

Управљање безбедношћу и ризицима

Управљање ризицима информационе безбедности



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

Класификација података

Лабеле (ознаке): Информациона или ИТ средства имају ознаке које су им додељене.

- Ознаке указују на одређена права приступа и коришћења информација или ИТ средстава.
- Ове ознаке често могу бити грануларније, нпр. уместо само „Строго поверљиво“, може да стоји „Строго поверљиво - Државна тајна“.

Дозвола: Информациона средства имају дозволу (Clearance) који им је додељен.

- Што је дозвола већа, већа је потреба за додатним и дубинском личним проверама особе (увек у војним структурама), није обавезно у пословном окружењу.

Класификација података - Пример

Top Secret (TS) - Exceptionally grave damage Weapon blueprints, theater or war plans, espionage data.	Confidential - Exceptionally grave damage Proprietary information, trade secrets, source code, anything that gives us a competitive advantage.
Secret (S) - Serious damage Troop plans, deployment plans, plans not included in TS plans, reports on shortages or weaknesses.	Private - Serious damage PHI, PII, financial data, employee data, payroll.
Confidential (C) - Damage Intelligence reports, operational or battle reports, mobilization plans.	Sensitive - Damage Networking diagrams, IP assignments, system and software specific information.
Unclassified (U) Available upon request, does not need a particular classification or has been declassified.	Public Websites, advertisements, any information we make publicly available.

Војна (некад и државна) институција

Приватна корпорација

Класификација података - Принципи

Формално одобрење за приступ

- Документ, којим власник података одобрава приступ подацима одређеној особи - субјекту
- Веома важно: Субјект мора разумети све одговорности који произилазе из приступа подацима и последица које следе ако подаци буду компромитовани, изгубљени или уништени.
- Само зато што имате приступ не значи да вам је дозвољено да користите податке како год хоћете
- Потребан вам је валидан разлог за приступ подацима. Ако га немате, можете бити отпуштени/тужени/затворени/кажњени.

Принцип „Најмање могуће привилегије“

- Корисници имају минимално неопходан приступ за обављање својих радних задатака.

Класификација података - Осетљиве информације и медији

Руковање подацима

- Подацима треба да рукују само одобрени и проверени појединци
- Политике о томе како, где, када и зашто се са подацима рукује

Складиштење података

- Чувани у сигурном, климатизовано контролисаном објекту
- Подаци не треба да буду чувани дуже од периода коришћења или преко законских лимита
- Свака индустрија има своје регулативе - политике компанија могу се разликовати од законских захтева.

Класификација података – Улоге и одговорности

Сви чланови организације имају јединствене улоге и одговорности које се тичу заштите података.

Топ менаџмент

- Извршни директори креирају политике које дефинишу класификацију и заштиту података.

Власници података

- Додељују лабеле (ознаке) осетљивости, фреквенцију бекапа и остале атрибуте по потреби

Старатељи (Custodian) података

- Технички запослени који брину о подацима (back-up, рестаурације података, управљање закрпама, конфигурисање система). Поступају по упутствима власника података.

Власник система

- Често менаџер центра података или менаџер инфраструктуре

Контролори и обрађивачи података

- Контролори креирају и управљају осетљивим подацима у организацији
- Обрађивачи управљају подацима за контролоре (нпр. екстернализација)

Класификација података – Улоге и одговорности

Администратори безбедносних система

- Одговорни за firewall, IPS (Системи за превенцију напада), IDS (Системи за детекцију напада), безбедносне закрпе, креирање налога и додељивање приступа подацима по упутствима власника података.

Супервизори

- Директно одговорни за праћење, помоћ и едукацију корисника - потребно је да обавесте администратора безбедности ако дође до било каквих промена у статусу запослења корисника, правима приступа корисника или било којим другим релевантним променама у статусу запосленог.

Корисници

- Корисници података. Свест корисника мора бити на високом нивоу - треба да знају шта је прихватљиво а шта не, и последице за непоштовање политика, процедура и стандарда.

Ревизори

- Одговорни за преглед и уверавање да су безбедносне политике исправно имплементиране, да их се запослени придржавају и да пружају потребну заштиту.

Управљање ризицима – Основни задаци

Детаљна анализа ресурса информационог система са аспекта сајбер ризика

- Поверљивост, интегритет и доступност (колико су угрожени?)

