СКМ-ЗП-РУ-04/01
Бр. 19-хххх/1
Датум: 27.11.2024



**“Онлајн” семинар на тема**

**САЈБЕР-БЕЗБЕДНОСТ И ЗАШТИТА НА ПОДАТОЦИ**

17-18.12.2024 година (вторник и среда)

09:00 – 13:00 часот

Во ера на дигитализација на работните процеси, сајбер безбедноста и приватноста се соочуваат со растечки предизвици. Оттука, несомнено се наметнува потребата од фокус кон сајбер безбедност и навременото идентификување, пресретнување, како и соодветно и навремено одговарање на ризиците, за да се спречи одреден настан кој би имал негативен исход врз работењето на компанијата.

За таа цел, Стопанската комора на Северна Македонија на **17 и 18 декември 2024 година** организира „онлајн“ семинар на тема **„САЈБЕР-БЕЗБЕДНОСТ И ЗАШТИТА НА ПОДАТОЦИ“.**

Овој семинар ќе им овозможи на учесниците да се здобијат со основни и со напредни знаења и вештини за управување со информациската безбедност и со заштитата на податоци, како и со актуелните ИТ-закани со кои можат да се соочат сите деловни субјекти. Семинарот овозможува учесниците постепено да се запознаат со ИТ-безбедноста и со чекорите што треба да се преземат за превенција и за заштита, како на ниво на компанија така и на индивидуално ниво.

Преку семинарот ќе се даде одговор на прашањата што се однесуваат на тоа како соодветно да се третираат ИТ-заканите, кои превентивни и детективни мерки да се применуват и кои се актуелните заштитни мерки од социјален инженеринг и од фишинг-напади, како да се класифицираат безбедносните ризици, какви прописи се потребни и кој треба да биде одговорен за нивната изработка и за нивното следење, како да се управува со кризните ситуации, на што треба да се обрне внимание при екстернализација на ИТ-услугите, но и како безбедно да се управува со интерниот развој и како правилно да се применат крипто-алгоритмите и различните методи за автентификација. Во рамките на семинарот ќе се опфати и изработката на анализа за позитивни, но и за негативни искуства од големи компании при управувањето со информациската безбедност и со заштитата на податоци.

**Семинарот е наменет** за ИТ-менаџери во компании, за раководители и вработени во ИТ-сектори кои се задолжени за развој на софтвер, тестирање на функционалности и за квалитет на софтверот, како и за ИТ-поддршка; за ИТ-сервис менаџери и за ИТ-проектни менаџери, за вработени во службите за безбедност на информациските системи, за интерни и екстерни ревизори, за вработени кои работат на развој на софтвери, како и на деловни и клиентски апликации, за лица задолжени за креирање и за контрола на ИТ-договорите и за следење на ризикот над екстернализираните ИТ-процеси, за вработени кои работат на развој на софтвер, за вработени во деловните сектори кои сакаат да го зголемат нивото на контрола над своите ИТ-процеси, како и за оние кои се занимаваат со развој на нови услуги преку дигитализација на работењето (електронски бизнис, мобилни услуги и сл.); за оние кои имаат потреба од заштита на информации за клиентите и за деловното работење поради висок степен на одговорност, регулаторни барања и на ризици во секојдневното работење.

Напомена: за следење на семинарот потребно е учесниците да имаат основно разбирање на ИТ-системите и на деловните процеси, како и познавање од основите на ИТ-нападите и на ранливоста на компаниите.

**Целта на семинарот** е учесниците да се здобијат со основно и со напредно знаење од областа на управувањето со информациската безбедност и со заштитата на податоци, да научат како да ги дефинираат и реално да ги проценат безбедносните ризици во организацијата, но и како подобро да ја разберат ИТ-контролата што се применува за детектирање и за превенција во начинот на кој се манифестираат безбедносните закани.

