

Управљање безбедношћу и ризицима

Вежба 3 – процена ризика информационе безбедности



Бранко Суботић, Консултант

Контакт: ~~branko.subotic@rs.ey.com~~ → branko.subotic@cedars.rs

Вежба 3 - Увод

Компанија АБЦ врши годишњу процену ризика информационе безбедности, како за потребе усклађивања са Стратегијом Компаније, тако и за потребе идентификације и процене ризика и дефинисања потребних мера заштите. У овој процени учествују:

1. **ИТ Сектор**, који је задужен за попис информационих средстава, али такође учествује у идентификацији и процени релевантних претњи и ризика.
2. **Власници пословних процеса** и информационих средстава, који су задужени за процену важности информационих средстава, те финалну процену утицаја
3. **CISO (Функција Информационе безбедности)**, као координатор целокупног процеса и неко ко је задужен за помогне све учеснике у идентификацији и процени свих кључних елемената.

Вежба 3 - Задатак

Ваш задатак је преузмете све три улоге и урадите следећи:

1. Да урадите процену важности информационих средстава, у оквиру документа Вежба 3, sheet Информациона средства, а на основу следећег:
 - Методологије процене ризика, страна 6
 - Информација које су доступне у оквиру документа Вежба 3, sheet Информациона средства
2. Да идентификујете релевантне претње и рањивости, у оквиру документа Вежба 3, sheet Оцена ризика (колоне Оцена претње и Оцена рањивости), а на основу следећег:
 - Методологије процене ризика, страна 7
 - Информација које су доступне у оквиру документа Вежба 3, sheet Информациона средства
 - Информација које су доступне у оквиру овог документа Преглед генеричких претњи и рањивости (страна 6 овог документа)
 - Информација које су доступне у оквиру овог документа Резултати прегледа Интерне ревизије за 2023. годину (страна 5 овог документа)

Вежба 3 - задатак

Ваш задатак је следећи:

3. Да оцените вероватноћу, у оквиру документа [Вежба 3, sheet Оцена ризика \(колона Оцена вероватноће\)](#), а на основу следећег:
 - Методологије процене ризика, страна 9
 - Информација које су доступне у оквиру документа [Вежба 3, sheet Преглед инцидента](#)
 - Информација које су доступне у оквиру овог документа [Резултати прегледа Интерне ревизије за 2023. годину \(страна 5 овог документа\)](#)
 - Додатна информација за Zero-day нападе: Иако није идентификован ни један овакав напад у току 2023. године, на основу доступног истраживања релевантне консултантске фирме, процена је да се овакав напад може десити једном у две године за компаније које раде у нашем индустријском сектору
4. Да оцените утицај, ризик и категорију ризика, у оквиру документа [Вежба 3, sheet Оцена ризика \(колоне Укупна оцена утицаја, Оцена ризика и Категорија ризика\)](#), а на основу следећег:
 - Методологије процене ризика, стране 8, 10, 11 и 12

Вежба 3 – Резултати прегледа Интерне ревизије у 2023. години

Интерна ревизија је спровела ревизију Компанију у области информационе безбедности и уочила следеће недостатке:

1. Уочене су слабости у процесу управљања системским конфигурацијама ЕРП решења на апликативном и ДБ нивоу
2. И даље је присутан значајан део запослених којима свест о важности информационе безбедности није на високом нивоу
3. Анитвирусно решење се није адекватно ажурирало у дужим временским периодима у току 2023. године. У оквиру ревизије је идентификовано и да се 35 malware инфилтрација у току 2023. уопште није идентификовало и забележило у прегледу инцидената
4. Уочена су одступања у оквиру процеса управљања корисничком администрацијом на апликативним и мрежним системима
5. Уочене су слабости у процесу управљања конфигурацијама на мрежним елементима LAN и WAN мреже
6. Нису уочена одступања по питању физичке безбедности

Вежба 3 – Преглед генеричких претњи и рањивости

Kategorija	Prijetnja	Ranjivost
Bezbednost - Cyber napadi i drugi eksterni napadi na informacioni sistem 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.
	OT (Operational Technology) ranjivosti: Uređaji koji se koriste u industrijskoj proizvodnji, i preko kojih se vrši generisanje i razmena industrijskih i proizvodnih podataka.	Nedostatak sigurnosnih ažuriranja i slabe sigurnosne postavke kod OT uređaja.
	Neadekvatna logička (interna) bezbednost sistema	Neautorizovan pristup kritičnim dijelovima informacionog sistema iz mreže organizacije, u svrhu zloupotrebe.
	Neadekvatna fizička bezbednost informacionog sistema	Zloupotreba ili krađa resursa informacionog sistema putem fizičkog pristupa, koja može prouzrokovati oštećenja, gubitak resursa i podataka odnosno prouzrokovati druge prijetnje.