Квантификација идентификованих ризика

- У циљу израде анализе трошкова и користи и плана третмана ризика

Обезбедити адекватну сегрегацију дужности у процесу процене ризика

- Избегавати ситуацију да администратор или CISO процењује ризик или самостално одређује мере

Креирање адекватног плана третмана ризика

- Дефинисање мера за ублажавање ризика

Управљање ризицима – Основни кораци

1. Одређивање обима анализе ризика
2. Попис информационих средстава
3. Процена важности средстава
4. Процена претњи и рањивости средстава
5. Процена вероватноће
6. Вредновање ризика
7. Третман ризика
8. Документовање и извештавање

Управљање ризицима – Одређивање обима анализе

- Анализа се може извршити за целокупно ИТ решење или за појединачне ИТ компоненте
- Полази се од процеса који постоје у организацији
- Дефинисати делове организације или део пословних процеса за који се врши анализа ризика

Управљање ризицима – Попис средстава

- **Окружење и општа инфраструктура** (Просторије, електричне инсталације, водоводне инсталације, противпожарна заштита)
- **Људски ресурси** (запослени, клијенти, шира заједница)
- **Физичка ИТ опрема** (физички рачунари, сервери, мрежна инфраструктура, комуникациона опрема, УПС, штампачи, пројектори, преносни медији, опрема за контролу уласка, остала техничка опрема)
- **Софтверска средства** (апликације, системски софтвер – ОС, развојни софтвер, ОТ – индустријски софтвер)
- **Информациона средства/добра у ужем смислу** (базе података, Филе сервери, физичке копије, процедуре-политике-упутства)

Управљање ризицима – Процена средстава

➤ За свако средство се дефинишу следећи подаци:

- Идентификација (ИД, назив, група)
- Кратак опис
- Старатељ средства
- Локација средства
- Оцена важности средства

➤ За свако средство се дефинишу следећи подаци:

- П/И/Д је безначајна - вредност 0
- П/И/Д је мало значајна - вредност 1
- П/И/Д је значајна - вредност 2
- П/И/Д је врло значајна - вредност 3
- П/И/Д је кључна, од суштинске важности - вредност 4

Управљање ризицима – Процена претњи и рањивости средстава

Оцена претње

Критеријуми претње

XN - нема утицаја

На посматрану карактеристику П/И/Д средства, претња нема утицаја.

N - Ниска

На посматрану карактеристику П/И/Д, претња има само мањи утицај:

П - догоди се откривање појединих података.

И - подаци су у начелу беспрекорни, осим неколико изузетака.

Д - доступност је изгубљена само на кратко време, корисници то скоро да не примете.

S - Средња

На посматрану карактеристику П/И/Д средства претња утиче на начин, да је карактеристика делимично угрожена:

П - Подаци су откривени, али у мањем обиму.

И - Подаци су спорни, али у ограниченом обиму. Грешка се брзо примети и отклони исти дан.

Д - Доступност је изгубљена само на кратко време, пословање је ометано највише 2 сата.

V - Висока

На посматрану карактеристику П/И/Д средства претња утиче на начин, да је карактеристика суштински угрожена:

П - Подаци су откривени у целости, или у значајном обиму.

И - Подаци су спорни у целости, или у значајном обиму. Грешка се примети касно, отклањање грешке траје дуже од 1 дана.

Д - Доступност је изгубљена за дуже време. Пословање је ометано више од 2 сата.

Управљање ризицима - Процена претњи и рањивости средстава

Ниво претње	Низак			Средњи			Висок		
Ниво рањивости	Низак	Средњи	Висок	Низак	Средњи	Висок	Низак	Средњи	Висок
Утицај - ниво озбиљности нежељеног догађаја	N - 1	N - 1	S - 2	N - 1	S - 2	V - 3	S - 2	V - 3	V - 3

Управљање ризицима – Процена вероватноће

➤ Процена вероватноће, односно учесталости претње

- V1 - врло ниска (сваких 10 година или ређе). Вредност 1
- V2 - ниска (сваке 2 године). Вредност 2
- V3 - средња (сваких годину дана). Вредност 3
- V4 - висока (сваких 6 месеци). Вредност 4
- V5 - врло висока (сваких месец дана). Вредност 5
- V6 - изузетно висока (сваки дан). Вредност 6

