Rizici primjene informacijske tehnologije u poslovanju

Adžić, Maria

Undergraduate thesis / Završni rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:419795

Rights / Prava: Attribution-NonCommercial-ShareAlike 3.0 Unported/Imenovanje-Nekomercijalno-Dijeli pod istim uvjetima 3.0

Download date / Datum preuzimanja: **2024-08-02**

Repository / Repozitorij:

REPEFZG - Digital Repository - Faculty of Economcs & Business Zagreb

SVEUČILIŠTE U ZAGREBU

EKONOMSKI FAKULTET

Maria Adžić

RIZICI PRIMJENE INFORMACIJSKE TEHNOLOGIJE U POSLOVANJU

Završni rad

Zagreb, 2020.

MARIA ADŽIĆ

Ime i prezime studenta/ice

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je završni rad
(vrsta rada)

isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Student/ica:

U Zagrebu, 2020.

(potpis)

SAŽETAK

Organizacije i njihovi informacijski sustavi suočavaju se sa sve većim rizikom i nesigurnostima iz različitih izvora, uključujući računalnu prijevaru, špijunažu, sabotaže ili cyber napade. Određeni izvori štete kao što su napadi upada ili uskraćivanje usluge s vremenom postaju sve češći, ambiciozniji i sofisticiraniji. Apsolutna sigurnost ne postoji te organizacije moraju usvojiti metode i strategije koje im omogućuju dati prednost onim rizicima koji, zbog vjerojatnosti pojave i razine utjecaja, predstavljaju veću potencijalnu štetu poslovanju. Prilikom pripreme za rješavanje vjerojatnih cyber napada ključno je razumijevanje logičkog tijeka akcija koje se mogu izvesti tijekom napada, ugraditi najbolje prakse procjene razine rizika s kojima se organizacija suočava i proaktivno osmisliti postupke za reakciju tijekom ovih scenarija.

Ključne riječi: **informacijski sustavi**, **rizici infomacijskih tehnologija**, **upravljanje rizikom**, **cyber napadi**.

ABSTRACT

Organizations and their information systems face increasing risk and uncertainty from a variety of sources, including cyber fraud, espionage, sabotage or cyber attacks. Certain sources of harm, such as intrusion attacks or denial of service, are becoming more frequent, more ambitious and sophisticated over time. There is no absolute certainty, and organizations must adopt methods and strategies that allow them to prioritize those risks that, due to their likelihood of occurrence and level of impact, pose a greater potential harm to the business. When preparing to deal with likely cyber attacks, understanding the logical course of action that can be taken during an attack is crucial, incorporating best practices for assessing the level of risk an organization faces, and proactively devising procedures for responding to these scenarios.

Keywords: **information systems**, **information technology risks**, **risk management**, **cyber attacks**.

SADRŽAJ

1. UVOD

Sigurnost informacija jedan je od najvažnijih područja danas u cijelom svijetu. Sigurnost informacija je praksa zaštite podataka od neovlaštenog pristupa, upotrebe, otkrivanja, ometanja, izmjene, uvida, pregleda, snimanja ili uništavanja. To je opći izraz koji se može koristiti bez obzira na oblik u kojem se podaci mogu preuzeti (npr. elektronički ili fizički podaci). Uz poznavanje informacijske sigurnosti, uvjereni smo da su naši podaci zaštićeni, a također smo uvjereni u sigurnost naših podataka. Nadalje, informacijska sigurnost je „spasitelj života“ organizacija širom svijeta. Ne smije se podcjenjivati utjecaj sigurnosnih incidenata koji mogu dovesti do gubitka podataka, curenja osobnih podataka, gubitka istih i širenja virusa. Sigurnosni incidenti koji se događaju na drugim računalima utjecat će i na nas. Sigurnost informiranja danas je od velikog značaja i zanima sve u svijetu tehnologije. Suvremena informacijska i komunikacijska tehnologija omogućuju tvrtkama svih veličina inovativnost, prodor na nova tržišta i dobrobit kupaca i društva. Poslovna praksa i politika moraju se prilagođavati izravnom i neizravnom utjecaju sveprisutnih komunikacijskih okružja i mrežnog protoka informacija koji su nužni za isporuku usluga i dobara. U brojnim se tvrtkama implementiraju suvremene informacijske i komunikacijske tehnologije, a da se ujedno nije u potpunosti razmotrila činjenica kako je zbog toga potrebno upravljati novim vrstama rizika.

2. INFORMACIJSKA TEHNOLOGIJA

Novi tehnološki razvoj postavlja nove zahtjeve pred tvrtke, ili pruža nove mogućnosti za razvoj ili poboljšanje tržišnih aktivnosti kao i proizvoda. Jedan od primjera takvog tehnološkog razvoja je upotreba informacijske tehnologije među industrijskim tvrtkama koje posluju. Postoje mnoge različite informacijske tehnologije, a samim tim i razne mogućnosti tvrtki da ih koriste tijekom obavljanja razmjene. Neka rješenja omogućuju korisnicima koji su geografski raspoređeni za razmjenu baza podataka i poruka koje se mogu kopirati i trenutno isporučiti ogromnom broju prijemnika.

Internet je u današnjoj eri pametnih telefona i računala promijenio ideju o komunikaciji. Zbog nedostatka sigurnosti, u prošlom desetljeću su se dogodili razni cyber zločini. Cyber sigurnost igra značajnu ulogu u trenutnom razvoju informatičke tehnologije i usluga, pri čemu se cyber sigurnost definira kao pokušaj korisnika da svoje osobne i profesionalne podatke zaštite od napada na Internetu. Glavna funkcija cyber sigurnosti je zaštita mreža, računala ili programa od neovlaštenog pristupa.

Izuzetno velik broj korisnika nije svjestan rizika i nesvjesno dijeli svoje podatke, a nedostatak znanja čini ih ranjivim na cyber napade. Stoga je cyber sigurnost glavna briga u današnjem svijetu računanja. Internetska prijetnja može biti nenamjerna i namjerna, ciljana ili nenamjerena, a može poticati iz raznih izvora, uključujući strane nacije angažirane u špijunaži i informacijskim ratovima, kriminalce, hakere, pisce virusa, nezadovoljne zaposlenike i ugovarače koji rade u organizaciji i mnoge druge. Nesporno je da web stranice na društvenim mrežama dobivaju na popularnosti, a broj korisnika brzo raste. Međutim, s ovim povećanjem raste i sigurnosni prijetnji koji utječe na privatnost, identitet i povjerljivost korisnika.

Iako su veoma brojne, sigurnosne prijetnje na društvenim mrežama se mogu podijeliti u četiri grupe:

- prijetnje privatnosti,
- prijetnje mrežama i podacima,
- prijetnje identitetu i
- društvene prijetnje.

Veće količine podataka koje se dijele na korisničkom profilu podrazumijevaju veću vjerojatnost zlouporabe podataka ako su u posjedu takvih podataka. Otkrivanjem informacija online, korisnici su izloženi mnogim opasnostima. Korisnici ostavljaju veliku količinu podataka, izravno ili neizravno, koje se mogu koristiti za povezivanje korisničkog profila sa stvarnom osobnošću.

Privatnost može biti složen pojam za definiranje, ali radna operativna definicija privatnost shvaća kao pravo kontrole pristupa osobnim podacima. Pravo na privatnost stoga se može definirati kao pravo na kontrolu ispravnog protoka osobnih podataka. Drugim riječima, treba imati pravo razumno vršiti kontrolu nad načinom i s kime se informacije dijele.

Međutim, iako pristup privatnosti ima pozitivne aspekte, to također može imati negativne posljedice. Stoga, s jedne strane, privatnost omogućuje ljudima da budu samostalniji, kreativniji, slobodniji, individualističniji i štiti dostojanstvo ljudi i štiti ljude od kršenja njihovih osobnih podataka. S druge strane, međutim, privatnost omogućuje i iskorištavanje, uključivanje u nejednakosti, tajnost i netransparentnost.[1]

[1] King, J.; Lampinen, A.; Smolen, A. (2011) Privacy: is there an app for that? In Proceedings of the SeventhSymposium on Usable Privacy and Security, Pittsburgh, PA, USA, 20–22.

3. IMPLEMENTIRANJE INFORMACIJSKE TEHNOLOGIJE U POSLOVANJE

S obzirom na brzi napredak i povećanu ovisnost o tehnologiji, pitanje kako mijenja posao i zaposlenost za znanstvenike je vrlo značajno pitanje organizacijske psihologije i organizacijskog ponašanja (OP / OB).

U kontekstu korištenja informacijske tehnologije u organizacijama za dobivanje poslovne vrijednosti, ljudske radnje stvaraju i mijenjaju tehnologiju, a ljudi tehnologiju također koriste da bi izveli pojedine akcije. Ovaj rekurzivni pojam tehnologije ono što se naziva dualnošću tehnologije.[2]

Orlikowski tehnologiju vidi kao produkt ljudskog djelovanja (što bi željeli postići), dok ona također pretpostavlja strukturna svojstva. Odnosno, tehnologiju fizički konstruiraju akteri koji djeluju u određenom društvenom kontekstu, a tehnologiju akteri društveno konstruiraju kroz različita značenja koja joj pridaju i različite značajke koje ističu i koriste.[3]

Razumijevanje u kojoj mjeri ta tehnologija stvara vrijednost za organizacije ovisi o sposobnosti razumijevanja značenja koje akteri (uprava i zaposlenici) pridaju tehnologiji i kako je koriste. Ova interakcija je svjesna i refleksna. Prema tome, možda ne možemo shvatiti kako IT doprinosi poslovnoj vrijednosti zanemarujući ovaj pojam interaktivnosti između tehnologije i aktera.[4]

Sadašnji tok istraživača vrijednosti IT-a, iako priznaje sinergiju između resursa i korisnika resursa, ne usvaja filozofsko stajalište koje omogućava bogatije razumijevanje ovog fenomena. Pretežno pozitivistički pristupi uzimaju koristi da su neovisni o korisnicima tehnologije u organizacijama. Većina nematerijalnih koristi proizvod je ove interaktivnosti između tehnologije i aktera, a interpretativni pristup je prikladan za dublje razumijevanje fenomena, koji će pružiti bolje razumijevanje načina na koji organizacije manifestiraju te koristi.[5]

Razumijevanje interakcije tehnologije i korisnika te tehnologije otkriva da ima puno više koristi koje IT ulaganja mogu donijeti od općenito razumljivih opipljivih koristi. Te su pogodnosti više na „osobnoj razini“ i možda ne postoje „u vanjskom svijetu“. To je

[2] Orlikowski, W. (1992) The Duality of Technology: Rethinking the Concept of Technology in Organizations, Organization Science, 3, 3., str. 398.
[3] Ibid., str. 399.
[4] Ibid., str. 399.
[5] Ibid., str. 400.

ohrabrujuće, posebno za zemlje u razvoju u kojima lokalne i multinacionalne tvrtke ciljaju svoja ulaganja u IT na operativnoj razini. Uz ovo razumijevanje, kompanije u zemljama u razvoju trebale bi biti u stanju shvatiti potencijal IT-a u povećanju učinkovitosti procesa i poboljšanju cjelokupnog okruženja pružanja usluga te bi u konačnici trebali vidjeti neto koristi svojih ulaganja.

