

Управљање безбедношћу и ризицима

Стратегија информационе безбедности



Бранко Суботић, Консултант
Контакт: branko.subotic@rs.ey.com

Принципи и кључни концепти управљања Информационом безбедношћу

► Стратегија информационе безбедности

Стратегија информационе безбедности – Основни концепти

Технике стратешког управљања и анализе

Пример стратешког плана информационе безбедности

► Управљачки оквир

Хијерархија управљачког оквира

Три нивоа политика

► Вежба

Стратегија информационе безбедности – Основни концепти

► Вредности

Шта представљају вредности? Етика, Принципи, Веровања

► Визија

Шта ми то хоћемо да будемо? Наде и Амбиције

► Мисија

Шта ми то радимо? Мотивација и Сврха

► Стратешки циљеви

Како ћемо то да урадимо? Циљеви и планови

► Акције

Које конкретне активности треба да спроведемо и како да то меримо? Акције, ресурси, резултати и њихово праћење (кључни индикатори перформанси)



Стратегија информационе безбедности – Основни концепти

► Стратешко планирање

Дугорочно, планирање на 3 до 5 година, годишња ревизија

► Тактичко планирање

Средњи рок, планирање на годину дана, буџетирање

► Оперативно планирање

Детаљно планирање према специфичним активностима



Технике стратешког управљања и анализе

► SWOT анализа

Интерни фактори:

- **Снаге:** Компаративне предности компаније, специфичне вештине и знања запослених или компанијски ресурси.
- **Слабости:** Компаративни недостаци компаније, ограниченост ресурса или знања
- Фокус на људске ресурсе, физичке ресурсе, финансије, активности и процесе, као и претходна искуства

Екстерни фактори:

- **Шансе:** Трендови и тржишта која могу бити искоришћена у будућности
- **Претње:** Негативни трендови или регулатива који могу негативно утицати на пословање
- Фокус на будуће трендове, економију, финансирање, регулативу, итд.

		Позитивне	Негативне
Интерне	Интерне	Strengths (Снаге)	Weaknesses (Слабости)
	Екстерне	Opportunities (Шансе)	Threats (Претње)

Технике стратешког управљања и анализе

► ГАП анализа - основни кораци

1. Идентификовати постојећи процес
2. Идентификовати постојеће резултате
3. Идентификовати жељени резултат
4. Идентификовати и документовати ГАП
5. Идентификовати процес како превазићи ГАП
6. Идентификовати средства потребна за превазилажење ГАП-а
7. Направити план и приоритета акција

Област	Постојеће стање	Жељено стање	Разлика (ГАП)	Акциони план	Приоритет
Енкрипција података	Енкрипција на мањем делу база	Енкрипција на свим базама	Већи део база без енкрипције	Имплементирати енкрипцију на продукционим базама	Висок
				Имплементирати енкрипцију на развојим и тестним базама	Средњи

Технике стратешког управљања и анализе

► Финансијско управљање

ОРЕХ vs. CAPEX

Процес буџетирања и пословног планирања

► Пословни случај и финансијски показатељи

РОИ - Поврат на уложене инвестиције. Израчунава се као укупна годишња корист подељена са износом укупне инвестиције

ТЦО - Укупни трошкови власништва. Израчунава се тако што поред очигледних трошкова набавке, укључује све трошкове који настају у будућности (трошкови лиценци, трошкови одржавања, трошкови интерно запослених, трошкови пропуштених прилика, а не само трошак чисте куповине).