Управљање ризицима – Вредновање ризика

➤ Формула за израчунавање вредности ризика

Ризик = Важност средства x Вредност утицаја x Учесталост претње

➤ Оцене ризика

- D - бела боја. Вредности ризика < 6
- C - зелена боја. Вредности ризика ≥ 6 и < 12
- B - жута боја. Вредности ризика ≥ 12 и < 32
- A - црвена боја. Вредности ризика ≥ 32

Управљање ризицима – Вредновање ризика

Оцене ризика

➤ А: неприхватљиви ризици

Резултат анализе разматра високи Орган организације (IT SEC Steering Committee, Одбор за ризике). Одмах треба припремити план мера за савладавање ризика (ради се посебна седница за тај ризик). Ризик се евидентира у централном организационим регистру ризика.

➤ В: условно неприхватљив ризик

Резултат анализе разматра високи Орган организације (IT SEC Steering Committee, Одбор за ризике). За условно неприхватљиве ризике је потребно припремити план мера за савладавање ризика. Ризик се евидентира у централном организационим регистру ризика.

➤ С: прихватљив ризик

Ризик постоји, али у прихватљивим границама. Ризик се прати на нивоу појединачних пословних одељења и CISO функције.

➤ D: нема ризика, или је минималан

Мере нису потребне.

Управљање ризицима - Вредновање ризика

Важност средства	Вредност утицаја	Учесталост претње (фреквенција инцидента)					
		V1 - 1 Врло ниска	V2 - 2 Ниска	V3 - 3 Средња	V4 - 4 Висока	V5 - 5 Врло висока	V6 - 6 Изузетно висока
1 - малозначајно	N - 1	1 (D)	2 (D)	3 (D)	4 (D)	5 (D)	6 (C)
	S - 2	2 (D)	4 (D)	6 (D)	8 (C)	10 (C)	12 (B)
	V - 3	3 (D)	6 (C)	9 (C)	12 (B)	15 (B)	18 (B)
2 - значајно	N - 1	2 (D)	4 (D)	6 (C)	8 (C)	10 (C)	12 (B)
	S - 2	4 (D)	8 (C)	12 (B)	16 (B)	20 (B)	24 (B)
	V - 3	6 (C)	12 (B)	18 (B)	24 (B)	30 (B)	36 (A)
3 - врло значајно	N - 1	3 (D)	6 (C)	9 (C)	12 (B)	15 (B)	18 (B)
	S - 2	6 (C)	12 (B)	18 (B)	24 (B)	30 (B)	36 (A)
	V - 3	9 (C)	18 (B)	27 (B)	36 (A)	45 (A)	54 (A)
4 - кључно/од суштинске важности	N - 1	4 (D)	8 (C)	12 (B)	16 (B)	20 (B)	24 (B)
	S - 2	8 (C)	16 (B)	24 (B)	32 (A)	40 (A)	48 (A)
	V - 3	12 (B)	24 (B)	36 (A)	48 (A)	60 (A)	72 (A)

Управљање ризицима – Третман ризика

Могући приступи код третмана ризика

- **Прихватање ризика:** прихватају се ризици чији су могући губици нижи од трошкова њиховог спречавања. Приступ је обично прихватљив за ризике ниске фреквенције (вероватноће) и ниског износа губитка (утицаја).
- **Смањивање ризика:** покушава се смањити фреквенција и/или утицај настанка ризика, што је могуће успостављањем одговарајућих контролних активности, постављањем правила у спровођењу процеса и слично. Овај начин савладавања ризика се користи претежно код ризика чија је вероватноћа настанка висока, а утицај низак. Други вид смањивања ризика је предузимање дефинисаних активности како би смањиле последице уколико се ризик ипак појави.
- **Избегавање ризика:** ризик је могуће избећи на начин, да се одстрани узрок ризика, нпр. не вршити одређене ризичне активности у оквиру организације. Избегавање ризика често није реални избор, уколико рецимо привредна организација хоће да сачува конкурентност на тржишту.
- **Пренос ризика:** ради се о преносу ризика на институцију за осигурање или екстерног извођача. Услов заштите од ризика је да је то врста ризика за коју постоји могућност осигурања. Организација може за одређену делатност узети екстерне извођаче, који имају више искуства, знања или других ресурса и могу обезбедити боље чување информација. При томе је битно нагласити да организација и у том случају остаје одговорна за законито, безбедно и транспарентно пословање.