Jedno od mogućih ograničenja prethodnih studija koje su pružile neuvjerljive argumente za potencijal ulaganja u IT jest to da su ove studije pokušale razumjeti sposobnost stvaranja vrijednosti IT-a na površinskoj razini, ignorirajući tako rekurzivnu sinergiju između alata i korisnika alata. Pristup koji ima za cilj razumjeti što koristi tehnologije znače za korisnike pruža uvjerljiviji argument da IT ulaganja zaista doprinose poslovnoj vrijednosti, i što je još važnije, ima potencijal u poboljšanju uspješnosti poslovnih procesa u zemljama u razvoju.

Razumijevanje i uvažavanje nematerijalne koristi od ulaganja u IT također je važno za kontinuitet ulaganja u IT, što je presudno za zemlje u razvoju. Uobičajene mjere naknade na razini kompanije ne moraju uvijek ukazivati na stvarni potencijal ulaganja, jer su mjere proizvoda manipulacija.

Na primjer, u procjeni povrata potencijala inovativnih IT ulaganja, potrebno je prepoznati značajne troškove ove investicije, a svaka veličina povrata od ove investicije nepovoljno će se odnositi na veličinu ulaganja.[6] U takvim situacijama kompanije koje investiraju u zemljama u razvoju i razvijenim zemljama mogu bolje razumjeti doprinose svojih ulaganja u IT uzimajući u obzir njihove nematerijalne koristi i kako pomaže u stvaranju vrijednosti.

Percepcije poduzeća o nematerijalnim koristima od ulaganja u IT pružaju ugodne poticaje da bi kompanije mogle izvući vrijednost iz svojih IT ulaganja, posebno na razini procesa. Ovo je važno za kompanije koje su spremne uložiti u IT, ali mogu biti zabrinuti s neuvjerljivim dokazima o tome kako IT doprinosi poslovnoj vrijednosti. Prema kompanijama koje već ulažu u IT, ako iste planiraju daljnja ulaganja u IT, trebale bi vidjeti poboljšanje razine procesa, a u konačnici, to bi se trebalo odraziti na neto korist.[7]

Takva uvjerenja poslovne zajednice važna su za poticanje drugih poduzeća, posebno u zemljama u razvoju da najbolje iskoriste raspoložive IT resurse i cijene vrijednost koju inozemno ulaganje u IT donosi njihovim gospodarstvima. Za kompanije koje su uložile u IT,

[6] Dehning, B. and Richardson, V.J. (2002) Returns of Investment Technology: A Research Synthesis, Journal of Information Systems, 16, 1., str. 8.
[7] Ibid., str. 9.

ova studija daje poticaje za daljnje ulaganje u IT, jer uvažavanje i uporaba IT-a promiče tehnološku spremnost. Kontinuitet ulaganja u IT važan je u održavanju učinkovitosti procesa i usluga te može poslužiti kao osnova za daljnja strana ulaganja.[8]

Razumijevanje prirode prednosti IT ulaganja važno je pri procjeniti kako IT doprinosi poslovnoj vrijednosti. Prethodne studije uvelike su ignorirale mogući doprinos nematerijalnih prednosti IT ulaganja u razumijevanju na koji način doprinosi poslovnoj vrijednosti. Prethodne studije također su zanemarile važnost razumijevanja prirode i veličine IT ulaganja u širem kontekstu, poput zemalja u razvoju. Iskustva zemalja u razvoju u percepciji nematerijalnih prednosti ulaganja u IT sugeriraju da IT zaista doprinosi poslovnoj vrijednosti, a razumijevanje prirode nematerijalnih koristi od ulaganja u IT može pružiti bogatiji uvid u to kako IT doprinosi poslovnoj vrijednosti.[9]

3.1. Uloga informacijske tehnologije u poslovanju

Informacijska tehnologija postala je vrlo važna u poslovnom svijetu, bez obzira na to radi li se o malom, srednjem ili velikom poduzeću, IT je pomogao organizaciji, menadžmentu i radnicima u učinkovitijem menadžmentu da se raspitaju o određenom problemu, osmisle njegovu složenost i generiraju nove proizvode i usluge poboljšavajući na taj način vlastitu produktivnost i poslovni rezultat.

3.2. Komunikacija

U poslovnom svijetu komunikacija igra važnu ulogu u održavanju odnosa između zaposlenika, dobavljača i kupaca. Stoga, pomoću IT-a možemo pojednostaviti način komuniciranja putem e-pošte, video chat soba ili web mjesta društvenih mreža.

3.3. Upravljanje zalihama

Organizacije moraju održavati dovoljno zaliha da bi zadovoljile potražnju bez ulaganja u više nego što je nužno. Sustavi upravljanja zalihama identificiraju količinu svakog proizvoda koju kompanija održava, redoslijed dodatnih zaliha pomoću načina upravljanja zalihama. To postaje sve važnije jer organizacija mora održavati dovoljno zaliha da bi zadovoljila potražnju kupaca. Korištenjem IT-a u upravljanju zalihama također će pomoći u praćenju količine svakog proizvoda koje kompanija održava, aktivirajući se u upravljanju zalihama.

[8] Ibid., str. 10.
[9] Ibid., str. 11.

3.4. Prednosti informacijske tehnologije u poslovanju

Budući da se računalni sustav tako široko koristio, korisno je ugraditi informacijsku tehnologiju u organizaciju. Informatička tehnologija pruža ogromnu korist poslovnom svijetu, kao što je omogućavanje organizaciji da radi učinkovitije i maksimizira produktivnost.

Među prednostima informacijskih tehnologija u poslovanju jesu:

- spremanje i zaštita podataka;
- rad na daljinu;
- automatizirani procesi;
- komunikacija;
- spremanje i zaštita podataka.

Informacijska tehnologija pomaže u sustavima za pohranu važnih podataka ili dokumenata kako bi se zaštitili vrijedni podaci u poduzeću. Sustavi za pohranu, kao što su trezori, mogu pomoći u očuvanju podataka sigurnima samo tako što određenim korisnicima u poduzeću omogućuju pristup, povlačenje, dodavanje ili promjenu dokumenata.[10]

Sustavima informacijske tehnologije može se pristupiti i iz udaljene mrežne elektronike, što omogućuje rad od kuće ili s bilo kojeg drugog mjesta, slijedom čega pomaže povećati produktivnost.[11]

Svaka organizacija pronalazi načine za obavljanje više posla u kratkom vremenu. Stoga, učinkovitost informatičke tehnologije razvijaju se automatizirani procesi kako bi se uklonio teret sa zaposlenika.[12]

U poslovnom svijetu komunikacija igra važnu ulogu u održavanju odnosa između zaposlenika, dobavljača i kupaca. Stoga, pomoću IT-a možemo pojednostaviti način komuniciranja putem e-pošte, video chat soba ili web mjesta društvenih mreža. To znači da je moguće komunicirati sa zaposlenicima, dobavljačem i kupcima bilo gdje.[13]

Tema najnovijeg napretka u informacijskoj tehnologiji privukla je širok raspon članaka o tehnološkoj teoriji, primjenama iz mnogih aspekata i dizajnerskim metodama informacijske tehnologije. Pregledajući radove iz ove teme, jasno je da su uključena sva područja poput

[10] Vukičević, M., Odobašić, S. (2012) Upravljanje rizicima, Zaprešić: Visoka škola za poslovanje i upravljanje s pravom javnosti Baltazar Adam Krčelić
[11] Ibid.
[12] Ibid.
[13] Ibid.

računalne znanosti, računanja u oblaku, senzorne bežične mreže, predviđanja, objašnjenja slika i pohrane podataka. Nadalje, publikacija o centraliziranim vrijednostima informacijske tehnologije pokazala je neznatna nedavna kretanja u gore spomenutim poljima, koja su utemeljena i primjenjiva.

Također, lako možemo zaključiti da većina suradnika „informacijsku tehnologiju" smatra sinonimom za alate poput računala, mobilnih uređaja i tableta te pitanja poput mobilnog učenja, društvenih mreža i otvorenih izvora. Kroz razvoj teme, istraživački dizajni su prikladni za proučavanje potencijala primjene informatičke tehnologije u kontroliranim situacijama.[14]

Definicija informatičke informacijske tehnologije (IT), kako ju je definiralo Američko udruženje za informatičku tehnologiju (ITAA), je „istraživanje, dizajn, razvoj, implementacija, podrška ili upravljanje računalnim informacijskim sustavima, posebno softverskim aplikacijama i računalnim hardverom."[15]

Ukratko, IT se bavi upotrebom elektroničkih računala i računalnog softvera za sigurno pretvaranje, pohranu, zaštitu, obradu, prijenos i preuzimanje informacija. U ovoj se definiciji izraz „informacija" obično može zamijeniti s „podaci" bez gubitka značenja.[16]

Upotreba elektroničkih strojeva i programa za obradu, pohranu, prijenos i prezentaciju informacija. To je jednostavna definicija i usvojili su je istraživači iz područja IT-a.

Komunikacijska tehnologija

Internetska komunikacija područje je koje najbrže raste. Mogućnost razmjene podataka i informacija između svih koji su uključeni u građevinski projekt ovisi o komunikacijskim mrežama. Kada se protok informacija poboljša, može se poboljšati timski rad i koordinacija.

[14] Andrijanić, I., Gregurek, M., Merkaš, Z. (2016) Upravljanje poslovnim rizicima, Libertas – Plejada, Zagreb., str. 12.
[15] Ibid., str. 13.
[16] Ibid., str. 14.

4. INFORMACIJSKI SUSTAVI U JAVNOM SEKTORU

Koncept „upravljanje informacijskom tehnologijom“ postao je jedan od vitalnih i značajnih koncepata koji se koristi u raznim područjima društva. Pored toga, vladin računovodstveni informacijski sustav je značajan informacijski sustav koji koristi tehnologiju unutar vladinih jedinica. Iako su razvojem informacijske i komunikacijske tehnologije i elektroničkog vladinog sustava postigli različite prednosti vladinih jedinica, pojavili su se brojni relevantni problemi.

Najvažnije je da takav sustav ugrožava sigurnost računovodstva i rezultira elektroničkom financijskom manipulacijom. Sukladno tome, studija želi prikazati ulogu mehanizama upravljanja informacijskom tehnologijom u smanjenju tih rizika u svjetlu primjene elektroničkog vladinog sustava u vladinim jedinicama, teoretski na taj način smanjujući elektroničku financijsku manipulaciju.[17]

Vladine jedinice su najistaknutija poduzeća koja su pogođena komunikacijskom i informacijskom tehnologijom; upotreba komunikacijske i informacijske tehnologije rezultirala je pružanjem vladinih usluga te pripremom i razmjenom podataka. Danas se većina državnih usluga pruža putem web stranica putem primjene programa e-uprave.[18]

Primjena programa e-uprave pruža razne prednosti, uključujući usluge za uštedu vremena, elektroničku razmjenu podataka i dokumenata, pružanje vladinih usluga tijekom tjedna bez pauze i provođenje elektroničkih financijskih prijenosa.

Međutim, elektronički se državni sustav suočava s nekoliko poteškoća i rizika, od kojih je najvažniji nedostatak povjerenja korisnika u ove sustave. S gledišta kupaca, u ove sustave može se probiti; a podaci mogu biti uništeni. Osim toga, podaci koji se odnose na financijske transakcije mogu se mijenjati, kao i podaci o imovini. Osim toga, vladina financijska izvješća, podaci o poreznim prijavama, financijska izvješća koja se odnose na porezne prihode i carinske prihode mogu se neovlašteno pregledavati, manipulirati i mijenjati.[19]

Za rješavanje takvih rizika važna je primjena koncepata i mehanizama upravljanja informacijskom tehnologijom jer pridonosi ograničavanju tih rizika.

