|  |
| --- |
| C:\Users\nemanja.vukotic\Desktop\RATEL.png  **Upitnik o bezbednosti IKT sistema** |
| 1. Da li u vašoj kompaniji/organizaciji postoji sektor/odeljenje koje se bavi bezbednošću IKT sistema? |
|  |
| 1. Ukoliko postoji, da li je to poseban tim koji je fokusiran samo na pitanja IKT bezbednosti ili je deo šireg IT sektora (službe, …) čiji je to samo jedan segment delovanja? |
|  |
| 1. Koliko zaposlenih broji tim koji se bavi poslovima IKT bezbednosti i u kom režimu radnog vremena radi (da li 24x7, 8x5 ili nešto treće)? Koliki je godišnji budžet namenjen za osoblje tima? |
|  |
| 1. Koji je obrazovni/stručni profil zaposlenih koji se bave poslovima IKT bezbednosti? |
|  |
| 1. Da li vaša organizacija sprovodi mere redovne obuke/treninga/sertifikacije zaposlenih koji su zaduženi za poslove IKT bezbednosti? Ukoliko je odgovor potvrdan koliki je godišnji budžet koji se planira za takve aktivnosti, i gde se, tj. na koji način vrši obuka (interno među članovima tima, kod vendora, u zemlji, u inostranstvu...)? Da li vaša organizacija sprovodi programe obuke na temu IKT bezbednosti i za ostale zaposlene u vašoj organizaciji, ili korisnike vaših servisa/usluga ? |
|  |
| 1. Da li vaša organizacija učestvuje na domaćim ili međunarodnim skupovima na temu IKT bezbednosti. Ukoliko da, koliko često i koliki je budžet namenjen za takve aktivnosti? |
|  |
| 1. Da li postoje posebne mere fizičkog obezbeđenja za prostorije u kojima rade članovi tima koji se bave poslovima IKT bezbednosti ili gde se nalazi njihova oprema (poseban objekat, posebne prostorije sa autentifikacijom na ulazu, posebni režimi boravka u prostorijama ...)? |
|  |
| 1. Da li postoji poseban softver/sistem u kojem se vrši evidencija prijava bezbednosnih incidenata, i koji je to softver/sistem? |
|  |
| 1. Da li postoji univerzalna forma za prijavu bezbednosnih incidenata i koje su ključne informacije koje ona sadrži? Na koje sve načine se vrši prijava bezbednosnih incidenata (telefon, elektronska pošta, forma na web sajtu...)? |
|  |
| 1. Da li postoje definisani servisi IKT bezbednosti koje vaša organizacija nudi? Ukoliko postoje, molimo vas da nabrojite koji su to servisi (reaktivni, proaktivni, analiza bezbednosti, konsultantske uluge i slično...)? |
|  |
| 1. Ko su korisnici vaših servisa ili usluga vezanih za IKT bezbednost (da li su u pitanju samo interni sistemi i zaposleni ili se usluge nude i spoljnjim korisnicima vaših sistema ili servisa)? Ukoliko svoje servise ili usluge u vezi sa bezbednošću IKT sistema nudite eksternim korisnicima (izvan svoje organizacije), koji je nivo ovlašćenja koje služba koja se bavi poslovima IKT bezbednosti ima nad eksternim sistemima/mrežama/korisnicima? |
|  |
| 1. Da li je vaša organizacija odgovorna za neke od IKT sistema od posebnog zanačaja i koji su sistemi u pitanju? Koji je nivo ovlašćenja i odgovornosti koje vaš tim ima u vezi sa IKT sistemima od posebnog značaja? |
|  |
| 1. Da li koristite neki poseban softver/sistem za analizu bezbednosnih incidenata i njihovih artefakata i koji softver/sistem je u pitanju ? Da li posedujete izolovani sistem (laboratoriju) za sprovođenje testova ili analizu uticaja potencijalnih bezbednosnih incidenata ili njihovih artefakata? Koliki je godišnji budžet za nabavku opreme i/ili softvera za te potrebe? |
|  |
| 1. Da li vaša organizacija sprovodi kampanje ili testove vezane za navike zaposlenih ili korisnika vaših usluga/servisa, u pogledu raznih aspekata IKT bezbednosti, ili sa ciljem podizanja svesti o IKT bezbednosti, koliko često i kakvi su rezultati tih kampanja ili testova? |
|  |
| 1. Da li u vašoj organizaciji postoje testovi bezbednosti IKT sistema, koliko su česti i kakvi su rezultati tih testova? Da li pravite periodične/godišnje izveštaje o stanju IKT bezbednosti (broj i vrsta otkrivenih ili prijavljenih bezbednosnih incidenata)? Ukoliko da, možete li da nam date na uvid takve informacije? |
|  |
| 1. Da li u poslovima vezanim za bezbednost IKT sistema vaša organizacija sarađuje sa drugim sličnim organizacijama u zemlji ili inostranstvu? Ukoliko je odgovor potvrdan možete li nam dati primer iz kojih privrrenoh segmenata su te organizacije ili konkretne organizacije sa kojima sarađujete? |
|  |
| 1. Na koji način je uređena saradnja sa drugim sličnim organizacijama u zemlji ili inostranstvu (ugovori o saradnji, ugovori u poverljivosti informacija, ugovori o uzajamnom pružanju usluga na temu IKT bezbednosti, neformalna saradnja i slično...)? |
|  |
| 1. Da li postoje unapred uređene forme za razmenu podataka sa drugim sličnim organizacijama u zemlji ili inostranstvu? Da li postoje definisani parametri bezbednosti prenosa podataka tokom razmene infrormacija (elektronski potpisi, enkripcija, autentifikacija...)? Ukoliko postoje možete li nam opisati detalje tih procesa i procedura? |
|  |
| 1. Da li ste članovi nekih nacionalnih ili međunarodnih udrženja organizacija koje se bave bezbednošću IKT sistema? Ukoliko jeste, koje su organizacije u pitanju i koji je vaš nivo članstva (da li ste na nekoj zvaničnoj listi CERT organizacija, da li ste akreditovani ili sertifikovani...)? |
|  |
| 1. Da li u okvirima svog delovanja na poslovima IKT bezbednosti imate potrebu za postojanjem nacionalne organizacije koja bi se bavila koordinacijom takvih aktivnosti (nacionalni CERT)? |
|  |
| 1. Kakve servise/usluge bi ste očekivali od nacionalne CERT organizacije (razmena podataka, saveti, konsultacije, edukacija, sertifikacija, operativna podrška...)? |
|  |
| 1. U kojoj meri biste bili spremni da razmenjujete informacije, tj. prijavljujete nacionalnoj CERT organizaciji bezbednosne incidente koje se dogode u okviru vaših sistema ili kod korisnika vaših servisa/usluga? |
|  |
| 1. Kakvu formu bi ta saradnja morala da ima da bi zadovoljila vaše interne procedure u pogledu razmene podataka (ugovor o saradnji, ugovor o poverljivosti informacija, memoradnum, neformalna saradnja...)? |
|  |