РОСИ - Поврат на уложене инвестиције у безбедност. Израчунава се као укупна годишња корист подељена са износом укупне инвестиције

Технике стратешког управљања и анализе

- $РОСИ = \frac{\text{Користи од инвестиције у безбедност} - \text{Трошак инвестиције}}{\text{Трошак инвестиције}}$

Пример (решење за е-маил безбедност):

1. Идентификовати релевантно решење и одредити трошкове инвестиције. Нпр. Трошкови куповине су 50к ЕУР и трошкови одржавања 10кЕУР годишње
2. Идентификовати и квантификовати користи од инвестиције. Уштеде у трошковима од смањеног ризика (нпр. Уштеда од 100кЕУР годишње на трошкове техничке подршке, као и уштеда од потенцијалних 500кЕУР, која може настати неуторизованим одливом података)
3. Израчунати РОСИ. $(100.000 + 500.000 - 50.000 - 10.000) / (50.000 + 10.000) = 5,25$

Закључак: Сваки уложени долар у систем филтрирања е-поште, компанија може очекивати да ће добити 5,25 долара финансијских користи

Пример Стратешког плана информационе безбедности

Компанија АБЦ се бави производњом висококвалитетних органских пољопривредних производа који се продају на светском тржишту коришћењем дигиталних (e-commerce) сервиса.

Компанија АБЦ је дефинисала своју стратешку доктрину кроз следећу изјаву о њеним вредностима, визији и мисији.

Основне вредности

1. **Одрживост:** Посвећени смо заштити околине кроз одрживе пољопривредне праксе које чувају земљиште, воду и биодиверзитет.
2. **Интегритет:** У свим аспектима нашег пословања поступамо транспарентно и етички, гарантујући аутентичност и квалитет наших органских производа.
3. **Квалитет:** Не правимо компромисе када је у питању квалитет наших производа. Користимо само најбоље, природно узгајане састојке без употребе пестицида, хербицида или вештачких адитива.
4. **Заједница:** Изградња снажне, здраве заједнице је срж нашег пословања. Подржавамо локалне пољопривреднике, послујемо одговорно и учествујемо у друштвеним иницијативама.
5. **Иновација:** Непрестано тежимо иновацијама у начину на који узгајамо, пакујемо и дистрибуирамо наше производе, како бисмо побољшали квалитет и доступност органске хране.

Пример Стратешког плана информационе безбедности

Визија

Наша визија је да будемо лидер у индустрији органске хране, пружајући здраве, одрживе и висококвалитетне производе који обогаћују животе наших купаца и штите наше окружење.

Мисија

Наша мисија је да производимо и достављамо свеже, чисте и етички произведене органске производе који промовишу здрав начин живота и подржавају добробит заједнице. Тежимо да инспиришемо и едукујемо потрошаче о предностима органске исхране, осигуравајући приступачност и практичност кроз нашу онлајн платформу.

Компанија АБЦ обрађује велике количине приватних података и процесира бројне онлине и картичне трансакције, тако да је значајно изложена ризицима који угрожавају информациону безбедност. На основу анализе ризика, спроводне од стране екстерних консултаната, идентификовани су следећи ризици, као најкритичнији за пословање компаније:

1. Ризик крађе података о личности
2. Ризик крађе информација о кредитним картицама и трансакцијама
3. Финансијске преваре кроз креирање лажних фактура и SWIFT платних налога
4. Ransomware напади

Пример Стратешког плана информационе безбедности

Обзиром на наведено, компанија АБЦ је дефинисала стратегију информационе безбедности која дефинише следеће елементе:

Визија

Постати лидер у индустрији у погледу информационе безбедности, обезбеђујући највиши ниво заштите наших информационих средстава и ресурса.

Мисија

Заштити интегритет, доступност и поверљивост информационих ресурса кроз континуирано унапређење наших безбедносних политика, процедура и технологија, уз истовремено усклађивање са регулаторним захтевима и индустријским стандардима.

Пример Стратешког плана информационе безбедности

Стратешки циљеви

1. Усклађеност са Међународним Стандардима

Постићи и одржати сертификацију по ISO/IEC 27001 стандарду до краја првог квартала прве године.

2. Управљање Ризицима

Развити и имплементирати свеобухватан програм управљања ризицима који идентификује, процењује и ублажава потенцијалне безбедносне претње.

3. Свест о Безбедности

Спровести редовне обуке и програме освешћивања за све запослене, с циљем смањења инцидената изазваних људским фактором за 50% у року од три године.