[17] Vukičević, M., Odobašić, S. (2012) Upravljanje rizicima, Visoka škola za poslovanje i upravljanje s pravom javnosti Baltazar Adam Krčelić, Zaprešić
[18] Ibid.
[19] Ibid.

Električna financijska manipulacija jedna je od najopasnijih metoda financijske korupcije s kojom se suočava proces pripreme vladinih računovodstvenih informacija. Što se tehnologija i komunikacija koriste u obradi i razmjeni podataka između vladinih jedinica, kupaca i korisnika u svrhu primjene e-uprave, to se više pojavljuju rizici elektroničke financijske manipulacije i sigurnosti podataka vladinih jedinica. Stoga se moraju osigurati metode koje doprinose smanjenju rizika od obrade podataka. Tu se pojavljuje potreba za primjenom mehanizama upravljanja.

Upravljanje informacijskom tehnologijom osigurava okruženje koje gradi odnos između informacijske tehnologije s dobavljačima s jedne strane i strategijama vladinih jedinica s njihovim ciljevima s druge strane. Osim toga, poboljšat će odluke na državnoj razini i stvoriti širi raspon transparentnosti i odgovornosti. Nadalje, upravljanje informacijskom tehnologijom osigurava mogućnost prepoznavanja i upravljanja informacijskom tehnologijom povezanom s rizicima i njenim primjenama.

Napredak u informacijskoj tehnologiji (IT) u prošlim desetljećima i, posebno, univerzalno proširenje i primjena poslovnog softvera u kombinaciji sa širenjem mrežnih tehnologija (Interneta) u posljednjih nekoliko godina, omogućili su poduzećima da podrže umjerene nedostatke preko tradicionalnih granica, uključujući i geografske granice.[20]

Prijedlozi ove reorganizacije rada koji su u razmatranju opsežni su i utječu na kompanije, radnike i, na kraju, na vladinu ili međunarodnu politiku. Doista, povratak koji su proizvele outsourcing suradnje na političkim poljima dokaz je koliko je ovo važno pitanje postalo i kompanijama i ekonomiji uopće.[21]

Novi tehnološki razvoj postavlja nove zahtjeve pred poduzeća, ili pruža nove mogućnosti za razvoj ili poboljšanje tržišnih aktivnosti kao i proizvoda. Jedan od primjera takvog tehnološkog razvoja je korištenje informacijske tehnologije među industrijskim kompanijama koje posluju.[22]

[20] Brynjolfsson E, Hitt L, Yang S (2002) Intangible assets:computers and organizational capital. Brookings Papers onEconomic Activity 1., str. 138.
[21] Ang S, Straub D (1998) Production and transaction economiesand IS outsourcing: a study of the U.S. banking industry. MISQuarterly 22(4)., str. 535-538.
[22] Deeter-Schmelz, D. R., Norman Kennedy, K. (2002) An exploratory study of the Internet as an industrial communication tool, examining buyers' perceptions. Industrial Marketing Management, 31., str. 145.

Postoji mnogo različitih informacijskih tehnologija, a samim time su i razne mogućnosti poduzeća da ih koriste tijekom obavljanja razmjene.[23]

Neka rješenja omogućuju korisnicima koji su geografski orijentirani i raštrkani za razmjenu baza podataka i poruka koje treba kopirati i odmah ih dostaviti ogromnom broju prijemnika. Korištenje, na primjer, elektroničke razmjene podataka (EDI) način je puštanja nekih tokova informacija u potpunosti putem informacijske tehnologije, poput naručivanja proizvoda i informacija o dostavi ili za plaćanje.[24]

Integrirani EDI povećava učinkovitost i omogućuje poslovnim odnosima uštedu vremena i smanjenje troškova.

Razvoj informacijske tehnologije u poslovanju privukao je pažnju istraživača posljednjih godina. Jedno utvrđeno stajalište o poslu u akademskom istraživanju jest proučavanje poslovanja između poduzeća, a to je izučavanje dugoročne orijentacije. Takvi poslovni odnosi sadrže elemente poslovnih, informacijskih i društvenih elemenata i postoji niz studija koje nameću utjecaj informacijske tehnologije na te različite elemente.[25]

Dok neki izjavljuju da informacijska tehnologija povećava učinkovitost odnosa, drugi istraživači navode negativan utjecaj informacijske tehnologije. Na primjer, utjecaj informacijske tehnologije na sadržaj industrijske razmjene razmatra više istraživača.

Istraživanja u ovom polju o tome kako informacijska tehnologija utječe na različite dimenzije odnosa je opsežna, ali specifično područje o tome kako informacijska tehnologija utječe na društvenu interakciju poslovnih odnosa dobiva malo pozornosti.

Kako se posao odvija između dviju poduzeća, ljudi iz njih sastaju se kako bi razmjenjivali informacije o svemu što se odnosi na proizvod i posao. S vremenom se dvije strane međusobno upoznaju i tako se u poslovnom odnosu kroz interakciju razvija socijalna dimenzija. Društvena interakcija uključuje susrete ljudi dviju poduzeća koje posluju, pa su susreti od interesa za proučavanje socijalne interakcije.

[23] Ibid., str. 146.
[24] Angeles, R., Nath, R. (2000) An empirical study of EDI trading partner selection criteria in customer-supplier relationships. Information and Management, 37., str. 241.
[25] Leek, S., Turnbull, P. W., Naude, P. (2003) How is information technology affecting business relationships? Results from a UK survey. Industrial Marketing Management, 32., str. 119.

Nedavni napori istraživača na području integracije informacijske tehnologije u poslovni odnos i utjecaj informacijske tehnologije na poslovne mreže dodali su nova znanja o poslovnim odnosima i mreže.[26]

4.1. Društvena interakcija i informacijske tehnologije

Izmjene poslovnog odnosa neminovno uključuju interakciju i društvenu aktivnost. Stranke se međusobno upoznaju dok međusobno komuniciraju.

4.2. Sastanci i informacijske tehnologije

Društvena interakcija poslovnog odnosa može se raspravljati u smislu koliko često se ljudi iz poduzeća sastaju ili koliko se dobro poznaju strane. Tvrdi se da ovisno o opsegu korištenja informacijske tehnologije za različite razmjene može utjecati na obrasce društvene interakcije koji se provode bez informacijske tehnologije. Jedan argument koji bi se mogao iznijeti u teoretiziranju o učinku uporabe informacijske tehnologije u poslovnim odnosima jest taj da će se broj sastanaka, odnosno potreba za sastancima smanjivati, jer upotreba tehnologije podnosi veliku razmjenu informacija, tj. zamjenjuje neke od osobne razmjene informacija.

Pitanje je smanjuje li se potreba za osobnim sastancima kada se povećavaju razine korištenja informacijske tehnologije. To bi sugeriralo povećanu efikasnost sastanaka, budući da upotreba informacijske tehnologije zamjenjuje druga sredstva interakcije za neke vrste razmjena. S druge strane, korištenje informacijske tehnologije može zahtijevati dodatne sastanke, ako je tehnologija teška za uporabu ili je svrha njezinog zapošljavanja drugačija od poboljšanja učinkovitosti razmjene informacija smanjenjem potrebe za sastancima. O razlozima zbog kojih bi se upotrebom informacijske tehnologije u poslovnim odnosima smanjila ili povećala potreba za osobnim sastancima može se samo nagađati.

[26] Dahlin, P. (2007) "Turbulence in Business Networks - ", Doctoral Dissertation No 53, School of Business, Mälardalen University, Sweden.

5. REVOLUCIJA U INFORMACIJSKOJ I KOMUNIKACIJSKOJ TEHNOLOGIJI

U posljednjih nekoliko desetljeća došlo je do revolucije u računarstvu i komunikacijama, a sve su naznake da će se tehnološki napredak i uporaba informacijske tehnologije nastaviti. Revolucija u informacijskoj i komunikacijskoj tehnologiji promijenila je ne samo naše živote, već i način na koji ljudi posluju. Koristeći informacijsku tehnologiju, poduzeća posjeduju potencijal da dosegnu više kupaca, brzo uvedu nove proizvode i usluge i surađuju s dobavljačima i poslovnim partnerima iz cijelog svijeta.

Transformacija iz industrijskog društva u informacijsko društvo i industrijske ekonomije u ekonomiju znanja rezultat je utjecaja upotrebe ICT-a i Interneta.

Informacijska tehnologija (IT) rasla je i evoluirala u posljednjih 50 godina; nije moguće promišljati i planirati projekt, posao ili neku drugu inicijativu bez korištenja ove tehnologije. Pod pojmom informacijska tehnologija podrazumijevaju se ne samo osobna računala ili pametni telefoni, već i suvremeni strojevi u tvornicama, automobilskoj industriji, zrakoplovnoj industriji, raznim kućanskim aparatima itd.

Istraživanja pokazuju da četvrtina radnika u Sjedinjenim Američkim Državama radi od kuće tijekom većeg dijela godine, dok još jedna četvrtina radi „mobilno“ – u pokretu. Prepoznaju se velike mogućnosti koje pružaju informacijska tehnologija i Internet kao važan alat za implementaciju u organizacijama i javnim institucijama. Ekonomisti visoko cijene važnost informacijske tehnologije za rast poslovanja, smanjenje troškova i promociju najboljih proizvoda.

Posljednjih godina globalizacija i informatizacija izmijenili su industriju, politiku, kulturu i društveni poredak. Globalizacija se odnosi na konačno integriranje ekonomskih i kulturnih institucija. Ova integracija nastaje kao rezultat uporabe informacijske tehnologije.

Tehnološka revolucija pretpostavlja globalne računalne mreže i slobodno kretanje roba, informacija i naroda preko državnih granica. Dakle, Internet i globalne računalne mreže omogućuju globalizaciju stvaranjem tehnološke infrastrukture za globalno gospodarstvo. Računalne mreže, satelitski komunikacijski sustavi, softver i hardver povezuju se i olakšavaju globalno gospodarstvo.[27]

[27] Douglas, K. (2002) Sociological theory. Vol. 20, No. 3., str. 285-305.

5.1. Pregled interneta kao resursa

Korištenje ICT-a također olakšava proizvodnju robe u kratkom vremenu uz pomoć računalnih informatičkih sustava, a usluge su brze i efikasne.[28] Informacijska i komunikacijska tehnologija poznata kao ICT tehnologija postala je glavni alat u poslovnim aktivnostima u suvremenom svijetu.[29] Internet postaje dio svakodnevnog života cijelog svijeta. U novije vrijeme elektroničko poslovanje razvilo se u važnoj poslovnoj disciplini.

„E" kao posljednje slovo u korištenju Interneta poprimilo je veliku važnost ne samo u svijetu informatičke i komunikacijske tehnologije, već i u poslovanju. Postalo je važna sastavnica za veliki broj područja istraživanja. Tako možemo spomenuti: elektronički marketing, elektronička trgovina, elektroničko upravljanje, elektronička trgovina, elektroničko učenje, tržište elektronike i drugo. Internet predstavlja tehnološku inovaciju, čiji se učinci kreću u rasponu od komunikacije do interakcije; međutim, njegov potencijal nije u potpunosti istražen i proučen.[30]

Prodaja se u Europi povećala tijekom 2010. u usporedbi s mrežnom prodajom u 2009 za 19,6% što čini 5,5% svih maloprodajnih poduzeća.[31]

Na temelju sljedećih podataka o korištenju interneta u svijetu u 2014. godini postoji više od 3 milijarde korisnika mreže, što predstavlja postotak od 42,3% cijelog čovječanstva. Informacijska tehnologija danas je postala redovita obilježje globalnog društva.