ДОДАТАК: Управљање ризицима – База претњи и рањивости

Kategorija	Prijetnja	Ranjivost
Bezbednost - Cyber napadi i drugi eksterni napadi na informacijske sisteme organizacije	Ransomware napadi: Napadači koriste ransomware softver kako bi šifrovali podatke žrtve, zahtevajući otkupninu za dešifrovanje.	Slabe sigurnosne postavke, nedostatak redovnih ažuriranja softvera.
	Phishing napadi: Prevaranti šalju lažne e-poruke koje izgledaju legitimno kako bi naterali korisnike da otkriju osetljive informacije poput lozinki ili brojeva kreditnih kartica.	Niska svest korisnika o prevarama i slaba edukacija o sajber bezbednosti.
	Supply Chain Attacks: Napadači kompromituju legitimne softverske dobavljače kako bi distribuirali maliciozni kod kroz njihove proizvode.	Nedostatak sigurnosnih provera kod trećih strana i dobavljača.
	Zero-day pretnje: Ranjivosti u softveru koje su nepoznate proizvođaču i koje napadači mogu iskoristiti pre nego što se izdaju zakrpe.	Brz razvoj i distribucija novih softverskih verzija bez adekvatnog testiranja.
	Distributed Denial of Service (DDoS) napadi: Napadi koji preplave mrežu ili server ogromnim brojem zahteva, ometajući ili potpuno onemogućavajući njihove usluge.	Neadekvatna zaštita mrežnih infrastruktura i servera.
	Malware napadi: Zlonamerni softver koji može ukrasti podatke, oštetiti sisteme ili omogućiti neovlašćen pristup.	Nedostatak odgovarajućih antivirusnih i anti-malware rešenja.
	Credential stuffing napadi: Napadači koriste ukradene korisničke akreditive da bi pristupili računima na različitim platformama.	Ponovna upotreba istih lozinki na različitim sajtovima i servisima.
	IoT (Internet of Things) ranjivosti: Uređaji povezani na internet koji često imaju slabe sigurnosne mere, omogućavajući napadačima da ih kompromituju.	Nedostatak sigurnosnih ažuriranja i slabe sigurnosne postavke kod IoT uređaja.
	Advanced Persistent Threats (APT): Ciljani napadi koje izvode sofisticirani napadači sa ciljem dugotrajnog infiltriranja i prikupljanja podataka.	Nedostatak naprednih detekcijskih sistema i nedovoljna obuka zaposlenih u prepoznavanju kompleksnih napada.

ДОДАТАК: Управљање ризицима – База претњи и рањивости

Kategorija	Prijetnja	Ranjivost
Bezbednost – Neadekvatna fizička i logička bezbednsot	Neadekvatna logička (interna) bezbednost sistema	Neautorizovan pristup kritičnim dijelovima informacionog sistema iz mreže banke, u svrhu zloupotrebe.
		Neautorizovane izmjene nad informacionim sistemom uslijed neadekvatnog upravljanja pristupom, procedura i prakse.
		Sigurnosne prijetnje uslijed nedostatka svijesti o sigurnosnim rizicima, gdje zaposleni ne razumiju, odbijaju iii ne poštuju politike sigurnosti.
		Neautorizovano pohranjivanje iii iznošenje, objavljivanje povjerljivih podataka izvan banke.
	Neadekvatna fizička bezbednost informacionog sistema	Zloupotreba iii krađa resursa informacionog sistema putem fizičkog pristupa, koja može prouzrokovati oštećenja, gubitak resursa i podataka odnosno prouzrokovati druge prijetnje.
		Namjerno iii slučajno fizičko oštećenje resursa informacionog sistema prouzrokovano terorizmom, nesrećama, neadekvatnom upotrebom od strane zaposlenih banke iii pružaoca usluga i slično.
		Nedovoljna fizička zaštita od prirodnih nepogoda koja može prouzrokovati djelimično iii kompletno uništenje resursa informacionog sistema.

