POLITIKA BEZBJEDNOSTI ISMS-a

Odgovornosti

Verzija	4
Datum kreiranja (inicijalna verzija)	23.11.2017
Datum kreiranja (Trenutna verzija)	01.07.2024
Kreirao	Adis Pijadžer, Adi Osmanović
Odobrio	Petar Mrkonjić, Mirza Kahvedžić
Oznaka	ISMS-POL-01
Opis	Izmjena u obimu posla Kompanije. Napomena: Kompanija se ne bavi dizajnom niti razvojom softvera.
ISO	

Historija dokumenta

Datum	Verzija	Odgovoran	Opis
23.11.2017	1	Adis Pijadžer	Inicijalna verzija
11.02.2020	2	Adis Pijadžer	Uklonjene su politike i procedure koje su bile napisane odvojeno, kao i svi dijelovi koji se odnose na zaposlenike ili IT. Promijenjen je oblik politike tako da može biti javno dostupan
13.02.2023.	3	Adis Pijadžer	Definisana strategija i ciljevi informacijske sigurnosti.
26.04.2024	3	Adi Osmanović	Male izmjene
01.07.2024	4	Adi Osmanović	Izmjena u obimu posla Kompanije. Napomena: Kompanija se ne bavi dizajnom niti razvojom softvera.

SADRŽAJ

1. POLITIKA

EOS MATRIX d.o.o. za poslovne usluge Sarajevo je kao jedan od svojih bitnih procesa podrške prepoznala proces upravljanja bezbjednosti informacionog sistema. Informacioni sistem Kompanije je uspostavljen u skladu sa prirodom, obimom i složenošću poslovanja. Informacioni sistem Kompanije ima zadatak da osigura informacije koje su značajne za obavljanje poslovnih aktivnosti i za donošenje poslovnih odluka. Cilj sveobuhvatnog upravljanja bezbjednosti informacionog sistema jeste da svim korisnicima informacionog sistema obezbijedi:

- **Povjerljivost**
  Pristup informacijama treba biti ograničen na one koji imaju odgovarajuću ovlast i poslovnu potrebu za pristupom informacijama.
- **Integritet**
  Informacije moraju biti potpune i tačne. Svi sistemi, imovina i mreže moraju raditi ispravno, prema specifikaciji.
- **Dostupnost**
  Informacije moraju biti dostupne i dostavljene pravoj osobi u trenutku kada su potrebne.

Rukovodstvo Kompanije politikama bezbjednosti ISMS-a definiše svoj sistem upravljanja bezbjednošću informacija (ISMS, eng. Information Security Managment System), čime potvrđuje da će ISMS u Kompaniji biti uspostavljen prema zahtjevima standarda ISO/IEC 27001:2013. ISMS će biti uspostavljen na analizi internih i eksternih faktora važnih za sposobnost postizanja željenih ciljeva sistema upravljanja bezbjednosti informacija. Politika IT bezbjednosti primjenjuju se u svim organizacionim dijelovima i ima namjenu da:

- Definiše predmet i područje primjene sistema upravljanja bezbjednosti informacija u Kompaniji.
- Uspostavi jasan pravac djelovanja rukovodstva u skladu sa poslovnim ciljevima i da rukovodstvo iskaže svoju podršku i privrženost bezbjednosti informacija.
- Definiše ciljeve i mjere zaštite saglasno najboljoj praksi definisanoj u međunarodnom standardu ISO/IEC 27001:2013.
- Promoviše načelo da su informaciono - komunikacijske tehnologije, uključujući i podatke koji se na njima obrađuju, prenose i čuvaju u vlasništvu Kompanije.
- Ukaže da zaposleni u Kompaniji, korisnici IT sistema Kompanije, prihvataju obavezu da neće praviti neautorizovane kopije podataka i softvera.
- Ukaže da će se svi korisnici IT sistema Kompanije sami starati o IT bezbjednosti. Osigura da korisnik prihvati obavezu da IT sistemu Kompanije i podacima pristupa samo u svrhu obavljanja posla za potrebe Kompanije.
- Promoviše princip da Kompanija nadzire upotrebu sistema u svrhu bezbjednosti.

- Definiše opće i posebne obaveze za upravljanje zaštitom informacija, uključujući izvještavanje o incidentima narušavanja bezbjednosti.
- Definiše objašnjenje politike zaštite, principa, kriterijuma i zahtjeva za usaglašenost sa posebnim značajem za Kompaniju, kao npr. usaglašenost za zakonskim i ugovorenim zahtjevima, zahtjevi za educiranje u pogledu zaštite povjerljivosti, dostupnosti i integriteta informacija, otkrivanje virusa i zlonamjernih softvera, upravljanje kontinuitetom poslovanja.
- Definiše posljedice kršenja politika zaštite.
- Opiše ključne procese i njihove međusobno djelovanje u Sistemu bezbjednosti
- Obuhvati dokumentovane procedure koje se primjenjuju u Sistemu upravljanja bezbjednosti informacija ili se pozove na procedure definisane u okviru drugih uvedenih sistema upravljanja.
- Služi kao osnovni dokument za upravljanjem bezbjednosti informacija, za njegovu efikasnu primjenu i održavanje.
- Služi kao osnova za stalna poboljšanja Sistema upravljanja bezbjednosti informacija.