Globalizacija i informatizacija s jedne strane smanjuju nacionalni koncept, a s druge strane, omogućuju temeljito znanje. Informatička tehnologija i računalne mreže također omogućavaju globalnu ekonomsku, kulturnu i političku povezanost. Dvije sile snažno utječu na ekonomski i kulturni integritet. Tehnološke inovacije, posebno u području informacija i komunikacija, igrale su i dalje igraju središnju ulogu.

Globalizacija financijskih tržišta, lakši brzi transfer nezamislivih iznosa novca širom svijeta bio bi nemoguć bez ove tehnologije, baš kao što bi bila organizacija transnacionalne proizvodnje i puno više. Ogromno povećanje trgovine kao daljnjeg središnjeg elementa

[28] Miles, P. (2001) Globalization – Economic Growth and Development and Development Indicators. Planet Papers., str. 232.
[29] Dimovski. V., Škerlavaj. M. (2004) Comunication Technologies as Management Tools: Case of Slovenia", Faculty of Economocs University of Ljubljana., str. 636.
[30] Hoffman, L., Novak, I., Peterson, T. (1997) et al Services Quality, str. 123.
[31] Center For Retail Research (2010) E-Commerce and Online Retail. Dostupno na: http://www.retailresearch.org/onlineretailing.php (15.1.2020).

komercijalne globalizacije rezultira ne samo zato što su troškovi transporta naglo potonuli, a roba se mogla brže transportirati, već posebno zato što se proizvodi poput softvera ili baza podataka mogu slati iz jednog kraja svijeta u drugi preko podatkovnih linija u sekundi.

5.2. Elektronsko poslovanje

E-business (elektroničko poslovanje) sastoji se od vođenja poslovnih procesa na Internetu. Ovi elektronički poslovni procesi uključuju kupovinu i prodaju proizvoda, potrepština i usluga; servisiranje kupaca; obradu plaćanja; vođenje kontrole proizvodnje; suradnja s poslovnim partnerima; dijeljenje informacija; pokretanje automatiziranih usluga zaposlenika i više.

E-poslovanje može sadržavati niz funkcija i usluga, u rasponu od razvoja intraneta i ekstraneta do e-usluga, pružanja usluga i zadataka putem Interneta od strane pružatelja usluga aplikacija. Danas, kao velike korporacije, neprekidno promišljaju svoje poslovanje u pogledu Interneta, posebno njegove dostupnosti, širokog dosega i stalno mijenjajućih mogućnosti, oni vode e-poslovanje kako bi kupili dijelove i zalihe od drugih poduzeća, surađivali na promocijama prodaje i provodili zajednička istraživanja.

Informacijska tehnologija jedan je od relevantnih čimbenika koji danas pomaže poduzećima da prodru na nova tržišta zbog inovativnosti i proizvodnje novih proizvoda i usluga. Prije toga možemo doći do zaključka da je uloga informacijske tehnologije u proizvodnji novih proizvoda i usluga ogromna. Ako poduzeće na odgovarajući način identificira informatičku tehnologiju za svoje konkurentno poslovno tržište pružajući odgovarajuću softversku opremu, moći će obavljati organizaciju i akumulaciju podataka i informacija potrebnih za razvoj novih proizvoda i usluga.

Elektronsko poslovanje putem elektroničke pošte, glasovna pošta s videokonferencijama, podatkovne konferencije, telekonferencije i elektronička razmjena podataka omogućuju internetu koji je donio novi procvat u nagloj promjeni tržišta, gospodarstva, društva i politike promjenom proizvoda, usluga, ponašanja potrošača itd. Istodobno će se provoditi pravila europske i nacionalne konkurencije kako bi se osiguralo da male tvrtke imaju sve mogućnosti za ulazak na nova tržišta i nadmetanje pod fer uvjetima. Ključni elementi okoline uključuju[32]:

- globalnu infrastrukturu;

[32] European Commission (2004) Education for entrepreneurship: Making progress in promoting entrepreneurial attitudes and skills through primary and secondary education. Dostupno na: .http://europa.eu.int/comm/enterprise/enterprise_ policy/charter (15.1.2020)., str. 23.

- veze s dobavljačima;
- veze s kupcima / klijentima;
- veze s posrednikom.

Dakle, povezane s internetom, kompanije imaju priliku brže istraživati, izrađivati web stranice koje promoviraju svoje proizvode, prate ponašanje potrošača i razvijaju video konferencije. Vrijedno je spomenuti jedan od najrevolucionarnijih događaja u naprednim komunikacijskim tehnologijama, poput glasovnog protokola putem Interneta (VoIP), koji uključuje sve vrste govorne komunikacije koje se prenose putem interneta, između računala ili u hibridnom obliku između računala i običnog telefona.

Napredna računalna tehnologija je sofisticirana, iako je skupa i zahtijeva više vremena da je poduzeće implementira pa se poslovni procesi transformiraju iz fizičke u digitalnu stvarnost.

Informacijska tehnologija i pristup Internetu od strane malih i srednjih preduzeća u informacijskoj tehnologiji koriste se kao strateško sredstvo za kompanije kako bi poboljšali svoje konkurentske prednosti u vrijeme kada se neizvjesnost povećava.[33] Mnoga empirijska istraživanja prihvaćaju i podržavaju ideju da informaciona tehnologija može doprinijeti optimizaciji resursa poduzeća, ojačati, omogućiti i poboljšati poslovne rezultate.[34]

Informacijska tehnologija i Internet nisu samo važne značajke za olakšavanje komunikacije među ljudima, već su način na koji se stvaraju novi poslovni modeli, mijenjajući razvoj poslovanja i transformirajući ih na pozitivan način. Internet se može smatrati strateškim resursom na kojem tvrtke mogu promovirati svoj rad i usluge kao i proširiti se na nova tržišta.

Tvrtke koje koriste ovu novu tehnologiju mogu biti uglednije u obavljanju poslovnih aktivnosti i stvaranju konkurentskih prednosti. Elektronsko poslovanje promijenilo je ekonomiju, društvo i politiku. To je glavni razlog zašto su poduzeća koja su danas pooštrena konkurencija orijentirana na tržište ispunjavajući zahtjeve kupaca.

[33] King, W. R., Grove, V., Hufnagel, E.H. (1989) Using Information and Information Technology for Sustainable Competitive Advantage: Some Empirical Evidence. Information & Management, vol. 27, nr. 2., str. 93.
[34] Sethi, V., King, W. R.. (1994) Development of Measures to Assess the Extent to which an Information Technology Application Provides Competitive Advantage. Journal of Management Science, vol. 40, no. 12., str. 1601-1627.

Čovječanstvo je u svojoj povijesnoj evoluciji svjedočilo i aktivno sudjelovalo u razvoju više poljoprivrednih, industrijskih, tehničkih i znanstvenih revolucija. Sve su te revolucije imale utjecaja na ekonomski razvoj ljudskog društva. S druge strane, oni su donijeli i velike kvalitativne skokove što je s vremenom dovelo do poboljšanja životnog standarda ljudi na globalnoj razini. U današnjem poslovnom svijetu tehnologija se smatra važnim katalizatorom za restrukturiranje komercijalnih aktivnosti i strategije poslovnog razvoja. Digitalne tehnologije pokazale su se pokretačima gospodarskog rasta i konkurentnosti.

Povjesničari će sigurno pamtiti 21. stoljeće kao razdoblje neviđenih promjena u poslovnom svijetu. U nekoliko godina radikalno su se transformirale čitave industrije, pojavile su se stotine tisuća novih poduzeća, ogromno bogatstvo su izgubili ili osvojili poduzetnici i investitori. Sve su to rezultati digitalne tehnologije.

Nove tehnologije poput interneta, digitalne televizije, mobilnih telefona, kućanskih aparata i „pametne“ elektronike postale su uobičajena oprema. Ovo je otvorilo put za nove načine poslovanja, načine koji nisu viđeni od industrijske revolucije. Mnogi su ovaj postupak nazvali „e-business revolucija“ (elektronička poslovna revolucija), idejom koja je plijenila maštu mnogih poduzeća, vlada i ljudi diljem svijeta.

Praksa naprednih zemalja pokazala je da čak i upotreba novih tehnologija zahtijeva niz ulaganja u tehnička sredstva, posebno u ljudske resurse, prednosti e-poslovanja sve su vidljivije i na mikro i na makro razini. Nedostatak inicijative i uključenosti u proces prelaska na digitalnu ekonomiju može imati ozbiljne posljedice, kako na organizaciju preživljavanja / održavanja / razvoja, tako i na sektor gospodarstva, regiju ili državu u cjelini.[35]

5.3. Evolucija Interneta u svijetu

Internet može biti vrlo koristan alat za bilo koju kompaniju, veliku ili malu, lokalnu, nacionalnu ili globalnu, kada se upotrebljava na odgovarajući način. Za poslovno okruženje u svijetu, tehnološka revolucija koju predstavlja Internet, stvorila je planetarni okvir dizajniran tako da proizvođačima omogući otvaranje potrošačima širom svijeta i stalni interaktivni dijalog s njima. Ovo otvaranje potrošačima ima važne posljedice za svakog poslovnog čovjeka koji Internet smatra alatom za promicanje svojih interesa na nacionalnoj i međunarodnoj razini.

[35] Caraiani G., (2008)„TranzacYii internaYionale: E-business & tipuri de contracte”, Editura C.H. Beck, Bucure3ti

U smislu broja korisnika, posljedice Interneta sve su veće. Međunarodna statistika koju pruža Internet World Stats pokazuje da je svjetska populacija dosegla 7 milijardi, od čega su 2 milijarde korisnici interneta.

Internet pruža nerazvijenim regijama brojne mogućnosti za razvoj. Ako se pravilno koristi, može smanjiti postojeće ekonomske nedostatke puno lakše nego što je to moguće tradicionalnim sredstvima. Međutim, razumijevanje prednosti mora se staviti u kontekst globalne konkurentnosti.

Internet je stvorio mogućnosti i izazove za postojeće kompanije i start-up poduzeća koji imaju izravan odnos s kupcima. Što se tiče lanca opskrbe, pojavili su se neki posrednici, dok su drugi zamijenjeni. Pojavili su se novi poslovni modeli koji su organizacijama pokazali kako koristiti tehnologiju kako bi postigli konkurentsku prednost i veći prihod.[36]

Kako bi bila konkurentna, organizacija mora usvojiti nove tehnologije kako bi razvila niske troškove, uspostavila bliske odnose sa svojim potrošačima i razvila vjernost. Ne samo da su nove vrste proizvoda, već su tu i novi konkurenti, nova tržišta, istraživačke metode i drugo što potiče poduzetnike da budu cijelo vrijeme konkurentni, inovativni i kreativni. Putem Interneta organizacija može izgraditi ili povećati konkurentsku prednost, prednost koja se treba temeljiti na stvarnim činjenicama, koja je različita od ponude konkurencije i važna za potencijalne kupce.

Internet je brz, učinkovit i pun resursa koji svakome pomažu da pronađe ono što im u tom trenutku treba. Internetska prisutnost nudi ugled poduzećima, poboljšava vidljivost marke i povećava povjerenje potencijalnih kupaca u ponudu poduzeća. Najnovija istraživanja pokazuju da nedostatak internetske prisutnosti potiče kupce osjećaj da se bave malom i siromašnom tvrtkom, postajući suzdržani od kupovine proizvoda. Moderno poslovanje, bez obzira na veličinu, bez internetske prisutnosti nije samo lokalna tvrtka, bez ikakve praktične primjene na daljinu, bilo jednostavno implementirano poslovanje, bez puno perspektive vremena i prostora.

