https://www.pexels.com/photo/photo-of-person-holding-mobile-phone-3183153/

ОСНОВНИ ПОЈМОВИ УПРАВЉАЊА РИЗИКОМ И КОНТИНУИТЕТОМ ПОСЛОВАЊА

ПРИЈАВИТЕ СВАКИ ИНЦИДЕНТ
НА НАШЕМ ПОРТАЛУ

СРБ-ЦЕРТ

ОСНОВНИ ПОЈМОВИ УПРАВЉАЊА РИЗИКОМ И КОНТИНУИТЕТОМ ПОСЛОВАЊА

Без употребе информационих технологија пословне организације[1] не могу замислити своје пословање. Процес дигитализације је унапредио пословање, донео бројне бенефите, али се паралелно са развојем нових технологија повећала изложеност ризицима и претњама, што може имати утицај на имовину, запослене, информације, друге организације, као и на само пословање.

Претње по информациони систем укључују прекиде под утицајем околине, људске грешке, хардверске грешке, сајбер нападе који су често добро организовани и веома софистицирани, а последице могу бити катастрофалне по организације.

Учесталост сајбер напада је све већа и присутнија у државним институцијама, финансијским институцијама, удружењима, али и у малим и средњим предузећима, а који за циљ имају нарушавање угледа и репутације, крађу података или идентитета, прекид пословања, финансијске преваре, новчане изнуде и др. Чињеница је да је сајбер нападе све теже детектовати и адекватно и правовремено реаговати, односно није могуће у потпуности се заштитити, стога је веома важно дефинисати планове и акције којима се прецизира шта треба урадити када се сајбер напад догоди. Унапред дефинисани ризици као и начини поступања могу бити добар начин умањења последица проузрокованих сајбер нападима.

Пословне организације изложене су различитим врстама ризика који могу озбиљно угрозити њихово пословање. У циљу обезбеђивања пословања у случају нежељеног догађаја неопходно је превентивно планирање и предузимање корака ради умањења последица, омогућавања наставка рада и опоравка од непланираних прекида пословних функција.

Управљање континуитетом пословања (*Business Continuity Management* - **BCM**) је приступ целокупном пословању који се састоји од политика, процедура, смерница и са њима повезаних ресурса, организационих улога, одговорности, овлашћења, као и планирања активности које омогућавају функционисање у случају непредвиђених околности.

BCM обухвата **План континуитета пословања** (*Business Continuity Plan* - **BCP**) који описује приступ процени прекида, планирања опоравка од прекида, и сталног праћења опоравка. Добар план подразумева добро урађену идентификацију, анализу и евалуацију ризика, дефинисане кључне процесе, адекватно имплементирано решење за опоравак система, план активности и додељених одговорности.

Примерена процена ризика идентификује претње и рањивости којима је изложена организација, процењујући вероватноћу да ће се неки догађај догодити и његову потенцијалну последицу (Слика 1). На темељу тога се може одредити и проценити стварна изложеност ризику и учинковито планирати улагања како би се постигао очекивани ниво безбедности ИКТ система.

[1] Пословна организација обухвата, али није ограничена на предузетнике, компанију, корпорацију, фирму, предузеће, орган власти, партнерство, добротворну организацију или институцију, или њихов део или комбинацију, без обзира на то да ли су обједињени или не и да ли су јавног или приватног карактера.

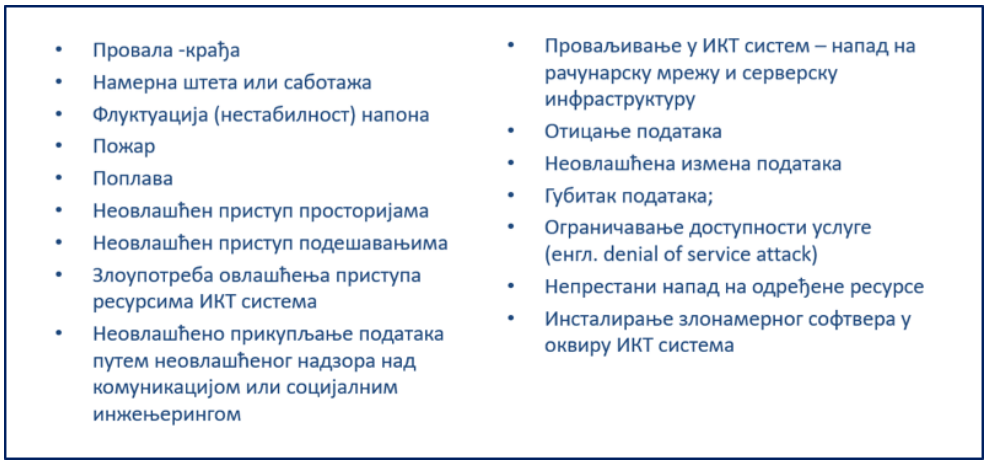
Слика 1 - Настанак безбедносних инцидената

Ризик је комбинација последица неког догађаја (укључујући и промене у околностима) и повезане вероватноће настанка. У контексту информационе безбедности, ризици по безбедност информација могу се изразити као ефекат несигурности на циљеве безбедности информација.