Politike bezbjednosti informacionog sistema preispituju se jednom godišnje (na početku godine) ili ukoliko se pojave značajne promjene. Saopštena je u okviru Kompanije i dostupna je svim zaposlenicima. Sistem upravljanja bezbjednosti informacija u Kompaniji će bit usklađen sa zahtjevima standarda ISO 27001:2013 Informaciona tehnologija - Tehnike sigurnosti - Sistemi upravljanja bezbjednosti informacija - Zahtjevi (eng. Information technology - Security techniques - Information security management systems - Requirements). Uprava Kompanije odgovoran je da osigura primjenu politika IT bezbjednosti. Uprava ima obavezu, ovlasti i organizacionu samostalnost da identifikuje probleme u funkcionisanju Sistema upravljanja bezbjednosti informacija i da pokrene, preporuči i primjeni odgovarajuća rješenja. Rukovodstvo Kompanije zahtjeva od svih zaposlenika da svoje poslove obavljaju u skladu sa odredbama politika IT bezbjednosti i usvojenim procedurama. Svaki zaposlenik koji prekrši pravila i odredbe iz ovog dokumenta podliježe disciplinskim mjerama predviđenim u Pravilniku o radu, procedurom ISMS-PRO-01 Procedura upravljanja ljudskim resursima i drugim općim aktima, procedurama i pravilima kod poslodavca na koje se obavezao ugovorom o radu. Upravljanje informacionim sistemom Kompanije je zasnovano na opće prihvaćenom konceptu upravljanja rizikom u oblasti informacionih tehnologija. Procjena rizika će se vršiti minimum jednom godišnje i izlaz iz procjene rizika predstavlja Plan tretiranja rizika koji predstavlja organizaciono-tehničke mjere a sve u cilju uklanjanja ili minimiziranja identifikovanih rizika.

1.1 EOS MATRIX d.o.o. za poslovne usluge Sarajevo

Kompanija je prisutna od 2011. godine u Bosni i Hercegovini, tačnije u Sarajevu kao dio EOS Grupe i na lokalnom tržištu nudi usluge upravljanja dugovima u sljedećim oblastima:

- Naplata kupljenih dugova;

- Kontingentna naplata duga;
- Međunarodna naplata;
- Osigurana potraživanja;

Kompanija posjeduje Call centar i koristi ga kao osnovni alat za naplatu i praćenje potraživanja putem softverske platforme KOLLECTO. Platformu razvija i održava EOS IT Services SRL. Svi podaci o dužniku i dugu i plaćanjima za taj dug se bilježe u bazi podataka i omogućavaju tačno izvještavanje i informisanje Klijenta o statusu duga i vjerovatnoći naplate. EOS Grupa je vodeća međunarodna organizacija koja pruža usluge koje pokrivaju cijeli životni ciklus odnosa sa klijentima: od pronalaženja kontaktnog broja dužnika do procesa plaćanja, naplate potraživanja za klijenta i kupovine portfolija. Glavna aktivnost je naplata duga. EOS je posvećen visokim standardima u naplati duga kako bi zaštitio vjerovnike i partnere. Potraživanja se naplaćuju putem:

- telefonskih poziva, kao osnovnog sredstva naplate
- pismenog obavještavanja dužnika o dugu,
- obavještenja putem sms / e-maila,
- naplata sudskim putem za otkupljena potraživanja.

EOS MATRIX d.o.o. za poslovne usluge Sarajevo se ne bavi razvojem niti dizajnom novih aplikacija/softvera.

1.2 Interesne grupe

U okviru uspostavljenog sistema upravljanja bezbjednosti informacija u skladu sa ISO/IEC 27001:2013, identifikovane su različite interesne grupe, od kojih su najznačajnije:

- Klijenti;
- Dužnici;
- Zaposlenici;
- Vlasnik;
- Partneri;
- Država.

Klijenti predstavljaju jednu od najvažnijih eksternih zainteresovanih strana čiji je interes očuvanje bezbjednosti svih kritičnih informacija vezanih za informacioni sistem koji predstavlja predmet pružanja finansijskih usluga. Također, korisnici su zainteresovani za kontinuitet servisa u pogledu bezbjednosti informacija. Kompanija je zainteresovana za ISMS u smislu svih zakonodavnih i ugovorenih obaveza vezanih za bezbjednost informacija i obezbjeđenje dostupnosti poslovanja sa aspekta bezbjednosti informacija. Zaposlenicima je fokus na osiguranju zaštite povjerljivosti ličnih podataka. Također, zaposlenici predstavljaju interne zainteresovane strane čiji interes očuvanja bezbjednosti svih informacija i informacionih servisa koji su neophodni kako bi se poslovni procesi odvijali na predviđen način. Partneri/Dobavljači su zainteresovane strane u pogledu očuvanja bezbjednosti informacija

vezanih za same organizacije i njihove zaposlene koje razmjenjuju u odnosima sa Kompanijom. Država je zainteresovana strana u domenu bezbjednosti informacija u kontekstu ispunjena zakonskih obaveza. Osnova sistema upravljanja bezbjednosti informacija Kompanije je analiza zahtjeva svih interesnih grupa, identifikacija ciljeva prema interesnim grupama, definisanje indikatora realizacije ciljeva, praćenje performansi i realizacija mjera poboljšanja.

