СТОПАНСКА КОМОРА НА СЕВЕРНА МАКЕДОНИЈА
ECONOMIC CHAMBER OF NORTH MACEDONIA

А Г Е Н Д А

“Онлајн” семинар на тема

САЈБЕР-БЕЗБЕДНОСТ И ЗАШТИТА НА ПОДАТОЦИ

17-18.12.2024 година (вторник и среда)
09:00 – 13:00 часот

I ден (17.12.2024 година)

Време	Тема
09:00 – 09:50	**I сесија: Информациска безбедност** • Управување со информацискатa 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
09:50 – 10:40	**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
10:40 – 11:20	**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
11:20 – 11:40	**Пауза**
11:40 – 12:00	**IV сесија: Социјален инженеринг во пракса** • Целен напад врз поединци – анализа на примери од пракса
12:00 – 12:40	**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
12:40 – 13:00	**VI сесија: Работилница** • Заштита на податоците во пракса – добри и лоши искуства

II ден (18.12.2024 година)

Време	Тема
09:00 – 09:40	**VII сесија: Криптографија и методи на автентификација** • Криптографија и примена • Крипто алгоритми • Дигитален потпис • Безбедносни протоколи • Методи на автентификација • Управување со лозинки
09:40 – 10:20	**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
10:20 – 11:00	**X 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
11:00 – 11:20	**Пауза**
11:20 – 12:00	**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
12:00 – 12:30	**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

12:30 – 12:50	**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
12:50 – 13:00	**XII сесија: Примери од пракса** Сајбер напади на компанијата