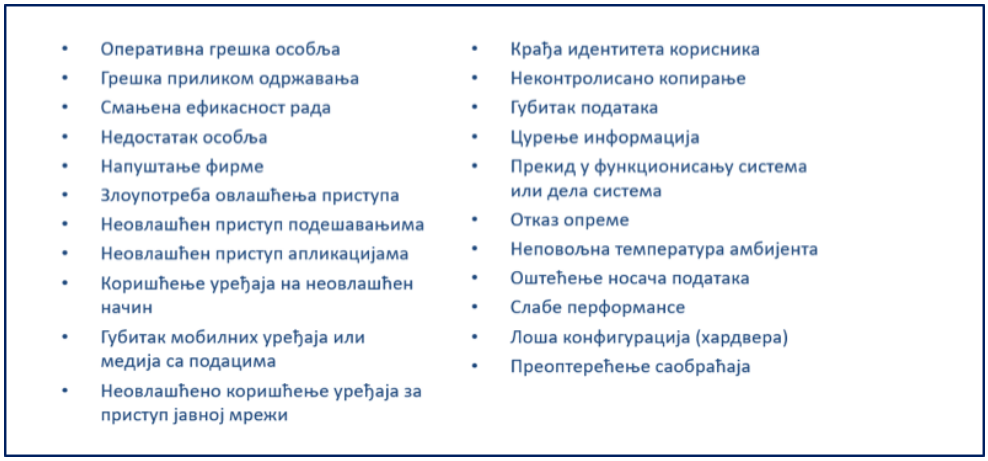
Управљање ризиком је процес који обухвата систематску примену политика менаџмента, процедура и праксе на активности комуницирања, консултовања, успостављања контекста и идентификовања, анализирања, вредновања, поступања, праћења, преиспитивања и извештавања о свим ризицима који могу утицати на достизање стратешких и финансијских циљева организације (Слика 2).

Слика 2 – Процес управљања ризиком

Идентификација ризика подразумева проналажење, препознавање и описивање ризика који могу помоћи или спречити организацију да постигне своје циљеве. Облици спољних претњи који се могу јавити приликом идентификације ризика приказани су на Слици 3, док су облици унутрашњих претњи приказани на Слици 4.



Слика 3 – Облици спољних претњи



Слика 4 – Облици унутрашњих претњи

Анализа ризика је процес разумевања природе ризика и утврђивања нивоа ризика.

Вредновање ризика захтева оцењивање ризика и методу поступања са ризиком, која може обухватити процену трошкова и користи, законске обавезе, бригу о заинтересованим странама и другим улазним елементима. Овим поступком је потребно квантификовати и одредити приоритете ризика према критеријумима за прихватање, односно неприхватање ризика.

Могуће опције за **поступање са ризиком** обухватају следеће одлуке:

- Примењивање одговарајућих мера да би се ризици отклонили или смањили;
- Промена вероватноће настанка ризика;
- Промена последица;
- Зналачки и објективно прихватање ризика, обезбеђујући да они јасно задовоље политику организације и критеријуме за прихватање ризика;
- Избегавање ризика не допуштајући мере које би довеле до појаве ризика, односно да се не почиње или не наставља са активношћу која доводи до ризика
- Дељење ризика са другом страном или странама, на пример осигуравајућим кућама.

Током целокупног процеса управљања ризиком треба имати у виду да поступање са ризиком може створити нове ризике или модификовати постојеће.

Сврха **надгледања и праћења ризика** је побољшање квалитета и ефикасности примене резултата процеса за поступања са ризиком, снимањем резултата и пружањем повратних информација.

Целокупан процес управљања ризиком и резултате процеса је потребно документовати и вршити **извештавање** помоћу одговарајућих механизама. На тај начин се пружају информације које су потребне за доношење одлука, побољшање активности за управљање ризиком као и за потребе одговорних лица за процес управљања ризиком.

С обзиром на чињеницу да се област сајбер безбедности брзо развија, да би процес управљања ризиком био успешан, неопходна је и константна провера идентификованих ризика и дефинисаних мера које треба применити, као и континуирано побољшање начина и планова за управљање ризицима.

Национални ЦЕРТ Републике Србије не промовише или фаворизује било који од коришћених јавних извора, међу којима су и комерцијални производи и услуге. Све препоруке, анализе и предлози дати су у циљу превенције и заштите од безбедносних ризика.

Извори:

- SRPS ISO/IEC 27000:2016 Информационе технологије – Технике безбедности – Системи менаџмента безбедношћу информација
- SRPS ISO/IEC 27005:2011 Информационе технологије – Технике безбедности – Системи менаџмента безбедношћу информација
- ISO 22301:2019(en) Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020(en) Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO 31000:2018(en) Risk management — Guidelines
- Студија изводљивости успостављања процедура националног ЦЕРТ-а и управљања системом за пријаву инцидента; Оквир плана континуитета пословања за ЦЕРТ платформу