2. STRATEGIJA BEZBJEDNOSTI INFORMACIJA

Ova Strategija informacijske sigurnosti predstavlja putokaz za budućnost pružajući pozadinske detalje i ističući potencijalne prijetnje i ranjivosti koje treba identificirati, procijeniti, razumjeti i neutralizirati. Ona predstavlja ukupnu viziju gdje trebamo biti, detaljno opisujući pokretače i ciljeve. Također pruža strateške prijedloge pod ključnim temama Identificiraj, Zaštiti, Detektuj, Reaguj i Oporavi, pri čemu svaka oblast detaljno opisuje individualne ciljeve, pristup i mjere uspjeha:

Identifikacija:

- Kreiranje održivog okvira za upravljanje informacijskom sigurnošću (uključujući politiku, standarde i procese) kako bi se osigurao dosljedan pristup upravljanju rizicima informacijske sigurnosti, kako interno, tako i kod ključnih dobavljača treće strane.

Zaštita:

- Razvoj dodatnih kontrola za upravljanje pristupom korisnika i procesa za uvođenje rutinske re-certifikacije potrebnih dozvola za pristup će osigurati da individualni korisnici imaju pristup samo sistemima i podacima koji su im potrebni za obavljanje trenutne uloge.
- Efikasna obavezna obuka korisnika, kako generička tako i specifična za ulogu, povećat će ukupnu svijest o rizicima i prijetnjama informacijske sigurnosti i individualnim odgovornostima koje svako ima za upravljanje informacijskom sigurnošću.
- Upoređivanje naših procesa sa standardima će pokazati našu posvećenost sigurnom poslovanju prema vanjskim partnerima i zainteresiranim stranama.
- Efikasno upravljanje zakrpama ključno je za suprotstavljanje mnogim prijetnjama. Uvođenjem robustnih procesa i upravljanjem punim životnim ciklusom sistema i softvera možemo biti sigurni da minimiziramo potencijalne vektore prijetnji koji bi mogli biti lako iskorišteni od strane zlonamjernih aktera.
- Procjena i upravljanje Cloud uslugama prije korištenja za obradu informacija kompanije.

Detektovanje:

- Uspostavljanje sposobnosti operacija sigurnosti će poboljšati naš odgovor na nastale prijetnje unutar mreže Kompanije i omogućiti veću analizu prikupljenih podataka.

Reakcija i oporavak:

- Sposobnost efikasnog odgovora i oporavka od incidenata informacijske sigurnosti ključna je za održavanje efikasnih operacija širom Kompanije i zadržavanje povjerenja zainteresiranih strana.

2.1. Vizija

Da bi bila efikasna, ključno je da ova Strategija podržava ukupnu Strategiju Kompanije. Stoga mora imati značajnu viziju:

Upravljanje rizicima informacijske sigurnosti je sveprisutno u cijeloj Kompaniji sa širokom sviješću o prijetnjama sa kojim se Kompanija suočava. Pojedinci razumiju svoje vlastite uloge i odgovornosti i prepoznaju prilike koje efikasno upravljanje rizicima informacijske sigurnosti može pružiti. Osoblje i menadžment primjenjuju dobre prakse upravljanja rizicima informacijske sigurnosti kako bi podržali inovacije i omogućili razvoj fleksibilnih i agilnih poslovnih rješenja. Kompanija djeluje kao kreator i praktičar dobre prakse informacijske sigurnosti.

Da bi se ostvarila vizija, implementirat će se mjere za rješavanje sljedećih ključnih funkcija:

- **Identifikacija**
  Organizacijsko razumijevanje i svijest o informacijskoj sigurnosti za efikasno identificiranje i upravljanje rizikom informacijske sigurnosti naših ključnih informacijskih sredstava, bilo da se radi o podacima ili uslugama.
- **Zaštita**
  Odgovarajuće kontrole i zaštitne mjere za stvaranje okruženja u kojem naše osoblje ima priliku postići svoje ciljeve i samopouzdanje da preuzme nove inicijative, omogućavajući pružanje ključnih poslovnih usluga.
- **Detekcija**
  Odgovarajući sistemi, sposobnosti, procesi i procedure za što ranije otkrivanje događaja vezanih za informacijsku sigurnost.
- **Odgovoriti**
  Odgovarajuće sposobnosti, procesi i partnerstva za efikasno djelovanje protiv otkrivenih događaja vezanih za informacijsku sigurnost koji utječu na Kompaniju.
- **Oporaviti**
  Sistemi, sposobnosti i procesi za poboljšanje planova za poslovnu otpornost i za obnovu bilo kojih sposobnosti i/ili ključnih usluga koje su bile oštećene događajem vezanim za informacijsku sigurnost na efikasan i efektivan način.

Ključne funkcije će biti podržane pratećim elementima:

- **Upravljanje, politika i vlasništvo nad podacima**
  Bitno je da postoji ekstenzivno upravljanje rizicima informacijske sigurnosti i politika kako bi se obezbijedio potreban kontrolni okvir koji će omogućiti Kompaniji da demonstrira svoj kohezivan pristup suprotstavljanju prijetnjama.

- **Svijest korisnika**
  Potrebna je efikasna i održiva svijest korisnika kako bi svako bio svjestan svojeg individualnog doprinosa upravljanju rizicima informacijske sigurnosti u skladu sa metodologijom upravljanja rizikom Kompanije.