U knjizi E-shock 2000, lansiranoj 2000. godine, Michael de Kare Silver - vizionarski savjetnik Interneta - predložio je deset opcija za politiku maloprodaje kako bi preživjeli u takozvanoj novoj ekonomiji. Usvajanje interneta smatralo se ključnim za opstanak. De Kare Silver naglašava da opcije ne osuđuju fizičke prodavaonice na nestanak, već pokazuju kako se mogu prilagoditi povećanom stupnju interesa za elektroničkim kupovinom.

[36] Gay R, et all (2009) „Marketing online - o abordare orientata spre client", Editura: ALL

Integracija elektroničkog poslovnog sektora s tradicionalnim poduzećima može se ostvariti u odnosu na funkcionalna područja kao što su: proizvodnja, pronalaženje izvora, logistika, marketing, ljudski resursi, izvori ulaganja i financiranja, kriteriji uspješnosti.

Evo nekih načina na koji je tehnologija promijenila način rada tvrtke. Globalne vijesti odmah, globalni utjecaj odmah – vijesti, ideje i informacije putuju brže. Geografija više nije tako značajna – lokacija je faktor koji je sve manje važan za donošenje ekonomskih odluka. Poduzeća posluju na računalu gdje pronalaze najbolju ponudu u pogledu vještina i produktivnosti.

Od devet do pet postali su 24 sata dnevno, sedam dana u tjednu – sada poduzeća posluju u tri smjene, ovisno o tri glavne zone: Americi, Istočnoj Aziji / Australiji i Europi. Izraz „radni dan“ gubi svoje značenje u globalnom stanju u kojem se elektronička komunikacija može odvijati u bilo koje doba dana i noći.

Veličina je manje bitna – mala poduzeća sada mogu ponuditi usluge koje su u prošlosti samo velika mogla pružati. Osim toga, troškovi osnivanja poduzeća se smanjuju i kao rezultat toga, pojavit će se mnoga mala poduzeća.

Promjene korisničke usluge – pitanjima i naredbama koje i dalje vode telefonske službe mogu se upravljati putem interneta uz znatno niže troškove. Internet izravnava uvjete igranja – poduzeća koja vjeruju da male kompanije koje stvaraju mnogo buke na Internetu ne prijete njihovim osnovnim aktivnostima izgrađenim na godinama pažljivog planiranja i istraživačkih aktivnosti jačanja branda i marketinga. Internet je novopridošle aktere izjednačio s velikim korporacijama, omogućavajući im da se natječu za nova poduzeća.

Ljudi – dragocjeni resurs od najveće važnosti – glavni će izazov za poduzeća biti zapošljavanje, zadržavanje kvalitetnih ljudi i dobivanje vrijednosti koju mogu ponuditi. Poduzeća će morati uvjeriti najbolje zaposlenike da rad za njih povećava njihovu pojedinačnu vrijednost. Korištenje novih tehnologija kao glavne metode inovacija i aktivnosti restrukturiranja organizacije – bez obzira na profil aktivnosti, veličinu, članstvo u javnom ili privatnom sektoru – dobiva novu dimenziju u posljednjih godina, naime strateška. U posljednjem desetljeću, okruženje u kojem poduzeće raste se radikalno promijenilo: preuzimanjem kontrole od strane klijenta, koji ne podržava da ga se doživljava članom zajednice.

Globalna konkurencija promijenila je očekivanja kupaca, a razvoj digitalnih tehnologija promijenio je njihovo iskustvo. Kad su kupci kupovali samo u trgovinama, putem telefona ili naručivali putem pošte, njihova je mogućnost uspoređivanja kvalitete i cijena bila ograničena. Internet omogućuje pojedincima ili kompanijama da prouče sve ponude i kupuju na najjednostavniji način, od kuće ili s posla.

Internet mijenja svaki aspekt našeg života, ali na poslovno okruženje najviše utječu brze i značajne promjene. Danas i velike tvrtke i male kompanije koriste web za komunikaciju sa svojim partnerima, za povezivanje sa njihovim sustavima i bazama podataka i za obavljanje transakcija.

E-poslovanje postaje područje u kojem se snaga tradicionalne informacijske tehnologije integrira s internetom, kao i s novom vizijom vođenja poslovanja. Ovo nije samo način prodaje na Internetu, već pomaže poboljšati usluge kupcima, modernizirati opskrbni lanac i sve vrste prodaje, razvijajući odnose između posla i poslovanja. Automatizira postupak narudžbi, povećava broj tržišta, smanjuje troškove i ističe konkurentnost; omogućuje tvrtkama da analiziraju svoje potencijalne kupce i pravilno raspoređuju resurse i omogućuje da tvrtke budu aktivne 24 sata dnevno.

Tvrtke iz svih sektora počinju usvajati novu ekonomsku paradigmu – restrukturiranje za e-poslovanje. Prve tvrtke koje su usvojile ovu strategiju bile su iz sljedećih sektora: telekomunikacije, informacijske tehnologije, proizvodnja audio-vizualnih i multimedijskih sadržaja. Ova poduzeća postala su današnji „divovi“. No, tu su i nove male inovativne tvrtke koje su našle niše na tržištu internetskih usluga, multimedijskog sadržaja i softvera. Nova paradigma može se primijeniti u svim sektorima, već su poznati uspjesi u turističkoj industriji, bankarstvu, burzi, prodaji računala i softvera, prodaji knjiga i ostalom robom.

Usvajanje ove paradigme dovodi do značajnog povećanja produktivnosti i nižih troškova u svim sektorima tradicionalne industrije. S druge strane, digitalna revolucija ne znači samo korištenje Interneta kao platforme za elektroničku trgovinu. Pravi izazov tvrtkama je preuređivanje organizacije i poslovnih procesa kako bi se povećala produktivnost putem Interneta i osjetila njihova prisutnost na globalnom tržištu.

Informacijska tehnologija više nije produžetak poslovanja, postala je glavna pokretačka snaga promjena. Tradicionalni pristup da se informacijska tehnologija koristila za pomoć / automatizaciju trenutnih aktivnosti u organizaciji trenutno je zastarjela zbog:

- dubokih strukturnih promjena u proizvodnji dobara i usluga;
- primjena novog koncepta re-inženjeringa poslovnih procesa;
- razvoj informacijske tehnologije i internetskih aplikacija koje pružaju nove mogućnosti inovacija i podrške tim procesima.

Elektronička poduzeća nisu samo trend, već predstavljaju revolucionarni pristup koncepta „poslovnog poslovanja“. Postoje promjene u načinu korištenja podataka u kontaktu s kupcima, dobavljačima i zaposlenicima u marketingu, načinu promocije i tako dalje. Posljednjih godina možemo primijetiti širenje komercijalne aplikacije koja donosi prednosti javnim standardima poslovanja koje nudi Internet. Tvrtke koje posluju u različitim sektorima (bankarstvo, zabava, telekomunikacije, distribucija) mijenjaju način poslovanja kako bi iskoristili snagu novih tehnologija.

Vrata tehnologije bila su širom otvorena za novu globalnu ekonomiju, elektroničku. Međutim, mrežna poduzeća nisu jednostavno izgrađena na brzoj distribuciji informacija. Postoji i pretpostavka za kontinuirane promjene koje po svojoj prirodi zahtijevaju stalna poboljšanja i inovacije. Da bismo se natjecali, moramo inovirati brže od našeg konkurenta koji pokušava učiniti isto. I, naravno, može biti bilo gdje, u bilo kojoj zemlji svijeta.

6. INFORMACIJSKA TEHNOLOGIJA U GOSPODARSKOM SEKTORU

U današnjim poslovima, velike i male informacijske tehnologije su ono što pokreće mnoge nevjerojatne inovacije koje smo vidjeli tijekom posljednjih nekoliko desetljeća, uključujući sve, od šaltera na kojemu se prodaju karte do sustava upravljanja odnosima s kupcima poput Salesforcea koji su u središtu sve većeg broja poduzeća. Ali što je točno informacijska tehnologija i kako je ona odgovorna za jednu od najvećih poslovnih revolucija u povijesti trgovine? Informacijska tehnologija specifičan je sektor gospodarstva koji je odgovoran za izgradnju računalnih sustava, njihovo programiranje i upravljanje računalnim mrežama. Ono što informacijsku tehnologiju čini tako značajnim je upravo u nazivu: informacije i obrada podataka u informacije brzinom koja je eksponencijalno veća od onoga što je ljudski um sposoban postići.

To uključuje stvaranje tih podataka – koji se razlikuju od informacija, prikupljanje i učinkovito arhiviranje tih podataka i prijenos tih podataka kroz mreže. Podaci nam postaju korisne informacije nakon što smo ih analizirali i obradili, pa je informacijska tehnologija ujedno i razvoj mehanike te obrade ili analize, obično u obliku algoritama koji uzimaju podatke kao ulaz i proizvode korisne informacije kakve su nam potrebne.

Ovo je posebno važno za poduzeća, jer čak i male tvrtke komuniciraju s velikim brojem kupaca i, na taj način, svakodnevno proizvode tisuće ili desetke tisuća podataka.

Trgovci i vladini administratori odavno koriste tehnologiju za praćenje primitaka, cijena, poreza i zaliha. Prve tablične konstrukcije u Mezopotamiji bile su poslovni dokumenti koji su korišteni za praćenje broja roba kupljenih i prodatih. Dakle, od samog početka ljudskog pisanja, trgovina je bila pokretačka snaga tehnoloških inovacija.

Ove su inovacije urođene potrebom, pa kako su tehnologije razvijene za olakšavanje poslovanja trgovine i administracije kako je trgovina tisućljećima rasla, te su inovacije povećale učinkovitost poslovanja, što je oslobodilo resurse koji bi se mogli preusmjeriti na inovacije dalje i brže nego prije.

S vremenom je ta sve veća stopa promjene skratila vrijeme između glavnih inovacija, tako da je vremenska udaljenost između europskog doba istraživanja u 16. stoljeću i industrijske revolucije 19. stoljeća bila znatno kraća od vremenske udaljenosti između prvog broda koji je prešao Sredozemno more i prvog broda koji je prešao preko Atlantika.

Poduzeća su usko vezana za ove ubrzavajuće promjene i iskorištavaju ih da povećaju svoj komercijalni potencijal. Iako bi ovo moglo biti dovoljno jednostavno da se, s revolucijom informatičke tehnologije, shvati da se ubrzanje u ciklusu inovacija približava izvanrednom trenutku za razliku od svega što trgovina nikad prije nije vidjela.

Svaka industrija u gospodarstvu sada ima softversku platformu osmišljenu da iskoristi galaksiju podataka relevantnih za industriju, kojima tvrtke odavno imaju pristup, ali ne i pravi način da ih iskoriste.

Uz strojno učenje, ponašanje kupaca može se modelirati na temelju individualizirane povijesti kupovine kako bi se proizveli ciljani poticaji i reklame kojima bi se moglo zadovoljiti te kupce s preciznošću koja graniči s proricanjem. Čak i poljoprivrednici uviđaju kako aplikacije i softverske usluge koje ih informiraju o vremenskim uvjetima, uvjetima tla i tržišnim informacijama koje mijenjaju način na koji se radi u jednoj od najstarijih profesija čovječanstva. Sama telekomunikacijska revolucija omogućila je vrstu udaljenih radnih mjesta koja su transformirala način na koji ljudi pristupaju ravnoteži između posla i života.