**НАПОМЕНА: Учесниците е потребно да имаат основно разбирање на ИТ системите и деловните процеси, разбирање на основните ИТ напади и ранивости во компанијата.**

**ПРОГРАМА**

 **I сесија: Информациска безбедност**

* **Управување со информациската безбедност во редовни и во кризни ситуации**
* **Управување со правата за пристап**
* **Улоги и одговорности на вработените**
* **ИТ-средства – хардвер и софтвер**
* **Приватни и службени уреди**
* **Управување со безбедносните барања**
* **Дигитална и виртуелна безбедност**
* **Годишна ревизија на правата за пристап во апликациите и известување**
* **Регулатива – општа регулатива за заштита на личните податоци (GDPR)**
* **Стандарди и најдобра пракса**
* **Актуелни случувања и примери од праксата**

**II сесија: Високотехнолошки криминал и ИТ-закани**

* **Злонамерни софтвери**
* **ИТ-напади и закани**
* **Keylogger – метод на напад, влијание и примери од пракса**
* **Ransomware – метод на напад, влијание и примери од пракса**
* **Како да се заштитиме**
* **Спречување напади, превенција и детектирање**

**III сесија: Социјален инженеринг и ИТ-закани**

* **Социјален инженеринг и *фишинг* (phishing)**
* **Актуелни закани и злоупотреби**
* **Примери на социјален инженеринг од регионот**
* **Видови напади и закани**
* **Што треба да преземете кога се сомневате дека сте нападнати**
* **Што треба да преземете кога се сомневате дека сте хакирани**

**IV сесија: Социјален инженеринг во пракса**

* **Целен напад врз поединци – анализа на примери од пракса**

**V сесија: Заштита на податоци**

* **Дефинирање процеси за заштита на податоци**
* **Класификација на информации**
* **Приватност на податоци од клиенти и од вработени**
* **Управување со лични податоци**
* **Информациски средства на компанијата**
* **Лична приватност – што да направите и како да се заштите**
* **Примери од пракса – актуелни случувања**

**VI сесија: Работилница**

* **Заштита на податоците во пракса – добри и лоши искуства**

**VII сесија: Криптографија и методи на автентификација**

* **Криптографија и примена**
* **Крипто алгоритми**
* **Дигитален потпис**
* **Безбедносни протоколи**
* **Методи на автентификација**
* **Управување со лозинки**

**VIII сесија: Злонамерни софтвери**

* **Дали секој злонамерен софтвен има јасна цел?**
* **Кој се’ не напаѓа?**
* **Бирање на мета и постигнување на целта**
* **Истражување и подготовки**
* **Грешки во текот на развој**
* **Пуштање и ширање на злонамерен софтвер**

**IX Сесија: Работа на одалечена локација**

* **Безбедносни предизвици – стари и нови**
* **Кои локации се безбедни**
* **Ажурирање на софтвери**
* **Користење на ИТ уреди и поврзување на Интернет**

**X сесија: Управување со безбедносни ризици**

* **Класификација и анализа на безбедносните ризици**
* **Превземање на мерки за ублажување на безбедносните ризици**
* **Кога прифаќаме безбедносни ризици?**
* **Примери на добро и лошо управување со безбедносни ризици**

**XI сесија: Скенирање на ранливост и имплементација на patch**

* **Дефинирање на процеси, улоги и одговорности**
* **Скенирање на софтверска ранливост**
* **Ажурирање (Update) и patch management**
* **Улога на екстерните партнери**
* **Известување**

**XII сесија: Примери од пракса**

* **Сајбер напади на компанијата**

 **Предавач:**

**- Лука Милинковиќ,** Менаџер за безбедност, управување и ризик во компанија за развој и дизајн на софтверски решенија. Милинковиќ има повеќегодишно искуство со контрола и со управување на електронските ризици, со специјализација во областа на дефинирањето на електронските процеси (ITIL-процеси) и на примена на самата контрола. Со информациска безбедност и со едукација се занимава повеќе од 10 години, а за време на тој период има работено и на Електротехничкиот факултет во Белград, како и во неколку банки во Р Србија. Има работено на развој и на примена на безбедносни методи, мрежни технологии и на алгоритми за енкрипција. Автор е на многубројни трудови и учествувал на домашни и на меѓународни научни конференции, а член е и на електронското списание PC Press. Тој, исто така, е сертифициран внатрешен ревизор за управување со ризик ISO/IEC 27001 и ISО 31000.

**За сите учесници ќе биде обезбедено:**

* + упатства за приклучување на „онлајн“ семинарот;
	+ работни материјали во електронска верзија и
	+ eлектронски сертификат за учество на семинарот.

***Сите заинтересирани за учество на овoj “онлајн“ семинар можат да се пријават најдоцна до 13.12.2024 година.***