3. CILJEVI INFORMACIJSKE BEZBJEDNOSTI

3.1 CILJEVI

Ciljevi su dizajnirani da budu S.M.A.R.T (specific, measurable, achievable, realistic and time-based). Ciljevi postavljaju naše ciljane državne ciljeve i fokus za budućnost pokazujući što želimo postići (više detalja o ciljevima uključeno je u Dodatak A):

- Upravljanje i usklađenost, upravljanje rizicima
- Pružiti smjernice i podršku menadžmenta za informacijsku sigurnost u skladu sa poslovnim zahtjevima i relevantnim zakonima i propisima.
- Upravljanje zakrpama, operacije sigurnosti
- Postići i održavati odgovarajuću zaštitu organizacijskih sredstava.
- Pristup korisnika, svijest i obuka
- Osigurati da informacije dobiju odgovarajući nivo zaštite.
- Pristup korisnika, upravljanje dobavljačima treće strane
- Osigurati da zaposlenici, izvođači i korisnici treće strane napuste organizaciju ili promijene zaposlenje na uredan način.
- Pristup korisnika
- Sprečavanije neovlaštenog fizičkog pristupa, oštećenja i ometanja prostorija organizacije i informacija.
- Operacije sigurnosti, odgovor na incidente, planiranje oporavka
  Sprječavanije gubitka, oštećenja, krađe ili kompromitacije sredstava i prekida aktivnosti organizacije.
- Operacije sigurnosti
- Osigurati ispravan i siguran rad objekata za obradu informacija.

- Operacije sigurnosti, planiranje oporavka
- Implementirati i održavati odgovarajući nivo informacijske sigurnosti i isporuke usluga u skladu sa sporazumima o isporuci usluga treće strane.
- Planiranje oporavka
- Održavanje integriteta i dostupnosti informacija i objekata za obradu informacija.
- Operacije sigurnosti
- Osigurati zaštitu informacija u mrežama i zaštitu podržavajuće infrastrukture.

3.2. Pristup

Pristup opisuje korake koje ćemo poduzeti da nam pomognu da postignemo svoje ciljeve.

3.3. Mjerenje uspjeha

Mjere uspjeha pružaju kvantificirani način praćenja naših akcija i napretka prema našim ciljevima. Pomažu nam razumjeti našu trenutnu poziciju i omogućuju nam da tu poziciju dijelimo interno i eksterno. Aktivnosti iz tačke 4. čine strategiju informacijske sigurnosti. Svaka od aktivnosti ima podjednak značaj u postizanju ciljeva informacijske bezbjednosti. Aktivnosti će biti praćene u skladu sa akcionim planom i korektivnim mjerama, te postoji mogućnost proširivanja aktivnosti. Provodit će se vanjsko praćenje kako bi se identificirala nova područja, promijenjena područja ili ona koja više ne predstavljaju materijalni rizik za Kompaniju.

4. IMPLEMENTACIJA CILJEVA

4.1 Identifikacija

4.1.1 Upravljanje i usklađenost

Politike, procedure i procesi za upravljanje i praćenje regulatornih, pravnih, rizika i operativnih zahtjeva Kompanije su razumljive i definišu smjer upravljanja rizicima informacijske sigurnosti.

Ciljevi

- Politike informacijske sigurnosti su razvijene, dokumentovane i ugrađene u cijelu Kompaniju.
- Vlasništvo nad politikom informacijske sigurnosti dodijeljeno je odgovarajućim zainteresovanim stranama.
- Procesi praćenja usklađenosti i izvještavanja koji podržavaju aktivnosti informacijske sigurnosti su razvijeni i ugrađeni u cijelu Kompaniju.

Pristup

- Konsultovati se i raditi sa menadžmentom i zainteresovanim stranama kako bi se razvila skupina politika informacijske sigurnosti prilagođenih strateškim ciljevima Kompanije i profilu rizika.
- Poduzeti odgovarajuće akcije kako bi politike informacijske sigurnosti bile lako razumljive i dostupne osoblju i vanjskim partnerima.
- Dizajnirati i implementirati pojednostavljene procese praćenja usklađenosti koji omogućuju redovno izvještavanje menadžmentu.

Mjerenje uspjeha

- Menadžment je odobrio dokumentovane Informacije.
- Menadžment kontinuirano podržava informacijsku sigurnost promovišući ključne politike i dobru praksu informacijske sigurnosti.
- Dodijeljeno vlasništvo i odgovornost za politike informacijske sigurnosti.
- Menadžment, osoblje i druge interne i eksterne strane razumiju svoje individualne i kolektivne uloge i odgovornosti.
- Zahtjevi za informacijskom sigurnošću i relevantne politike su komunicirane osoblju i drugim internim i eksternim stranama. Ustanovljeni su redovni kanali komunikacije.
- Politike informacijske sigurnosti su dostupne osoblju, i drugim internim i eksternim stranama.
- Politike informacijske sigurnosti se periodično pregledavaju.
- Usvojene su prakse kontinuiranog praćenja usklađenosti i koriste se za praćenje ključnih pokazatelja učinka (KPI) informacijske sigurnosti.
- Izvještavanje se generiše i redovno dijeli s Menadžmentom.