Prošli su dani prostorija ispunjenih ormarima koji sadrže analogne, papirne podatkovne točke koje je posao akumulirao tijekom nekoliko godina ili čak desetljeća. Sada softverske platforme u oblaku mogu sve digitalno pratiti, čineći taj poslovni podatak vrijedan i u cijelosti dostupnim moćnim algoritmima koje tvrtka može koristiti kako bi pronašla nove načine zaraditi novac ili kako bi uštedjela na troškovima.

S umjetnom inteligencijom na horizontu, poduzeća se više svog poslovanja prebacuju na računalne sustave koji posao mogu obavljati učinkovitije i sigurnije nego ljudski radnici koje zamjenjuju. Ovo nadilazi razgovore oko automatizacije u proizvodnji tijekom posljednjih nekoliko desetljeća, ovi su novi sustavi zamijenjeni razmišljajućim radnikom, a ne ručnim radnikom. Na kraju nijedan sektor ekonomije neće ostati netaknut – čak ni sam sektor informacijske tehnologije.

7. RIZICI INFORMACIJSKE TEHNOLOGIJE

Informatičke tehnologije koje se danas koriste u kompanijama prate značajan društveni i ekonomski razvoj, ali one neizbježno podrazumijevaju i pojavljivanje nekoliko rizika koji trebaju biti uzeti u obzir.

Usvajanje informacijsko-komunikacijskih tehnologija u suvremenom društvu generiralo je strukturne promjene i vremenom izazvalo manje ili više zabrinutosti za zahtjevna brza rješenja. Pod tim okolnostima, tvrtke u današnje vrijeme trebaju procijeniti prednosti povezane s novim tehnologijama i u isto vrijeme smanjiti urođene rizike.

7.1. Prednosti i rizici povezani s e-trgovinom i e-poslovanjem

Širenje upotrebe Interneta u svijetu dovelo je do impresivnog razvoja e-trgovine i e-poslovanja. Trenutno se čini da je jedna od prilika tvrtke da se razvije, smanji troškove, poveća brzinu aktivnosti, poveća kvalitetu proizvoda i usluga kako bi stekla nova tržišta, postala globalna. Navedene su neke bitne prednosti za opseg poslovanja pomoću interneta:[37]

- vrijeme potrebno za dovršavanje transakcija je kraće;
- smanjeni su transakcijski i marketinški troškovi;
- pristup globalnom tržištu je lakši;
- komunikacija s klijentima i dobavljačima je fluidnija i učinkovitija;
- dostupnost posla 24 sata dnevno;
- klijenti se suočavaju s proizvodima i uslugama na jednostavan način.

Ako trebamo razmotriti rizike, u ovom slučaju možemo reći da je za e-trgovinu brzina pogreške i prijetnji emisija mnogo veća od one koja je suočena s tradicionalnom trgovinom i poslovanjem, zbog nepostojećih granica u *cyberspaceu*. Postoji više klasifikacija rizika e-trgovine i e-poslovanja. Za neke narode oni mogu biti unutarnji i vanjski, ljudski ili strojno stvoreni, namjeravani ili ne.

[37] Avison, D., Fitzgerald, G. (2002) Information System Development. Methodologies, Techniques and Tools, 4th Edition, The McGraw-Hill Companies, New York., str. 9.

7.2. Identificirane vrste rizika

Identificirane vrste rizika su[38]:

7.2.1. Rizici povezani s tehnologijom

Rizici povezani s tehnologijom su povezani s pristupom infrastrukturi e-trgovine. Njihova prisutnost može uzrokovati odstupanja od ciljeva izvedbe koji se očekuju u odnosu elektroničke razmjene. Na primjer, i internetski prodavač i njegov partner mogu pretrpjeti hakerske napade. Evo nekih od najpoznatijih metoda napada koji se koriste na Internetu:

- lažno predstavljanje - što znači „kloniranje“ web mjesta e-trgovine i „privlačenje“ kupaca, e-mail porukama ili drugim tehnikama, na kloniranu stranicu koja od korisnika traži da unese osobne podatke, lozinke ili brojeve računa;
- „slanje“ paketa - ostvaruje se kroz posebne programe, smještene u mrežnim računalima partnera. Ovi programi „špijuniraju“ i „prihvaćaju“ poruke, spremajući one važne u datoteku koja će se kasnije koristiti. Ovu vrstu programa hakeri koriste kako bi otkrili korisnička imena i lozinke korisnika web stranica e-trgovine;
- skeniranje - znači proučavanje određenih mrežnih topologija pomoću naredbi koje su specifične za TCP / IP protokol;
- odbijanje usluge – ovaj napad sastoji se u poplavi web poslužitelja podatkovnim paketima dok ovaj web-poslužitelj ne bude blokiran i odbije uslugu ovlaštenim korisnicima (slučajevi web-poslužitelja Yahooa i Amazona u veljači 2000. vrlo su poznati).

Sigurnosni jaz uslijed hakerskog napada može dovesti do gubitka prihoda ili narušavanja „imidža“ prodavatelja. S druge strane, protok informacija između partnera ima ranjive točke: interne aplikacije partnerskih tvrtki, aplikacijsko sučelje, mrežne veze, poštanske kutije itd. Ako se napadnu ove ranjive točke, može doći do prezentiranja ažuriranih podataka ili dezinformacija klijenata i, čak i ako se situacija odvije u kratkom vremenu, oni mogu tužiti prodavača ili zatražiti financijsku naknadu.

[38] Ratnasingam, P. (2003) Inter-Organizational Trust for Business-To-Business E-Commerce, IRM Press, U.S.A., U.K., str. 48-50.

7.2.2. Relativni rizici

One se preusmjeravaju na nedostatak povjerenja između poslovnih partnera. Među njihove uzroke možemo ubrojiti:

- nedostatak iskustva i tehničkog znanja o sigurnosti e-trgovine;
- oportunističko ponašanje;
- otpor na promjene;
- neznanje u vezi s načinom revizije aktivnosti e-trgovine;
- neizvjesnost u poslovnom okruženju;
- neznanje o načinima snimanja (arhiviranja, pohranjivanja, provjere) elektroničkih transakcija itd.

Neki primjeri rizika u ovoj kategoriji mogu biti: kašnjenje u procesu proizvodnje, prekinuti novčani tokovi, gubitak dobiti; sve to moglo bi utjecati na predviđeni dohodak i kontinuitet poslovanja.

7.2.3. Generirani rizici

Generirani rizici odnose se na:

- poslovne postupke slabe kvalitete;
- okolišni rizici;

E-trgovina i razvoj e-poslovanja doprinijeli su socijalnom i ekonomskom doprinosu u mnogim organizacijama, zemljama i na globalnoj razini. Korištenju njihovih specifičnih metoda i praksi moraju prethoditi studije izvodljivosti potrebne za prepoznavanje mogućih prijetnji kojima bi tvrtka mogla biti izložena, pokušaja njihove prevencije, jer je u većini slučajeva dokazano da je prevencija rizika jeftinija i mnogo efikasnija od budućeg rješavanje problema koji se mogu pojaviti. Nužno je spomenuti i da je u nekim situacijama dokazano da mogućnost prijetnje raste izravno proporcionalna obujmu transakcija i zbog toga se preporučuje postupno testiranje učinkovitosti ovih metoda i praksi.

7.3. Prednosti i rizici

E-poslovanje i e-trgovina bitno su transformirali poslovne procese u proteklim desetljećima, ali njihovo provođenje u optimalnim uvjetima nije moguće bez koherentnog informacijskog sustava, jamče kroz Enterprise Enterprise Resource Planning (ERP). Prednosti koje ERP aplikacije uključuju su višestruke i u posljednje vrijeme se primjenjuju na štetu aplikacija djelomično integriranih ili neintegriranih. Najvažnije od tih koristi ERP-a su[39]:

Ideja implementiranja ERP-a u tvrtku mora biti povezana sa studijom izvedivosti koja mora razlikovati ne samo prednosti, već i rizike. Evo nekih potencijalnih izvora rizika koji su zabilježeni između nedostataka i osobnog mišljenja dodanog o:

- ovisnosti o jednom dobavljaču – u mnogim situacijama ERP može biti kupljen od jednog dobavljača i tvrtka postaje ovisnost o njemu. U slučaju kada postoji više dobavljača za isti proizvod, moraju se uzeti u obzir prednosti jedinstvenog dobavljača suočene s prednostima više dobavljača. Prva opcija je pružanje mogućnosti dugoročnog ugovora; druga je mogućnost odabira najboljeg profesionalca u ovom području, ovisno o određenim pitanjima;

značajnim troškovima - oni se kreću od nekoliko tisuća do stotina tisuća ili milijuna dolara, ovisno o veličini tvrtke, vrsti aktivnosti, zemljopisnom proširenju i razini tehnologije u trenutku instaliranja. Najveći troškovi nastaju iz rekonfiguracije procesa, nakon čega slijede troškovi za pretvorbu podataka iz stare aplikacije u novu, troškovi softvera, obuka i hardver.[40]

Jedna važna stavka koja se također mora uzeti u obzir su „skriveni troškovi“ – neidentificirani prilikom donošenja odluke o instalaciji – na primjer troškovi obuke osoblja, integracije, testova, nezavršenih konzultantskih usluga, implementacija tima, smanjenja post-instalacije, analiza podataka, prilagođavanje;

3. U slučaju vertikalnih rješenja može se pojaviti neusklađenost njegovih modula – arhitektura i komponente sustava ne uvažavaju poslovne procese unutar tvrtke, strateške ciljeve i njegovu kulturu. Vertikalna rješenja predstavljaju rezultat ograničene fleksibilnosti ERP-a koji je usmjeren na razvoj specifičnih aplikacija, prilagođenih domenama aktivnosti svake tvrtke (zdravlje, komunikacije, obrazovanje itd.).

[39] O'Brien, J., Makaras, G. (2006) Management Information Systems, 7th Edition, The McGraw – Hill Companies, Inc., New York., str. 262.
[40] Ibid., str. 10.

4. Prilagodljivost – postaje rizik kada zaposlenici nisu spremni pažljivo analizirati i razumjeti kako bi aplikaciju koristili na pravilan način ili preuzeli odgovornost koja bi se mogla povećati za ovako složeno rješenje.

