestracyjnym przetwarzane są wyłącznie przez administratora danych
- 5) dane osobowe są przetwarzane przez okres 5 lat;
- 6) osobie, której dane dotyczą, przysługuje prawo żądania dostępu do treści swoich danych osobowych oraz prawo żądania ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo wniesienia sprzeciwu wobec ich przetwarzania, a także prawo wniesienia skargi do organu nadzorczego;
- 7) podanie danych jest dobrowolne, ale niezbędne do wzięcia udziału w szkoleniu.