4.1.2 Upravljanje rizikom

Sklonost Kompanije prema riziku informacijske sigurnosti je dogovorena, jasno izražena i razumljiva svim zainteresovanim stranama. Kombinovani rizik informacijske sigurnosti s kojim se Kompanija suočava je razumljiv i procesi za identifikaciju i adekvatno upravljanje ovim rizikom su uspostavljeni i implementirani u Kompaniji.

Ciljevi

- Apetit kompanije za rizikom informacijske sigurnosti određuje se, dogovara i dokumentira u skladu s širim procesima upravljanja rizicima.
- Kompanija je razvila, dokumentovala i ugradila pouzdan način procjene rizika informacijske sigurnosti u svim svojim operacijama, kako interno tako i eksterno.

- Procesi za upravljanje rizicima informacijske sigurnosti, uključujući nadzor, upravljanje i redovno izvještavanje, razvijeni su i ugrađeni u cijelu kompaniju.

Pristup

- Konsultovati se i raditi s menadžmentom kako biste odredili i dokumentovali metodologiju rizika informacijske sigurnosti.
- Razviti i dokumentovati pouzdan način za identifikaciju i procjenu rizika informacijske sigurnosti te ih komunicirajte s relevantnim zainteresovanim stranama.
- Dizajnirati i implementirati pojednostavljene procese upravljanja rizicima koji omogućavaju efikasan nadzor i redovno izvještavanje.

Mjerenje uspjeha

- Kompanija ima jasno razumijevanje svog upravljanja rizicima informacijske sigurnosti. To je dokumentirano, odobreno od strane menadžmenta i komunicirano osoblju, te ostalim internim i eksternim zainteresovanim stranama.
- Dosljedan proces za identifikaciju i procjenu rizika informacijske sigurnosti je dokumentiran. Rizici se identificiraju rano, dokumentiraju i prate. Izvještaji se redovno dijele s menadžmentom.
- Poznati, prihvaćeni rizici se redovno pregledavaju i ponovno procjenjuju kako bi se potvrdila razina rizika koju predstavljaju za kompaniju u skladu s dogovorenom metodologijom rizika.

4.1.3 Upravljanje trećim stranama

Politike i procesi informacijske sigurnosti su na mjestu kako bi se identificirali, procijenili i razumjeli rizici kod ključnih dobavljača, uključujući, ali ne ograničavajući se na, provjeru, uključivanje i periodične preglede informacijske sigurnosti. Jednom kada se identificiraju, ti se rizici dokumentiraju, prate, redovito pregledavaju i izvještavaju.

Ciljevi

- Ključni dobavljači treće strane su upoznati sa zahtjevima kompanije za upravljanje rizicima informacijske sigurnosti i moraju prepoznati, i gdje je to praktično, pridržavati se politika i postupaka kompanije za informacijsku sigurnost.
- Rizici informacijske sigurnosti ključnih dobavljača treće strane identificirani su, procijenjeni i dokumentirani kao dio procesa dužne pažnje prije sklapanja ugovornih sporazuma.
- Rizici informacijske sigurnosti ključnih dobavljača treće strane se prate, redovno pregledavaju i izvještavaju. Učestalost ovih aktivnosti ovisi o povezanom nivou procijenjenog rizika.

Pristup

- Komunicirati metodologiju rizika informacijske sigurnosti kompanije i relevantne politike i postupke informacijske sigurnosti s ključnim nosiocima procesa treće strane.
- Učiniti relevantne politike i postupke informacijske sigurnosti dostupnima ključnim nosiocima procesa treće strane.
- Uključiti naše obavezne sigurnosne zahtjeve/klauzule u dokumente za nabavku i ugovorne dokumente u ranoj fazi procesa nabavke.
- Razviti, dokumentovati i implementirati održivi proces za identifikaciju i procjenu rizika informacijske sigurnosti kod ključnih trećih strana na dosljedan način.
- Konsultovati se i raditi s internim i eksternim grupama kako biste razvili procese i procedure za praćenje, pregled i izvještavanje o rizicima informacijske sigurnosti kod ključnih trećih strana.

Mjerenje uspjeha

- Zahtjevi i politike informacijske sigurnosti kompanije komuniciraju se i prihvataju od strane nosioca procesa treće strane prije angažmana, kako bi utjecali na to s kojim trećim stranama smo spremni surađivati.
- Dokumentovan je dosljedan proces za identifikaciju i procjenu rizika informacijske sigurnosti treće strane. Rizici se identificiraju rano, dokumentiraju i prate. Izvještaji se redovito dijele s menadžmentom.
- Rizici informacijske sigurnosti treće strane redovito se pregledavaju i ponovno procjenjuju kao dio praksi osiguranja kako bi se potvrdila razina rizika koju kompanija nosi u skladu s dogovorenom metodologijom rizika informacijske sigurnosti..

4.2. Zaštita

4.2.1. Pristup korisnika

Pristup informacijskim sredstvima i povezanim objektima ograničen je na ovlaštene korisnike, procese ili uređaje u skladu s principima kontrole pristupa na temelju uloga (RBAC).

Ciljevi

- Identiteti i akreditivi za ovlaštene uređaje i korisnike centralno se upravljaju u skladu s principima kontrole pristupa na temelju uloga (RBAC).
- Fizički i pristup na daljinu informacijskim sredstvima sigurno se upravlja.
- Korisnički pristup sistemima i podacima redovito se pregledava kako bi se osiguralo da se nepotrebni pristup ukloni.