ERP-ovi su značajno izmijenili metode postupanja i nadzora administrativnih procesa, kao što su platni spiskovi, računi koji se plaćaju, zalihe, prodaja i potraživanja računovođa. Promjene su rezultat prelaska s ručnih postupaka koje izvode osobe koje su upoznate i sa podacima i s računovodstvenim postupkom; automatizirani procesi velikih količina, koje izvode pojedinci koji nisu upoznati ni sa podacima ni sa računovodstvenom praksom.[41]

Bitni uvjet za optimalnu implementaciju i korištenje ERP-ova je osiguranje rigoroznih kontrola, koje nude mogućnost otkrivanja pogrešaka ili prijevara s utjecajem na poslovanje. Ako je kontrolirani sustav neadekvatan, smanjuje se mogućnost prepoznavanja tih prijetnji i rizika, posebno u slučaju sustava stvarnog vremena, distribucije i baze podataka. Stoga je imperativ da se ti sustavi preispitaju tijekom primjene; kako bi se osiguralo da su od početka formirane odgovarajuće kontrole i sigurnost u ERP sustavu.[42]

7.4. Prednosti i rizici povezani sa sustavima upravljanja odnosima s klijentima

Uspjeh e-trgovine i e-poslovanja u potpunosti ovisi o sposobnosti tvrtke da inicira i održi odnos s klijentima na tržištu koje kontinuirano fluktuira. Upravljanje informacijama o kupcima postaje bitno u načinu na koji je tvrtka u svakom trenutku u stanju doći do informacija o tome što prodaje, kome, položaju ispred konkurencije, tržišnim trendovima, koliko su efikasni prodajni zaposlenici i koji predviđanja za dugoročno ili kratkotrajno su. Na ovoj razini rješenja za upravljanje odnosima s kupcima ometaju se u svrhu usmjeravanja protoka odnosa s međunarodnim klijentima i pružanju podrške i e-trgovini i e-poslovanju, kao i tradicionalnim gospodarskim aktivnostima. Širenje CRM rješenja razvilo je tri specifične domene: operativni CRM, analitički CRM i e-CRM (ili suradnički CRM).

Što se tiče rizika povezanih s korištenjem CRM tehnologija, mogu se uzeti u obzir s dvije točke gledišta: jasne i skrivene.

Skrivenim se rizikom smatraju oni koji su određeni „neprijateljskim“ događajima koji se ne mogu predvidjeti, poput:

- zloupotrebe kod korištenja određenih privilegija uslijed podjele zadataka;

[41] Musaji, Y. (2002) Integrated Auditing of ERP Systems, John Wiley & Sons, Inc., New York., str. 17.
[42] Ibid., str. 17.

- havariji sigurnosnog sustava putem njegove web stranice;
- prijevara, uključujući krađu podataka o kreditnim karticama;
- netočni podaci i informacije;
- neusklađenost s važećim zakonodavstvom;
- prekidi tijekom usluga pomoći nakon transakcije;
- nedostupna web stranica ili nudi netočne podatke;
- zloupotrebe ili prijevara u komunikacijskom sustavu;

Očigledni rizici razvijaju se kad predviđanja nisu ostvarena, a samim tim se ne postižu očekivane koristi:

- neuspjeh u ispunjavanju zahtjeva kupaca;
- propuštene marketinške kampanje;
- pokvarena lojalnost kupaca i tržišne stope se smanjuju;
- mali kapacitet za iskorištavanje prilika u stvarnom vremenu;
- niski prihodi rezultirali su nesposobnošću da predvidi potrebe kupaca

CRM je složena tema i presijeca odjela marketinga, prodaje, usluga, financija i logistike; dodatno, ima snažnu stratešku komponentu, koja zahtijeva uključivanje najvišeg menadžmenta.

Implementacija takvog sustava ima veliki utjecaj na informacijski sustav organizacije, jer klijent može uspostaviti vlastite račune, promijeniti kontaktne podatke i pregledati te račune, odobrenja za kredit mogu se automatizirati, faktura se može automatski generirati i plaćanje se može izvršiti online.

Istodobno, organizacija mora učiniti sve kako bi razvila i primijenila učinkovite kontrole za sve unutarnje i vanjske komponente uključene u poslovni proces. U tim uvjetima, slično kao što su e-trgovina, e-poslovanje i ERP sustavi, odluci o primjeni CRM sustava moraju prethoditi studije izvodljivosti koje su potrebne kako bi se razlikovalo koji rizici i prednosti donose organizaciji u skladu s područjem aktivnosti i tržište na koje organizacija vrši transakcije.[43]

Prednosti i rizici povezani sa sustavima upravljanja opskrbnim lancima

[43] Deshmukh, A. (2006) Digital Accounting. The Effects of the Internet and ERP on Accounting, Idea Group, Inc., Hershey., str. 139.

Najznačajnije koristi od transakcija e-poslovanja ovise o sposobnostima poduzeća da povećaju učinkovitost opskrbnog i prodajnog procesa putem aplikacija za upravljanje lancima opskrbe. Ovdje su glavne prednosti korištenja SCM aplikacije[44]:

Povećava preciznost u predviđanju opskrbe s 25 na 80%;

- smanjuje troškove opskrbe za oko 60% radom virtualnog poslovanja;
- smanjuje za oko 50% vrijeme posvećeno transakcijama;
- povećava zadovoljstvo kupaca smanjujući vrijeme isporuke sa 50% na 25%;
- steći strateške prednosti od suradnje s tvrtkama u istoj domeni djelatnosti, i drugima od 3% do 25%;
- povećava dobit s oko 30% poboljšanjem lanca dodane vrijednosti;
- povećava godišnji prihod s oko 55%, dijeli tržište između aktera iz različitih domena kroz interaktivne sustave i poboljšava odnose s kupcima pomoću politike e-trgovine.

Kao što je već spomenuto, SCM sustavi su složeni i oni integriraju više podsustava tvrtke. U tim okolnostima, rizici tijekom instalacije i primjene su neizbježni. Oni se mogu grupirati u tri glavne kategorije: normativnu, stratešku i operativnu.[45]

Nadalje je predstavljena ova klasifikacija s identificiranim rizicima za svaku klasu:

1. Normativni aspekti generiraju rizike jer:
- obrazovanje i kulturološke razlike izazivaju različite interpretacije;
- sudionici očito imaju različita mišljenja;
- nedostaje panoramski pogled;
- povjerenje između poslovnih partnera je dovoljno.
2. Strateški aspekti su generatori rizika jer su ciljevi i motivacije nespojivi, a vanjsko poslovanje generira rizike, poput:

Tehnički rizici - pitanje koje treba održati znanje u tvrtki i, istovremeno, učinkovito upravljanje vanjskim aktivnostima i sigurnost da dobavljač koristi odgovarajuće tehnologije i rješenja su obvezna. Ravnoteža između ta dva zahtjeva teško je postići.

[44] Beckmann, H. (2004) Supply Chain Management. Strategien und Entwicklungstendendenzen in Spitzenunternehmen, Springer-Verleg, Berlin., str. 190-191.
[45] Hertel, J., Zentes, J., Schramm-Klein, H. (2005) Supply-Chain Manangement und Warenwirtschaftssysteme im Handel, Springer-Verleg, Berlin., str. 16-17.

Komercijalni rizici - rezultat su urođene nesigurnosti u vezi s troškovima koji proizlaze iz eksternalizacije poslovanja;

Ugovorni rizici - određuju se mogućnošću nepostojanja odredbi u ugovorima s dobavljačima, može se pojaviti nemogućnost pokrivanja svih potreba tvrtke i utvrđivanja potrebnih resursa i ciljeva;

Rizici izvedbe - mogu proizaći iz nesposobnosti dobavljača da ispune zahtjeve ugovora.

3. Operativni aspekti generiraju rizike poput:

poteškoće u komunikaciji kroz sučelja sustava;

različite interpretacije partnera o standardima kvalitete i konceptu produktivnosti;

različita stajališta poslovnih partnera u vezi s poslovnim prilikama (na primjer: eksternalizacija tržišta se može smatrati najboljim rješenjem za partnera, a neznatna za drugog partnera);

nekompatibilnost da se primijete podaci iz različitih sustava;

kašnjenje u isporuci ili ažuriranju podataka.

Ukratko, upravljanje opskrbnim lancem uključuje niz složenih odluka, strateških do operativnih, koje se vrte oko pravog proizvoda, prave cijene, prave cijene, prave kvalitete, prave količine, prave lokacije i pravog kupca.[46]

Kao i u slučaju bilo koje informacijske tehnologije, primjeni SCM sustava moraju prethoditi studije o njegovoj mogućnosti i učinkovitosti, a dok se on koristi, potrebno je uspostaviti i slijediti stroge i cjelovite politike kontrole kako bi se izbjegla moguća pojava rizika u vezi s aspektima izravno povezanima s upotreba informacijske tehnologije i ekonomska. U praksi je dokazano da prednosti koje nude SCM sustavi zaslužuju pretpostavku rizika koji se mogu pojaviti prilikom njihove primjene i uporabe.

U suvremenom društvu riječi „zakona“ su: globalizacija, integracija i virtualnost, a sve se određuje korištenjem informacijskih tehnologija na različitim razinama.

Globalizacija je uvjetovana ujednačenošću ekonomskih, pravnih i financijskih standarda i propisa a što se može postići komunikacijom i međunarodnim sporazumima. Komunikacija je

[46] Deshmukh, A. (2006) Digital Accounting. The Effects of the Internet and ERP on Accounting, Idea Group, Inc., Hershey., str. 233.

ostvarena u znatnom udjelu u virtualnom okruženju, uključujući uporabu informacijskih tehnologija.

U tim okolnostima, instalacija ERP sustava, sposobnih da udovolje različitim zahtjevima korisnika informacija, koje nude kompanije i komunicira u stvarnom vremenu s poslovnim partnerima kroz sustave poput SCM ili CRM, dovršavajući transakcije zbog objekata generiranih iz elektroničkog okruženja „conditio sine qua non“ uvjet za tvrtke zainteresirane za širenje ili samo opstanak na tržištu tržišnog natjecanja. U tim uvjetima, za svaku tvrtku treba provesti studije za prepoznavanje najboljih poslovnih praksi i najboljih sustava koji nude maksimalnu učinkovitost upravljanja resursima i poboljšanje protoka informacija.

Ove studije moraju vratiti detaljnu sliku o prednostima i rizicima vezanim uz upotrebu takvih aplikacija. Očito je da je u tim uvjetima svojstveni financijski rizik gospodarskog života nadopunjen rizikom informacijske tehnologije. Na taj način postaje nužno da svakom implementacijskom procesu informacijskog sustava prethodi iscrpna i detaljna analiza rizika koja mora započeti proučavanjem strateškog plana organizacije, prepoznavanjem uloge koju tehnologija igra i identificiranjem kritičnih točaka postojećeg sustav.

Omogućavanje većine slučajeva, dok djeluju, mogu se pojaviti rizici koji nisu bili prvobitno predviđeni, jedna od mjera preporučenih bilo kojoj organizaciji, s izravnim utjecajem na njihove gospodarske aktivnosti, je porast strogosti unutarnje kontrole koja je u mogućnosti spriječiti rizika. Također, metode revizije, posebno u fazi procjene rizika, mogu imati veliki doprinos u izbjegavanju mogućih prijetnji.

8. RIZICI PRIMJENE INFORMACIJSKE TEHNOLOGIJE

Rizik je uobičajena terminologija usvojena u svakom području, uključujući informacijsku tehnologiju / sustav (IT / IS). IT se odnosi na raspoloživa tehnička sredstva – opremu i prateće tehnike, koje su u osnovi orijentirani na aktivnosti, orijentirani na nabavu te tehnologiju i dostavu. S druge strane, IS su poslovne aplikacije, manje ili više temeljene na IT-u. Iako su u mnogim definicijama ponuđene iz različitih perspektiva, IT rizik u ovoj studiji usvaja definiciju IT rizika kao nesigurnost da predvidivi gubitak ili šteta mogu rezultirati takvim neizvjesnim vjerojatnim događajima.