4. Отпорност на Инциденте

Развити и тестирати планове одговора на инциденте и опоравка од катастрофа, осигуравајући способност брзог опоравка пословања у случају безбедносних инцидената.

Пример Стратешког плана информационе безбедности

5. Технолошко Унапређење

Имплементирати најновије безбедносне технологије које укључују следеће

1. Имплементирати најновије безбедносне технологије које укључују напредну детекцију претњи и аутоматизовани одговор на инциденте.

2. Заштита од ransomware-a

► Endpoint Protection: Имплементација напредних решења за заштиту крајњих тачака које укључују анализу понашања корисника и машинско учење за детекцију и блокирање ransomware-a пре него што изазове штету.

► Backup и Recovery: Редовна израда сигурносних копија свих критичних података на изолованим локацијама како би се осигурала брза обнова података у случају ransomware напада.

3. Заштита података о личности и кредитним трансакцијама

► Data Encryption: Имплементација енкрипције за све осетљиве податке, како у мировању тако и у преносу, за заштиту података о личности и трансакцијама.

► Access Controls: Ограничење приступа подацима о личности и трансакцијама само за овлашћене кориснике помоћу строге аутентификације и управљања идентитетима.

► Data Loss Prevention (DLP): Имплементација DLP решења за праћење, детекцију и блокирање неауторизованог приступа или преноса осетљивих података.

Пример Стратешког плана информационе безбедности

5. Технолошко Унапређење

Имплементирати најновије безбедносне технологије које укључују следеће

4. Заштита од финансијске крађе на онлине трансакцијским системима

- Fraud Detection Systems: Имплементација система за детекцију превара који користе аналитику и машинско учење за идентификацију сумњивих трансакција у реалном времену.
- Secure Payment Gateways: Употреба сигурних платних гејтвеја који подржавају напредне безбедносне протоколе као што су 3D Secure и токенизација за додатну заштиту трансакција.
- Regular Security Audits: Редовно извођење безбедносних ревизија и тестирања пенетрације на трансакцијским системима за идентификовање и адресирање потенцијалних безбедносних слабости.

Пример Стратешког плана информационе безбедности

Кључни показатељи успеха (KPI)

1. Усклађеност са стандардима:

Постотак усклађености са ISO/IEC 27001. На крају прве године да усклађеност буде 80%.

2. Индекс ризика:

Смањење укупног ризика по годишњем индексу ризика за 20% сваке године.

3. Проценат обука међу запосленима:

100% запослених прошло кроз обуку из информационе безбедности сваке године.

4. Време опоравка након инцидента:

Просечно време потребно за опоравак пословних операција након инцидента не сме премашити 4 сата.

5. Детекција и одговор:

Смањење времена потребног за детекцију и реаговање на безбедносне инциденте за 30% годишње.

Пример Стратешког плана информационе безбедности

Имплементација Плана

- ▶ **Квартал 1, Година 1:** Ревизија тренутних безбедносних политика и процедура, почетак сертификације ISO/IEC 27001.
- ▶ **Квартал 2, Година 1:** Имплементација обука за запослене и лансирање кампање освешћивања. Имплементација Secure Payment Gateways решења.
- ▶ **Квартал 3, Година 1:** Увођење нових технолошких решења за back-up/recovery, као и детекцију и одговор на претње.
- ▶ **Квартал 4, Година 1:** Први годишњи преглед, као и Security Audit и ажурирање програма управљања ризицима.

- ▶ **Година 2:**
Имплементација access controls, end-point и DLP решења
Унапређењу и проширењу планова за одговор на инциденте и опоравак од катастрофа.

- ▶ **Година 3:**
Имплементација Data encryption и Fraud detection решења
Евалуација постигнутих резултата и прилагођавање стратешких циљева и KPI-а на основу промена у пословном окружењу и технолошком напретку.

