Krovna varnostna politika

Kazalo vsebine

1 Poslanstvo in cilji 3
2 Vizija 3
3 Politika varovanja informacij 3
4 Namen 3
5 Odgovornosti 4
6 Zavezanost vodstva 4
7 Varnostni inženir 4
8 Cilji in njihovo merjenje 5
9 Pravna podlaga in usklajenost s predpisi 5
10 Varnostna politika 5
11 Plan ukrepanja v primeru odstopanj oziroma izrednih razmer 6
12 Referenčni dokumenti 6
13 Nosilec dokumenta 7

1 Poslanstvo in cilji

Podjetje XLAB smo eno vodilnih ponudnikov računalništva v oblaku v regiji. Ukvarjamo se z razvojem programske opreme in raziskavami na področju računalništva v oblaku ter porazdeljenih sistemov.

Osnovni cilj podjetja je ustvariti stimulativno okolje v katerem se razvijajo visoko kakovostni in inovativno tehnološki izdelki.

2 Vizija

Vizija podjetja XLAB je prenos vrhunskega akademskega znanja v visoko tehnološko industrijo, kjer proizvajamo izvrstne izdelke za najbolj zahtevne stranke. Naš slogan je »Have fun doing IT!«.

3 Politika varovanja informacij

Ključni cilj podjetja pri ponudbi celovitih tehnoloških rešitev s področja informacijske tehnologije je s kakovostnimi, zanesljivimi ter varnimi storitvami nenehno izpolnjevati pričakovanja in zahteve naših naročnikov ter v vseh pogledih opravičevati njihovo zaupanje.

Informacije in sistemi informacijske tehnologije so bistvena komponenta poslovanja naše organizacije ter glede na naravo našega dela tudi pomembna podpora poslovnih procesov naših poslovnih partnerjev. Politiko varovanja informacij je sprejel direktor po posvetu z vsemi vodilnimi strukturami v podjetju.

Politika varovanja informacij izraža odnos podjetja do podatkov s katerimi upravlja. Politika varovanja informacij podjetja vključuje zavezanost za izpolnjevanje zahtev do podatkov s katerimi upravlja, ter zagotavlja podlage za vodstveni pregled izpolnjevanja zastavljenih ciljev varovanja informacij. Politika varovanja informacij je stalno pregledovana glede ustreznosti trenutnim trendom na trgu ter trendom s področja varovanja informacij.

Vse informacije, s katerimi upravljamo, vsebujejo določeno vrednost in kot celota predstavljajo informacijsko premoženje. Zavedamo se, da je varovanje informacij eden temeljnih pogojev za uspešno poslovanje, zato sistematično varujemo zaupnost, celovitost in razpoložljivost informacij s katerimi upravljamo. Nenazadnje pa vse uporabnike informacijskega sistema izobražujemo na način, da se uporabniki zavedajo groženj, zanje skrbijo in se usposabljajo, in da med svojim vsakodnevnim delom podpirajo varnostno politiko podjetja.

4 Namen

Namen krovne varnostne politike je zagotoviti, da bodo informacije s katerimi se upravlja v podjetju zaupne, razpoložljive in celovite. Informacijska varnostna politika je skladna z SIST ISO/IEC 27001:2013 standardom.

Cilji varnostnih politik so:

- izboljšati varovanje vseh informacij v podjetju,

- povečati informacijsko-varnostno osveščenost vseh zaposlenih in jim dodeliti vloge ter odgovornosti na posameznih področjih znotraj podjetja, da bodo vsi skrbeli za varovanje informacij in tako učinkovito zmanjševali tveganja,
- zagotoviti nemoteno poslovanje tudi v primeru večjega incidenta ali izrednega dogodka,
- vzpostaviti dobro prakso varovanja osebnih podatkov.

5 Odgovornosti

Vsi zaposleni in pogodbeni sodelavci in študentje, ki imajo kakršnekoli stike z informacijskimi viri, ki so v lasti podjetja, so odgovorni za izvajanje varnostne politike. Zato morajo biti z njo vsi seznanjeni in se zavezati, da jo bodo dosledno upoštevali.

Zaposlenim se zagotavlja ustrezno izobraževanje in usposabljanje za zagotavljanje informacijske varnosti. Enako tudi za druge pogodbene sodelavce in študente, kjer se predvideva daljše sodelovanje. Vsi podpišejo ***Izjavo o zaupnosti***, s katero istočasno potrjujejo, da so seznanjeni s Krovno varnostno politiko in ostalimi politikami podjetja.

Pogodbeni izvajalci se k varovanju informacij lahko zavežejo tudi pisno s podpisom ustrezne listine. Pred podpisom se pogodbeni izvajalci seznanijo z vzpostavljeno politiko in postopki, ki jih zahteva vodstvo.

6 Zavezanost vodstva

Svojo zavezanost Sistemu upravljanja varovanja informacij (v nadaljevanju SUVI) vodstvo podjetja dokazuje:

- s svojim lastnim odnosom do strank, zaposlenih ter družbenega okolja,
- s poudarjanjem pomembnosti izpolnjevanja zahtev zakonodaje,
- z določanjem in izvajanjem poslanstva in vizije, strateških usmeritev, strategije in politike podjetja,
- z zagotavljanjem pogojev in virov za izpolnjevanje zahtev SUVI,
- s stalnim osveščanjem in izobraževanjem vseh zaposlenih ter osveščanjem zunanjih izvajalcev,
- s preverjanjem učinkovitosti delovanja SUVI na osnovi rezultatov iz ocen tveganj, notranjih presoj ter vodstvenih pregledov.

