HRVATSKA
REVIZORSKA
KOMORA

Stručno savjetovanje ovlaštenih revizora u organizaciji Hrvatske revizorske komore

za 2022. godinu

HRVATSKA
REVIZORSKA
KOMORA

Kibernetička sigurnost i revizija

Tihana Bažant i Ratko Drča

Napomena

Sadržaj ovog prezentacijskog materijala je informativnog karaktera. Upotreba prezentacijskog materijala ne oslobađa korisnika od poduzimanja potrebnih mjera predostrožnosti prije njegove uporabe, odnosno ne oslobađa korisnika od obveze primjene izvornih zakonskih odredbi i pravila struke, s toga se Hrvatska revizorska komora i autor prezentacijskog materijala ne mogu smatrati odgovornima prilikom uporabe ili u vezi s uporabom sadržaja koji se nalazi u prezentacijskom materijalu.

Uporaba sadržaja i podataka iz ovog prezentacijskog materijala dopuštena je pod uvjetom navođenja izvora podataka, osim u slučajevima kada je naznačeno drugačije.

Sadržaj

Što je kibernetička sigurnost?

*Kibernetička sigurnost je **primjena tehnologija, procesa i kontrola** za zaštitu sustava, mreža, programa, uređaja i podataka od kibernetičkih napada. Cilj joj je **smanjiti rizik** od **kibernetičkih napada** i zaštititi od neovlaštenog iskorištavanja sustava, mreža i tehnologija.*

Revizija i kibernetički rizici – MRevS315

Dodatak 5

- Ranjivost IT aplikacija, baza podataka I drugih aspekata IT okruženja od kibernetičkih rizika – ***Jedan od faktora za razumijevanje i procjenu IT okruženja***

Dodatak 6

- Svaki od IT rizika sadržava kibernetičku komponentu, a pogotovo:
  - Neovlašteni pristup podacima
  - Ovlasti šire od zahtjevanih
  - Neovlaštene promjene podataka
  - Gubitak i/ili nemogućnost pristupa podacima kad je potrebno

Revizija i kibernetički rizici – postupanje

*Ako je identificirana informacija o povredi sigurnosti revizor redovno razmatra **opseg** do kojeg takva povreda ima potencijal **utjecati na financijsko izvještavanje**. Ako može utjecati na financijsko izvještavanje, revizor može odlučiti razumjeti i testirati povezane kontrole radi **utvrđivanja mogućeg utjecaja** ili **opsega potencijalnih pogrešnih prikazivanja** u financijskim izvještajima ili može utvrditi da je subjekt pružio adekvatne informacije u vezi s takvom povredom sigurnosti.*

Revizija i kibernetički rizici – Utvrđivanje kibernetičkog incidenta

Primjeri procedura za stjecanje razumijevanja da li se kibernetički incident dogodio:

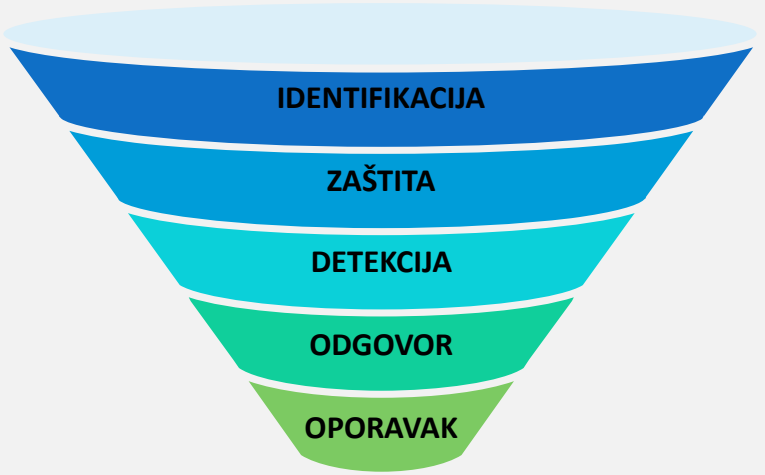
- *Razgovor s Voditeljem sigurnosti ili drugom osobom odgovornom za upravljanje kibernetičkom sigurnošću*
- *Razgovor s voditeljima IT-a i Financija*
- *Pregled izvještaja interne revizije i zapisnike nadzornog odbora te neovisnih izvora (mediji i sl.)*

Okvir upravljanja kibernetičkom sigurnošću - primjer

NIST Cybersecurity Framework Version 1.1

- Stvoren kako bi:
  - Integrirao funkcije i poboljšao komunikaciju
  - Optimizirao upravljanje operativnim rizikom
  - Približio prakse poslovnom okruženju, upravljanju i strategijama upravljanja rizikom
  - Olakšao odabir prioriteta aktivnosti za unaprjeđenje

- Navedeni okvir pruža okvir za implementaciju, usporedbu i reviziju politika, procedura, postupaka i tehnologija zastupljenih unutar upravljanja kibernetičkom sigurnošću.