Pristup

- Centralizirati kontrolu kako bi na siguran način upravljali identitetima i akreditivima za uređaje i korisnike.
- Usvojiti i implementirati dobre industrijske prakse i principe kontrole pristupa na temelju uloga (RBAC) kako bi kontrolisali i upravljali korisničkim pristupom informacijskim sredstvima, uslugama i objektima.
- Implementirati procese i procedure za pregled dozvola za pristup korisnika, uključujući privilegovani pristup na redovnoj osnovi.

Mjerenje uspjeha

- Alati su implementirani za upravljanje identitetom i pristupom informacijskim sredstvima, uslugama i objektima na centraliziran i automatiziran način. Ovi alati su konfigurirani prema industrijskoj praksi.
- Dozvole za pristup, kako logičke tako i fizičke, dodjeljuju se u skladu s principima kontrole pristupa na temelju uloga (RBAC) i redovito se pregledavaju.
- Privilegovani pristup zahtijeva odobrenje vlasnika sredstva i redoviti pregled, najmanje jednom godišnje.
- Korisnici zadržavaju samo pristup potreban za njihove trenutne uloge, a pristup se pregledava prilikom promjene uloga.
- Pristup 'odlaznih' korisnika sistemima i informacijama kompanije uklanja se čim je to praktično moguće nakon što je njihov odnos s kompanijom završen.

4.2.2. Svijest o informacijskoj sigurnosti i obuka

Osoblje kompanije i ostali korisnici sistema i podataka kompanije primaju odgovarajuću obuku o svijesti o informacijskoj sigurnosti kako bi obavljali svoje dužnosti i odgovornosti u skladu sa organizacijskim i pravnim politikama, procedurama i sporazumima.

Ciljevi

- Menadžmentu je pružena adekvatna obuka o informacijskoj sigurnosti kako bi razumjeli svoje uloge i odgovornosti.
- Osoblju i ostalim internim i eksternim korisnicima koji pristupaju informacijama kompanije pružena je odgovarajuća obuka o informacijskoj sigurnosti i/ili pristup relevantnim informacijama.
- Privilegovanim korisnicima je pružena pojačana obuka o informacijskoj sigurnosti kako bi osigurali da razumiju dodatne odgovornosti vezane za njihove uloge.

Pristup

- Uvesti obaveznu obuku o svijesti o informacijskoj sigurnosti za sve zaposlenike i izvođače koji imaju pristup sredstvima informacija kompanije kao dio lokalnih procesa uvođenja i na redovnim intervalima nakon toga.
- Komunicirati zahtjeve, politike i procedure informacijske sigurnosti sa svim internim i eksternim nosiocima procesa.
- Razviti prilagođeni materijal za obuku o informacijskoj sigurnosti za ključne grupe korisnika, uključujući, ali ne ograničavajući se na, menadžment, osoblje i privilegovane korisnike. Obuka za prepoznavanje holističke prirode efikasne ublažavanja rizika i obuhvatanje raspona ljudi, procesa i tehnoloških ulaza potrebnih za postizanje potrebnih rezultata.
- Učiniti materijal za obuku lako dostupnim korištenjem tehnologije digitalnog učenja na webu.
- Razviti i implementirati proces koji omogućava komunikaciju relevantnih poruka o informacijskoj sigurnosti na nivou cijele organizacije.
- Razviti efikasan mehanizam izvještavanja koji omogućava praćenje i izvještavanje o stopama završetka obavezne obuke o svijesti o informacijskoj sigurnosti.

Mjerenje ciljeva

- Trening o informacijskoj sigurnosti korisnika u obliku uvodnog treninga i godišnjeg obnovljenog treninga uredno završeni.
- Trening o informacijskoj sigurnosti je lako dostupan korištenjem tehnologije digitalnog učenja na webu i drugih centraliziranih resursa.

4.2.3. Upravljanje zakrpama

Sveobuhvatna strategija upravljanja zakrpama i ažuriranjima, zajedno s podržavajućim procesima, uspostavljena je kako bi se identificirale, procijenile i primijenile potrebne sigurnosne zakrpe i ažuriranja, dok se osigurava dostupnost ključnih poslovnih resursa, uključujući informacijske sisteme i aplikacije. Ovo će pomoći da se osigura da oprema ostane prikladna za namjenu i pruža očekivani nivo zaštite tokom svog životnog vijeka u upotrebi, te će identificirati kada je vjerovatno da će postati zastarjela ili bez podrške, jer zadržavanje takve opreme uvodi dodatne rizike.

Ciljevi

- Proces je uspostavljen za identifikaciju, evaluaciju i primjenu sigurnosnih zakrpa i ažuriranja na vrijeme za ključne poslovne resurse, uključujući informacijske sisteme i aplikacije.
- Ključni poslovni resursi, uključujući informacijske sisteme i aplikacije, ažurirani su najnovijim sigurnosnim zakrpama i ažuriranjima.
- Proces je uspostavljen za upravljanje cjelokupnim životnim ciklusom ključnih sredstava, uključujući nadogradnje, pristup kraju životnog vijeka i sigurno odlaganje.