ДОДАТАК: Управљање ризицима – База претњи и рањивости

Kategorija	Prijetnja	Ranjivost
Dostupnost i kontinuitet	Neadekvatno upravljanje kapacitetom informacionog sistema	Nedostatak resursa (hardver, softver, zaposleni, pružaoci usluga i drugo) može prouzrokovati nemogućnost održavanja sistema na potrebnom nivou, poteškoće u ispunjavanju poslovnih potreba, prekide u radu sistema i pojavu grešaka.
	Greške u radu informacionog sistema	Nedostupnost sistema uslijed hardverskih grešaka.
		Nedostupnost sistema uslijed grešaka u softveru.
	Neadekvatno planiranje kontinuiteta rada i oporavka informacionog	Greške u planiranju, arhitekturi i testiranju kontinuiteta rada i oporavka informacionog sistema.
	Cyber napadi koji uzrokuju prekid i usporenje rada informacionog sistema	Razni vidovi napada, koji mogu rezultirati prevelikim opterećenjem informacionog sistema i mreže, prouzrokujući nedostupnost, sporost i ostale probleme u radu i dostupnosti sistema korisnicima.
		Napadi na komunikacione linije i ostale vidove komunikacije sa ciljem prikupljanja informacija i zloupotrebe.
Upravljanje izmjenama		Neautorizovano pohranjivanje i iznošenje, objavljivanje povjerljivih podataka izvan banke.
	Neadekvatna kontrola nad razvojem i izmjenama informacionog sistema	Incidenti prouzrokovani nedetektovanim greškama i ranjivostima koje su nastale kao rezultat izmjena nad sistemom.
	Neadekvatna arhitektura informacionog sistema	Neadekvatno upravljanje arhitekturom informacionog sistema prilikom njegovog dizajna, razvoja i održavanja, koje može vremenom rezultirati kompleksnom, otežanom, skupom održavanju i upravljanju, te koje više nije u mogućnosti zadovoljiti poslovne potrebe.
	Neadekvatno upravljanje životnim ciklusom i nadogradnjama informacionog sistema	Neadekvatno održavanje registra resursa informacionog sistema, upravljanja životnim ciklusom i nadogradnjama, može voditi ka nepravovremenoj i neadekvatnoj nadogradnji, ažuriranju informacionog sistema, te sistemu koji ne može zadovoljiti poslovne potrebe.

ДОДАТАК: Управљање ризицима – База претњи и рањивости

Kategorija	Prijetnja	Ranjivost
Integritet podataka	Greške pri upravljanju i obradi podataka	Uslijed sistemskih, komunikacijskih i/ili aplikativnih grešaka, pogrešno procesiranih podataka, procesa prijenosa i unosa podataka, podaci mogu biti korumpirani i izgubljeni.
	Neadekvatan dizajn kontrola na validaciji podataka.	Greške koje se odnose na nedostatak neefikasnost automatizovanih kontrola unosa i prihvata podataka, transfera podataka, procesiranja i izlaznih kontrola.
	Neadekvatna kontrola nad izmjenom podataka	Greške u podacima uslijed nedostatka kontrola nad izmjenama podataka.
	Neadekvatno dizajnirana arhitektura podataka, tok podataka, model podataka i rječnik podataka	Neadekvatno upravljanje arhitekturom podataka i modelom, može rezultirati nekonzistentnošću podataka.
Eksternalizacija	Neadekvatne mjere zaštite i upravljanje od strane pružaoca usluga	Nedostupnost kritičnih eksternalizovanih servisa, telekomunikacionih servisa i usluga; gubitak i korupcija kritičnih/osjetljivih podataka koje su povjerene pružaocu usluga.
	Neadekvatno upravljanje eksternalizacijom od strane banke	Značajna degradacija sistema i greške uslijed nedovoljne pripremljenosti kontrolnih procesa kod pružaoca usluga; neadekvatno upravljanje eksternalizacijom može rezultirati u nedostatku odgovarajućih znanja i kapaciteta u cilju identifikacije, pristupa, umanjenja i nadzora nad rizikom informacionih sistema i ograničivanju bančnih operativnih kapaciteta.
	Neadekvatne kontrole sigurnosti informacionog sistema kod pružaoca usluga	Napadi hakera na sisteme pružaoca usluga, sa direktnim uticajem na izvršavanje eksternalizovanih aktivnosti i/ili pristup kritičnim/povjerljivim informacijama kod pružaoca usluga; osoblje pružaoca usluga ima omogućen neautorizovan pristup kritičnim/osjetljivim podacima banke koji se nalaze kod pružaoca usluga.