Технике стратешког управљања и анализе – Континуитет пословања

Plan	Svrha	Opseg
Plan za kontinuitet poslovanja (BCP)	Definiše procedure za održavanje osnovnih poslovnih operacija tokom oporavka od značajnog prekida	Bavi se poslovnim procesima; IT se bavi samo podrškom za poslovne procese
Plan za oporavak poslovanja (BRP)	Definiše procedure za brz oporavak poslovnih operacija nakon katastrofe	Bavi se poslovnim procesima; nije fokusiran na IT; IT se bavi samo podrškom za poslovne procese
Plan kontinuiteta operacija (COOP)	Definiše procedure i preduslove za održavanje suštinskih, strateških funkcija organizacije na alternativnoj lokaciji do 30 dana	Bavi se najkritičnijim procesima organizacije; obično se piše na nivou centrala; nije fokusiran na IT
Plan za krizne komunikacije (CCP)	Definiše procedure za distribuciju izveštaja o statusu krizne situacije zaposlenima i javnosti	Bavi se komunikacijama sa osobljem i javnošću; nije fokusiran na IT
Plan za odgovor na sajber incidente (CIRP)	Pruža strategije za detekciju, reagovanje i ograničavanje posledica zlonamernih sajber incidenata	Fokusiran je na odgovore informacione sigurnosti na incidente koji utiču na sisteme i/ili mreže
Plan za oporavak od katastrofa (DRP)	Pruža detaljne procedure za olakšavanje oporavka sposobnosti na alternativnoj lokaciji	Često fokusiran na IT; ograničen na glavne poremećaje s dugoročnim efektima
Plan za hitne intervencije (ERP)	Pruža koordinisane procedure za minimiziranje gubitka života ili povreda i zaštitu od štete na imovini kao odgovor na fizičku pretnju	Fokusiran je na osoblje i imovinu specifičnu za datu lokaciju; nije baziran na poslovnom procesu ili funkcionalnosti IT sistem

Управљачки оквир - хијерархија

► Политике - ОБАВЕЗНЕ

Доносе се од стране високог менаџмента, нису детаљне. Дефинишу принципе, а не начин реализације принципа

► Стандарди - ОБАВЕЗНИ

Описују специфичну употребу технологије (нпр. Сви лаптопи морају имати инсталиран Windows 11 - 64 bit, BitLocker итд.)

► Смернице - Нису обавезне

Препоруке, на који начин нека технологија може бити имплементирана или конфигурисана

► Процедуре - ОБАВЕЗНЕ

Детаљан опис процеса, корак-по-корак, са додељеним одговорностима. Тиче се специфичне технологије или активности



Управљачки оквир - хијерархија

Ниво политика (Нивои 1 - 3)

- Ниво 1.

Глобална, креирање свеобухватне визије и правца организације (Code of conduct). Нпр. власништво над подацима, адекватно руковање подацима, забрана изношења и дељења података итд.

- Ниво 2.

Политика фокусирана на део организације или одређену област пословања или система који се опет односи на већи део компаније. Мења се чешће по потреби (често када се технологија промени).

- Ниво 3.

Специфична политика која се односи на појединачну апликацију, решење, део система. Релативно често се мења.

Вежба 2

- Подела у тимове

Тимови по два (или три члана)

- Додела тема тимовима

- Политика потребе интернета, Политика употребе е-маил-а, Политика контроле приступа
- Политика мобилних уређаја, Политика чистог стола и празног екрана, Политика заштите од малвера
- Политика коришћења носача података, политика удаљеног приступа, политика физичке безбедности сервер сале
- Политика back-up-а и архиве, Политика криптографије, Политика управљања закрпама (Patch management)

Вежба 2

Свака појединачна политика не би требало да буде дужа од једне А4 странице (фонт 10-12) – идеално пола странице и требало би да садржи следећа 4 сегмента:

- Тема – кратак опис сврхе и теме политике (кратко, сажето и треба да прикаже суштину политике)
- Опсег – детаљнији опис опсега и принципа политике (на кога се односи политика, на које делове организације, опис основних принципа који дефинишу политику)
- Одговорност – одговорност за спровођење политике (по позицијама)
- Последице неусклађености са политиком – мере/дисциплинске казне за неусклађеност са захтевима политике