Pristup

- Definisati, složiti se i dokumentovati proceduru upravljanja zakrpama kompanije.
- Uspostaviti i implementirati podržavajuće procese upravljanja kako biste identificirali, evaluirali i primijenili sigurnosne zakrpe na vrijeme.
- Komunicirati strategiju zakrpa i podržavajuće procese upravljanja sa relevantnim nosiocima procesa.
- Redovito pregledavati i izvještavati o statusu zakrpa ključnih poslovnih resursa.

Mjerenje ciljeva

- Procedura upravljanja zakrpama je definisana, dokumentovana i komunicirana sa relevantnim nosiocima procesa.
- Podržavajući procesi su ugrađeni i rade kako je predviđeno.
- Redovno se provode pregledi kako bi se procijenila efikasnost strategije upravljanja zakrpama i njenih podržavajućih procesa upravljanja.
- Informacije o upravljanju statusom zakrpa ključnih poslovnih resursa dijele se sa relevantnim nosiocima procesa najmanje kvartalno.
- Ključni poslovni resursi, uključujući informacijske sisteme i aplikacije, ažurirani su najnovijim zakrpama u skladu sa strategijom upravljanja zakrpama.

4.3. Detektovanje

4.3.1. Operacije sigurnosti

Tehnička rješenja za informacijsku sigurnost i podržavajući procesi su na mjestu za upravljanje operacijama informacijske sigurnosti i pružanje sposobnosti za nadzor, procjenu i odbranu informacijskih sistema i mreža.

Ciljevi

- Segmentacija mreže i podržavajuće kontrole sigurnosti mreže implementirane su kako bi se poboljšale performanse i povećala otpornost i sigurnost mreže.

- Uspostavljena je centralizirana funkcija tehničkih operacija za nadzor, procjenu i odbranu informacijskih sistema i mreža.
- Implementirano je rješenje za upravljanje sigurnosnim informacijama i događajima (SIEM) kako bi se omogućila real-time korelacija i analiza sigurnosnih događaja generiranih od strane informacijskih sistema i mreža. Ovo će uključivati feedove iz alata za nadzor, kao što su sistemi za detekciju/preventivu upada.
- Razvijen je opseg testiranja sigurnosti i dogovoren je raspored testiranja za redovne sigurnosne procjene na informacijskim sistemima i mrežama koristeći i internu i eksternu sposobnost.

Pristup

- Pregledati i procijeniti trenutni dizajn i arhitekturu mreže. Implementirati poboljšanja i/ili dodatne kontrole sigurnosti mreže gdje je to prikladno.
- Uložiti u tehničku funkciju operacija sigurnosti sa sposobnošću da nadzire, procjenjuje i brani informacijske sisteme i mreže.
- Kupiti i implementirati specijalističke sigurnosne alate, uključujući, ali ne ograničavajući se na, upravljanje sigurnosnim informacijama i događajima (SIEM) koje koristi tehnička funkcija operacija sigurnosti.
- Razviti i dokumentovati opseg testiranja informacijske sigurnosti koji pokriva ključne informacijske sisteme i mreže i prati redovni raspored testiranja.

Mjerenje ciljeva

- Performanse, otpornost i sigurnost mreže su povećane zbog segmentacije mreže i implementacije podržavajućih kontrola sigurnosti mreže kao što su sistem za detekciju i prevenciju upada (IDPS).
- Formirana je funkcija tehničkih operacija i ima resurse sastavljene od stručnog specijalističkog osoblja za procjenu i odbranu informacijskih sistema i mreža.
- Sigurnosni alati, uključujući ali ne ograničavajući se na upravljanje sigurnosnim informacijama i događajima (SIEM), su kupljeni i implementirani kako bi omogućili tehničkom osoblju za operacije sigurnosti da izvršavaju real-time korelaciju i analizu sigurnosnih događaja.

4.4. Reagovanje

4.4.1. Reagovanje na incident

Procesi i procedure za reagovanje na incidente informacijske sigurnosti su definisani, dokumentovani i komunicirani svim relevantnim nosiocima procesa. Strateška partnerstva su uspostavljena kako bi se pružali vanjski savjeti, podrška i dopunili internu sposobnost gdje je to

prikladno. Redovno se provode testiranja i obuke kako bi se osiguralo da su svi nosioci procesa i sigurni u svoje odgovornosti i potrebne radnje te u efikasnost plana.

Ciljevi

- Procesi i procedure za reagovanje na incidente informacijske sigurnosti su razvijeni, dokumentovani, implementirani, testirani i komunicirani sa relevantnim nosiocima procesa.
- Obuka za reagovanje na incidente informacijske sigurnosti se pruža onima koji imaju aktivne uloge u reagovanju.
- Razvijena su strateška partnerstva sa vanjskim nosiocima procesa.
- Aktivnosti reagovanja na incidente informacijske sigurnosti se poboljšavaju istragama o osnovnom uzroku i uključivanjem naučenih lekcija iz prethodnih aktivnosti detekcije i/ili reagovanja.

Pristup

- Razviti, dokumentovati i implementirati proces reagovanja na incidente informacijske sigurnosti na nivou cijele kompanije i komunicirati ga sa relevantnim nosiocima procesa.
- Uspostaviti internu sposobnost reagovanja na incidente informacijske sigurnosti u obliku specijalizovanog tima za reagovanje na incidente.
- Uspostaviti internu sposobnost digitalne forenzike informacijske sigurnosti u obliku specijalističke opreme i resursa.
- Razviti i pružiti relevantnu obuku za reagovanje na incidente informacijske sigurnosti za one koji imaju aktivne uloge u reagovanju.
- Razviti vanjska partnerstva kako bi pomogla savjetovanje, podršku i dopunila interne sposobnosti gdje je to prikladno.