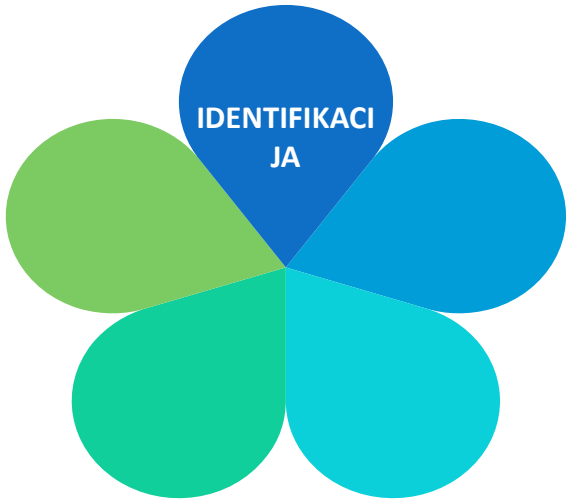


Provedba revizije kibernetičke sigurnosti

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management & Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Provedba revizije kibernetičke sigurnosti



Primjeri revidiranih ciljeva:

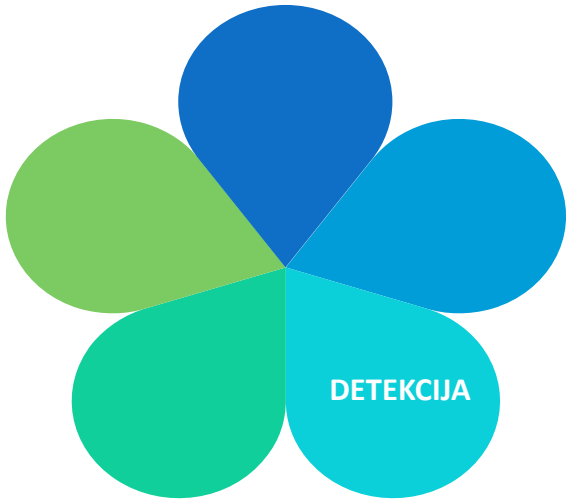
- *Kako je subjekt izvršio identifikaciju fizičke i softverske imovine za uspostavljanje programa upravljanja imovinom?*
- *Jesu li politike kibernetičke sigurnosti identificirane i formalizirane?*
- *Kako je strategija upravljanja rizicima definirana unutar organizacije?*

Provedba revizije kibernetičke sigurnosti

Primjeri revidiranih ciljeva:

- *Kako je zaštita podataka implementirana u svrhu osiguravanja povjerljivosti, integriteta i dostupnosti?*
- *Na koji način se upravlja tehnologijama za zaštitu kako bi se osigurala sigurnost i otpornost sustava i pomoćnih alata?*
- *Kako je subjekt proveo podizanje svijest o kibernetičkoj sigurnosti i obuku unutar organizacije?*

Provedba revizije kibernetičke sigurnosti



Primjeri revidiranih ciljeva:

- *Kako su definirane mogućnosti sigurnosnog kontinuiranog nadzora za praćenje kibernetičkih događaja?*
- *Kako se osigurava otkrivanje anomalija i događaja te razumijevanje njihovog potencijalnog utjecaja?*
- *Provodi li se provjera učinkovitosti zaštitnih mjera?*

Provedba revizije kibernetičke sigurnosti

Primjeri revidiranih ciljeva:

- *Kako se osigurava da se procesi planiranja odgovora provode tijekom i nakon incidenta?*
- *Kako se upravlja komunikacijom tijekom i nakon događaja?*
- *Provodi li se Analiza učinkovitosti odgovornih aktivnosti?*

Provedba revizije kibernetičke sigurnosti

Primjeri revidiranih ciljeva:

- *Kako se provode procesi i procedure planiranja oporavka?*
- *Provode li se poboljšanja na temelju naučenih lekcija?*
- *Kako se koordinira komunikacija tijekom aktivnosti oporavka?*

Suradnja revizora i IT revizora

U slučaju suradnje s IT revizorima, potrebno ih je uključiti unutar fazi razumijevanja IT okruženja, razumijevanja programa upravljanja kibernetičkom sigurnošću, utvrđivanja nastanka kibernetičkog incidenta te u možebitnoj analizi utjecaja samog kibernetičkog incidenta, ukoliko je identificiran.

Potrebno je naglasiti da je revizor financijskih izvještaja dužan donijeti i dokumentirati vlastite zaključke vezano uz kibernetičke rizike i učinkovitost IT kontrola!

Hvala na pažnji

Tihana Bažant

tbazant@deloittece.com

Ratko Drča

rdrca@deloittece.com