U mesecu informacione bezbednosti EU, pozivamo vas na regionalno savetovanje:

INFORMACIONA BEZBEDNOST
- Zakonodavstvo, GDPR, praksa -

Mesto: Zemun, Pregrevica 168, nastavna sala Instituta
Vreme: 25. i 26. oktobar 2018. od 10,00 do 15,30 časova

Predavači:

1) Slobodan Stojadinović, šef Odseka za bezbednost informacionih sistema Ministarstva spoljnih poslova Republike Srbije i član Tela za koordinaciju poslova informacione bezbednosti Republike Srbije.
2) prof. dr Gojko Grubor, ekspert za zaštitu podataka i informacija u računarskim sistemima i mrežama, digitalnu forenziku i upravljanje procesima u informacionim sistemima sa dugogodišnjim praktičnim iskustvom u institucijama koje se ovim poslovima bave na najvišem profesionalnom nivou.

O Savetovanju:

- Informaciona bezbednost je aspekt bezbednosti koji se odnosi na rizike povezane sa upotrebom IKT, uključujući bezbednost podataka, uređaja, informacionih sistema, mreža, organizacija i pojedinaca.
- Napadi na informacione sisteme su nadnacionalnog karaktera, pa, stoga, i odgovor na njih mora biti nadnacionalni, oličen u međudržavnim saradnjama i zajedničkim preventivnim aktivnostima.
- Opšta regulativa za zaštitu podataka (General Data Protection Regulation – GDPR) je u punoj primeni od 25. maja ove godine, pa su se pojavili i prvi problemi u primeni. Svi koji ostvaruju uvid u lične podatke građana su morali da usaglase svoje sisteme zaštite prema ovim pravilima. Posledice neusaglašavanja sa zahtevima GDPR za poslovne sisteme se kreću od opomena i zahteva za ispravljanje inspekcijskih nalaza, do novčanih kazni koje se kreću do 4% ukupnog prometa u prethodnoj godini. U narednom periodu, očekuje se porast ransomware napada (šifrovanja diska i iznude novca za dešifrovanje), upravo zbog rigorozne kazne za GDPR neusaglašenost.
- Na savetovanju kojeg realizujemo, uz instrukcije vrhunskog stručnjaka, saznajte sve o opštim odredbama GDPR, posebno o presudnim zahtevima za uspešnu implementaciju i dokumentaciju politika i procedura za GDPR usaglašenost i proverite da li ste na dobrom putu uspostavljanja ovih procedura, rešite probleme koji su se u njihovoj implementaciji eventualno pojavili i obezbedite bezbedno poslovanje, čime ćete izbeći ogromne kazne predviđene za nezakonito postupanje.

prijava@economicdiplomacy.co.rs; jmarinkov@economicdiplomacy.co.rs; ied.bg@mts.rs;
www.economicdiplomacy.co.rs

Namena:

Savetovanje je namenjeno odgovornim licima za informacionu bezbednost, kao i izvršiocima privrednog sektora, javne uprave i organizacija od posebnog značaja (iz svih organizacija koje skupljaju, obrađuju, prenose, skladište ili arhiviraju lične podatke zaposlenih, partnera, klijenata i kupaca), potom – informatičarima i drugim zaposlenima koji obrađuju lične i poslovne podatke, kao i profesionalcima različitih profila koji žele unaprediti znanja iz oblasti zaštite ličnih podataka u sistemima e-poslovanja uopšte.

Program savetovanja

I BLOK: INFORMACIONA BEZBEDNOST

1. Šta štitimo?
- Pojam i značaj informacije
- Informaciono komunikacione tehnologije
- Internet i njegovi servisi
- Informaciono društvo
- Aktivnosti na razvoju informacionog društva

2. Informaciona bezbednost
- Razvoj bezbednosti kroz istoriju
- Pojmovnik: bezbednost, sigurnost, zaštita
- Pojam informacione bezbednosti
- Ranjivost, pretnje i napadi
* Ranjivost
* Pretnje – vrste i izvori, pretnje vezane za ljudsku aktivnost, pretnje nevezane za ljudsku aktivnost
* Napadi – klasifikacija, napadači i njihovi ciljevi, alati, pristup, anatomija napada
- Sigurnosni servisi
- Rizici – analiza, upravljanje i nadzor
- Točak bezbednosti
- Strategija ostvarivanja bezbednosti
- Bezbednosna politika

3. Zaštita informacionih sistema
- Vrste zaštite
- Hardversko-softverska zaštita – firewall, proxy, DMZ, e-mail gateway, sistemi za detektovanje upada u mrežu...
- Zaštita softvera – otkaz, uništenje, gubljenje...
- Zaštita baza podataka, bekapi i druge bezbednosne mere
- Fizička i organizaciona zaštita – fizičke mere bezbednosti, organizacione mere bezbednosti
- Administrativna kontrola zaštite

- Zaštita na prenosnom putu – kriptozaštita
* Osnovni pojmovi kriptozaštite
* Digitalni potpis
* Digitalni sertifikati

4. Standardi za upravljanje informacionom bezbednošću
- Opšti model standarda zaštite
- Klasifikacija standarda
- Prednosti i nedostaci standarda
- Standardi za upravljanje IB
* ISO 27001:2005
* Klasifikacija informacione imovine
- Zaštita privatnosti i intelektualne imovine
- Dokumentacija zaštite

5. Informaciona bezbednost u Srbiji
- Zakon o informacionoj bezbednosti
* Na koga se odnosi
* Osnovna načela
* Definisanje osnovnih pojmova i entiteta
* CERT
* Kritična infrastruktura
* Samostalni rukovaoci informacionim sistemom
* Kriptobezbednost
* Telo za koordinaciju informacione bezbednosti
* Obaveze koje proizilaze iz Zakona
- Podzakonski akti
- Nadzor nad primenom Zakona

II BLOK: GDPR – PRIMENA

1. EU GDPR – opšte odredbe, principi i ključni termini

2. Ključni zahtevi za GDPR usaglašenost

3. GDPR opšti uslovi za nametanje administrativnih kazni (čl. 83)

4. Postavljanje, uloga i zadaci menadžera zaštite podataka–DPO (Data Protection Officer) – (čl. 37)

5. GDPR zahtevi za dobijanje pristanka vlasnika LP za pristup, brisanje, bekapovanje i arhiviranje LP, koji uključuju najdublje promene svih relevantnih procesa – poslovnih, pravničkih i tehnoloških.

6. Osnove ISMS i GDPR dobre prakse zaštite.

7. Početni problemi u primeni i kako ih prevazići

Kotizacija
Kotizacija za oba nastavna dana iznosi 19.000,00 (+PDV).

Prijavu je moguće izvršiti i za samo 1 nastavni dan, pa tako kotizacija po jednom bloku iznosi 10.500,00 (+PDV).

Popusti
Za prijave na oba nastavna dana odobravamo ukupan popust od 20%

Za prijave po blokovima odobravamo 5% popusta za uplate izvršene u roku od 2 dana od dana prijavljivanja i dodatnih 10% za dva i više učesnika iz iste organizacije.

Kontakt i prijava:
011/3077612, 3077613, 063/506097

prijava@economicdiplomacy.co.rs
ozizovic@economicdiplomacy.co.rs
ied.bg@mts.rs