Mjerenje ciljeva

- Procesi reagovanja na incidente informacijske sigurnosti su definisani, dokumentovani, testirani i komunicirani sa relevantnim nosiocima procesa.
- Specijalistički tim za reagovanje na incidente informacijske sigurnosti je na mjestu, a članovi tima su obučeni i svjesni svojih uloga i odgovornosti.
- Kompanija održava vanjska partnerstva kako bi podržala i dopunila svoje interne sposobnosti reagovanja na incidente kada je to potrebno.

4.5. Oporavak

4.5.1. Planiranje oporavka

Procesi, procedure, sistemi i sposobnosti oporavka informacijske sigurnosti su na mjestu i poznati su odgovarajućim nosiocima procesa.

Ciljevi

- Procesi i procedure oporavka informacijske sigurnosti su razvijeni, dokumentovani i implementirani. Ključni procesi i procedure informacijske sigurnosti su podijeljeni sa odgovarajućim nosiocima procesa.
- Pružena je odgovarajuća obuka onima koji imaju aktivne uloge u oporavku.
- Aktivnosti oporavka su poboljšane uključivanjem naučenih lekcija iz prethodnih aktivnosti oporavka.

Pristup

- Razviti, dokumentovati i implementirati procese i procedure oporavka na nivou cijele Kompanije. Komunicirati ih sa odgovarajućim nosiocima procesa.
- Uspostaviti internu sposobnost oporavka informacijske sigurnosti u obliku specijalizovanog tima za oporavak.
- Razviti i pružiti odgovarajuću obuku za oporavak onima koji imaju aktivne uloge u oporavku.

Mjerenje uspjeha

- Procesi i procedure oporavka informacijske sigurnosti su definisani, dokumentovani i komunicirani sa relevantnim nosiocima procesa.
- Specijalizovani tim za oporavak informacijske sigurnosti je na mjestu, a članovi tima su obučeni i svjesni svojih uloga i odgovornosti.

5. DODATAK A – REZIME CILJEVA ZA INFORMACIJSKU SIGURNOST

CILJEVI INFORMACIJSKE SIGURNOSTI

Ključna tema	Ciljevi	Opis	Implementacija
IDENTIFIKACIJA	Upravljanje i Usklađenost	Politika informacijske sigurnosti je razvijena i dodijeljen joj je vlasnik.	2020- 2023
		Procesi i resursi za praćenje usklađenosti i izvještavanje su implementirani.	2023
	Upravljanje rizikom	Procedura za rizik informacijske sigurnosti je postavljena i dogovorena.	2020
		Razvoj metodologije za procjenu rizika.	2021
		Razvoj procesa upravljanja rizicima i izvještavanja.	2023
	Upravljanje ključnim eksternim dobavljačima	Ključni eksterni dobavljači su upoznati sa zahtjevima za upravljanje rizicima informacijske sigurnosti.	2024
		Rizici informacijske sigurnosti ključnih dobavljača treće strane su procijenjeni.	2024
		Rizici informacijske sigurnosti ključnih dobavljača treće strane se prate i izvještavaju.	2024
ZAŠTITA	Korisnički pristup	Upravlja se pristupom korisnika u skladu sa principima RBAC	2018
		Upravlja se pristupom sigurno	2018
		Upravlja se pristupom korisnika putem IDAM	2024
		Pristup korisnika se redovno pregleda	2021
	Svijest i trening	Ključni menadžment prima trening o informacijskoj sigurnosti.	2023
		Trening o informacijskoj sigurnosti je dostupan.	2023
		Korisnici sa proširenim pristupom primaju dodatni, specifični trening za ulogu.	2023
	Upravljanje zakrpama	Strategija upravljanja zakrpama i ažuriranjem je implementirana	2018 - 2023
		Ključni resursi se redovno ažuriraju.	2020
		Postoji proces za upravljanje cjelokupnim životnim ciklusom informacijskih sredstava.	2024
OTKRIVANJE	Sigurnosne operacije	Segmentacija mreže i podržavajuće kontrole su implementirane.	2021
		Centralizovana funkcija sigurnosnih operacija je uspostavljena	2023
		SIEM rješenje je implementirano	2024
		Sigurnosno testiranje je obuhvaćeno i sprovedeno.	2024
ODGOVOR	Odgovor na incident	Procesi odgovora na incidente informacijske sigurnosti su razvijeni i implementirani.	2021
		Trening za odgovor na incidente informacijske sigurnosti je implementiran.	2024
		Strateška eksterna partnerstva su uspostavljena	2023
		Analiza korijenskog uzroka i kontinuirano poboljšanje je urađeno.	2023
OPORAVAK	Planiranje oporavka	Procesi oporavka informacijske sigurnosti su razvijeni i implementirani	2021
		Obuka se pruža onima koji su uključeni u aktivnosti oporavka.	2023
		Aktivnosti oporavka se poboljšavaju identifikacijom slabih tačaka.	2024

[potpisi na narednoj stranici]