7 Varnostni inženir

Vodstvo podjetja je pooblastilo varnostnega inženirja, ki bo skrbel za dokumentacijo SUVI. Direktor podjetja varnostnega inženirja imenuje za petletno obdobje, katerega lahko podaljša.

Naloge vsakokratnega varnostnega inženirja so:

- priprava in pregledovanje informacijske varnostne politike,
- posredovanje varnostne politike v potrditev vodstvu,
- spremljanje pomembnih sprememb pri vzpostavljanju informacijskih sredstev,
- izogibanje pomembnejšim nevarnostim,
- pregledovanje in spremljanje varnostnih dogodkov,

- potrjevanje glavnih pobud za povečanje informacijske varnosti,
- skrb za aktivno vključevanje zaposlenih v proces varovanja informacij,
- vodenje preiskav o vseh domnevnih incidentih, prekrških in izrednih dogodkih, ki so vezani na informacijsko varnost.

Poleg tega je varnostni inženir odgovoren za uvajanje, izvajanje, implementiranje, administriranje in interpretacijo politik, standardov, napotkov in postopkov v zvezi z informacijsko varnostjo v podjetju. Odgovoren je za preverjanje izvajanja varovanja informacij. Odgovornost za varnost informacijskega sistema je vsakodnevna naloga vseh uporabnikov in skrbnikov informacijskega sistema.

8 Cilji in njihovo merjenje

Za spremljanja izvajanja politike varovanja informacij smo oblikovali naslednje cilje:

1. Izboljšati želimo informacijsko varnost podjetja. To spremljamo preko zaznanih incidentov s področja varovanja informacij. Na letnem nivoju povečujemo informacijsko varnost podjetja z zmanjševanjem števila enakih oziroma podobnih incidentov.
2. Vključevanje informacijske varnosti kot enega od ciljev projektov. Vsak projekt mora imeti vsaj tri preverbe s področja varovanja informacij, četudi naročnik tega ne zahteva.

9 Pravna podlaga in usklajenost s predpisi

Pri pisanju varnostnih politik, pravilnikov, navodil, izjav in procedur se upošteva trenutno veljavna zakonodaja Republike Slovenije, standard ISO/IEC 27001:2013 in dobre prakse na področju varovanja informacij, ki niso v nasprotju z zakonodajo.

10 Varnostna politika

Varnostna politika ter ostala dokumentacija SUVI vključuje zahteve ter priporočila standarda ISO/IEC 27001:2013. Posamezna poglavja varnostne politike opisujejo področja, ki jih določa standard. Poglavja varnostne politike se medsebojno prepletajo in dopolnjujejo.

Poglavja, ki jih opredeljuje varnostna politika, so:

- politika varovanja,
- organiziranost varovanja,
- varnost človeških virov,
- upravljanje dobrin,
- nadzor dostopa,
- kriptografija,
- fizična okoljska varnost,
- varnost operacij,
- varnost komunikacije,
- pridobivanje, razvoj in vzdrževanje informacijskih sistemov,
- odnosi z dobavitelji,
- upravljanje informacijskih varnostnih incidentov,

- vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja,
- skladnost.

Po potrebi se za posamezna področja uporabe lahko oblikujejo dodatna poglavja.

11 Plan ukrepanja v primeru odstopanj oziroma izrednih razmer

Vsi zaposleni, pogodbeni izvajalci in študentje so dolžni prijaviti vse izredne dogodke (odstopanja od normalnega stanja) varnostnemu inženirju. O izrednem dogodku se poroča ustno, telefonsko ali pa se pošlje elektronsko sporočilo oziroma izpolni predpisan obrazec, papirni ali elektronski. Varnostni inženir je odgovoren, da incident zabeleži in v primeru, da je to potrebno tudi ustrezno ukrepa.

Prijave se opravijo v primeru:

- izrednih dogodkov pri varovanju informacij,
- pomanjkljivosti ali ob vsakem sumu pojava pomanjkljivosti pri varovanju informacij kot tudi ob vsaki grožnji, ki ogroža sisteme ali storitve,
- nepravilnega delovanja programske ali strojne opreme.

Vsako obvestilo o sumu kršitve varnostne politike se obravnava posebej. V času preiskave se lahko odvzamejo dodeljene pristopne pravice, pristojnosti oz. pooblastila. Incidente raziskuje oseba ali skupina oseb, ki delujejo v sklopu podjetja, ki jih določi vodstvo.

V primeru kršitev varnostnih politik se ukrepa skladno z zakonodajo in predpisanimi pravili v varnostni politiki. Proti zunanjim izvajalcem se ukrepa skladno s podpisano pogodbo.

12 Referenčni dokumenti

- SIST ISO/IEC 27001:2013 Informacijska tehnologija – Varnostne tehnike – Sistemi upravljanja informacijske varnosti – Zahteve.
- SIST ISO/IEC 27002:20013 Informacijska tehnologija - Varnostne tehnike - Pravila obnašanja pri kontrolah informacijske varnosti.
- http://www.eugdpr.org/
- Izjava o zaupnosti.

13 Nosilec dokumenta

Nosilec je Varnostni inženir, ki je odgovoren za vzdrževanje, dopolnjevanje in spreminjanje dokumenta.

dr. Gregor Pipan, direktor

Ljubljana, 1.9.2017