Priroda informacijskog rizika u velikoj mjeri ovisi o vrstama imovine, informacija ili projekata. Svaki IT hardver, softver, sustav ili projekt ima svoj inherentni i slučajni rizik koji mu je svojstven. Ovo poglavlje klasificira IT rizik u tri vrste, i to:

1) tehnički i operativni rizik;
2) rizik od podataka i informacijske sigurnosti; i
3) organizacija, projekt i ljudski rizik.[47]

Sigurnosni zahtjevi za IT u modernim organizacijama mogu proizlaziti iz organizacije (radne prakse, korporativni propisi, organizacijske politike) ili iz okruženja (tržišni trendovi i akti o zaštiti podataka). Zbog toga postoji potreba za identifikacijom i provedbom sigurnosnih kontrola kako bi se osigurala zaštita imovine, podataka i informacija od potencijalnih prijetnji.

Ne mogu se razumno razviti politike i procedure informatičke sigurnosti bez jasnog razumijevanja sustava, imovine, podataka i informacija koje moraju biti zaštićene i koliko su vrijedne za poduzeće. Uz to, treba utvrditi vjerojatnost da će imovina biti ugrožena. Stoga je cilj analize IT rizika identificirati i procijeniti rizike kojima su izloženi IT / IS i njegova imovina u svrhu odabira odgovarajućih i opravdanih sigurnosnih mjera zaštite.

Analiza IT rizika provodi se u pet faza (temeljeno i na Zajedničkom tehničkom odboru 1 Međunarodne organizacije za standardizaciju i Međunarodnoj elektrotehničkoj komisiji (ISO / IEC / JTC1, 1996.):

- identifikacija i procjena imovine;
- procjena prijetnji;

[47] Ahlan, A. R., Arshad, Y. (2012) Understanding Components of IT risks and Enterprise Risk Management: A Literature Review" in Risk Management / Book 1", InTech Open Access Publisher

- procjena ranjivosti;
- procjena postojećih / planiranih zaštitnih mjera; i
- procjena rizika.

Upravljanje IT projektima nije oslobođeno od rizika koji nastaju iz različitih okolišnih izvora. Stoga je sveobuhvatno razumijevanje ovih mogućih rizika i stvaranje strateških politika za njihovo suočavanje jedan od temeljnih zahtjeva za uspješnu implementaciju IT projekata. Rizici s kojima se suočavaju tijekom implementacije IT projekata nisu samo povezani s financijskim aspektima.

Rukovoditelji IT projekata moraju prihvatiti ta temeljna pitanja s cjelovitijeg pogleda, a ne samo usredotočiti se na financijska pitanja. Kako bi se spriječilo da potencijalni problemi nastanu ili eskaliraju u veće razmjere, potrebno im je posvetiti ozbiljnu pozornost prije provedbe bilo kojeg IT projekta.

Znanje je prepoznato kao vitalni izvor inovativnim tvrtkama, konkurentska prednost i stvaranje vrijednosti. Znanje je ključni sastojak razvoja dinamičkih temeljnih kompetencija i, općenito, kao odlučujući faktor za tvrtke s globalizacijama za suočavanje s izazovima.

Tvrtke su sada prisiljene organizirati svoje projekte i svoje strukture. Mnogi od njih ovise o vlastitim resursima ili vanjskim resursima kako bi ostvarili svoje ciljeve i bili bolje pripremljeni za promjene u svom okruženju.

Nadalje, tvrtke se svakodnevno suočavaju s više vrsta rizika, jer promjene u svjetskom okruženju mogu dovesti do novih rizika. Izvor rizika razlikuje se od unutarnjeg ili vanjskog okruženja. Nesigurnost okoliša i ponašanja koji utječu na probleme praćenja rezultata suradnje na razini i riziku ulaganja.

Ako se tim rizičnim okruženjem ne upravlja na odgovarajući način, to može negativno utjecati na sadašnje i buduće korporacije. Iz tog razloga menadžeri moraju uzeti u obzir rizike koji mogu utjecati i oni moraju umanjiti svoj utjecaj na organizaciju.

Jedna od bitnih funkcija upravljanja informacijskom tehnologijom (IT) je upravljanje rizikom, koje ima za cilj osigurati sigurno okruženje za e-poslovanje, jer IT projekte karakterizira visok stupanj rizika.

Brza transformacija informacijskih tehnologija kombinira promjene u poslovnim procesima kako bi stvorili iznenađujuće pomake u troškovima, odnosu troškova i koristi i izvedivosti

konkretnih stvari. Podrška ovim različitim IT organizacijama koje se bave standardima objavile su različite metode upravljanja rizikom. Ove su metode djelomično ili u potpunosti usvojile poduzeća koja koriste informatičku tehnologiju, radi prepoznavanja, analiziranja i minimiziranja rizika za svoje IT aktivnosti.

Rizici s kojima se susreću IT projekti u osnovi nisu financijski rizici. Shvaćajući ove temeljne probleme u stvarnom smislu, a ne kroz njihov financijski utjecaj, menadžeri IT projekata mogu se brže riješiti problema prije nego što postanu glavni problemi koji prijete ciljevima projekta.

Praktičari razumiju da u projektima postoje i drugi rizici osim financijskog rizika. Rizik IT projekata, sastoji se od financijske, tehnologije, sigurnosti, informacija, ljudi, poslovnog procesa, upravljanja, vanjskog, pa čak i rizika od uspjeha (koji se događa kada je projekt tako dobro izveden da izvuče više transakcija nego što se očekivalo i ne uspije razmjeriti zahtjevima preopterećenja).

8.1. Rizik i nesigurnost

Poznati ekonomist i osnivač Chicago škole razlikuje rizik od nesigurnosti tako što povezuje rizik s „količinom osjetljivom na mjerenje“… „mjerljivom neizvjesnošću“ suprotstavljajući je stvarnoj neizvjesnosti „neizmjernoj“. mjerljivi i mjerljivi događaji nalaze se također u literaturi o upravljanju projektima. Rizik je povezan s „prepoznatljivim događajem koji će imati negativne posljedice, dok se neizvjesnost odnosi na izvor (rizika).[48]

Nesigurnost je situacija koja je izvor rizika – kontekst za rizike kao događaje koji imaju negativan utjecaj ili mogućnosti koje imaju blagotvoran utjecaj.

Proširenje posljedice identificiranog događaja na mogućnosti ima pohvalnu namjeru poticanja upravljanja prilikama, ali djeluje zbunjujuće kad se pokušava razlučiti rizik od nesigurnosti. Rizik mora sadržavati dva elementa, a to su neizvjesnost i gubitak.

RM se odnosi na strategije, metode i pomoćne alate za prepoznavanje i kontrolu rizika na prihvatljivu razinu.

Projekti informacijskog sustava uvijek i posvuda širom svijeta imaju reputaciju za neuspjeh, tj. neiskorištene, djelomično korištene, otkazane i mnoge druge čimbenike. Svaki se projekt

[48] Knight, H. (1921) Risk, Uncertainty and Profit. Dostupno na: www.econlib.org/library/Knight/knRUP.html (29.12.2019.)

razlikuje od drugog, čak i ako se radi o istom sustavu, jer svaki projekt ima svoje zahtjeve, upravljanje projektima, korisnike, kulturu organizacije, timske vještine i znanje i mnoge druge aspekte koji su izravno povezani s organizacijom, a ne s projektom sebe.

Stupanj neizvjesnosti projekta važna je dimenzija konteksta. Mnogi se izvori nesigurnosti mogu prepoznati generirajući različite razine nesigurnosti i potrebni su različiti odgovori uprave. Glavni izvor neizvjesnosti u IT projektima je neizvjesnost u pogledu opsega ili specifikacija projekta. Predloženi profil nesigurnosti projekta trebao je pomoći u određivanju stupnja nesigurnosti, od predvidive nesigurnosti koju može kontrolirati tradicionalno upravljanje rizikom tehnike nepredvidive neizvjesnosti i kaosa koji se mogu naći u nekim vrlo inovativnim projektima.

8.2. Upravljanje rizikom

Upravljanje rizicima proučavano je u različitim područjima, kao što su osiguranje, ekonomija, upravljanje, medicina, istraživanje poslovanja i inženjering. Svako se polje bavi rizikom na način koji je relevantan za njegov predmet analize, dakle, uzima određenu perspektivu.

S obzirom na ovu perspektivu, rizicima se može upravljati korištenjem osiguranja, čime se nadoknađuje subjekt ako se dogodi; njima se također može upravljati pomoću planiranja u nepredviđenim situacijama i na taj način se pruža put kojim se može dogoditi ako dođe do neželjenog događaja.

Neka se polja, umjesto usredotočenja na negativne događaje, primarno bave vjerojatnošću nastanka događaja. Na primjer, medicina se često fokusira samo na vjerojatnost pojave bolesti (npr. Srčani udar), jer negativna posljedica je smrt u mnogim slučajevima.

Financije prihvaćaju drugačiju perspektivu rizika, gdje se rizik izjednačava s varijancom raspodjele ishoda. Stupanj varijabilnosti rezultata (bilo pozitivnih ili negativnih) mjerilo je rizika. Rizik je ovdje definiran kao volatilnost vrijednosti portfelja. Ostala polja, poput osiguranja od nezgode, prihvaćaju rizik rizika kao očekivani gubitak. Oni definiraju rizik kao produkt dviju funkcija: funkcije gubitka i funkcije vjerojatnosti. Druga je važna razlika u analizi rizika.

8.3. Pojam endogenog nasuprot egzogenom riziku

Egzogeni rizici su rizici nad kojima nemamo kontrolu i na koje ne utječe naše djelovanje. Potresi ili uragani dobri su primjeri egzogenih rizika. Iako imamo određenu kontrolu nad

visinom štete odabirom građevinskih standarda, mi nemamo kontrolu nad pojavom takvih prirodnih događaja. Endogeni rizici su, s druge strane, rizici koji ovise o našem djelovanju.

9. PROCES UPRAVLJANJA RIZIKOM

Upravljanje rizikom je proces trajnog ciklusa koji uključuje aktivnosti za uspostavljanje, nadzor i osiguravanje stalnog unapređenja aktivnosti organizacije. Ovaj proces uključuje četiri glavne aktivnosti koje se moraju trajno primjenjivati i razvijati.

Dizajn sustava upravljanja uključuje identificiranje poslovnih zahtjeva, procjenu vjerojatnosti i utjecaja rizika, uključujući provedbu sigurnosne politike i odabir odgovarajućih protumjera za postojeće rizike.

Primjena sustava upravljanja uključuje primjenu kontrolnih mjera i radnih postupaka, raspodjelu resursa, postavljanje odgovornosti i provođenje programa obuke i podizanja svijesti.

Nadgledanje, pregled i ponovna procjena sustava upravljanja uključuju i procjenu učinkovitosti kontrola i radnih postupaka, poslovnih promjena, prethodnih izvještaja o incidentima i postojećih rizika.

Poboljšanje i ažuriranje sustava upravljanja uključuje ispravljanje utvrđenih disfunkcija ili uklanjanje neodrživih odluka ili primjenu novih mjera kontrole.

Upravljanje rizikom obuhvaća tri procesa:

1. Procjena rizika je postupak koji uključuje utvrđivanje kriterija pod kojima se provodi evaluacija (postupak postojećih prijetnji i ranjivosti i rizici povezani s njima, postupak koji se odnosi na utjecaj i vjerojatnost identificiranih rizika, postupci procjene rizika, postupci za identificiranje mjera za ublažavanje ili uklanjanje rizika, postupak odabira najboljih mjera za ublažavanje ili uklanjanje rizika) te identificiranje i procjenu rizika.

Ublažavanje rizika odnosi se na utvrđivanje optimalnih mjera za uklanjanje ili ublažavanje rizika, na planiranje, provođenje optimiziranih odabranih mjera, prema planu, i kontrolu ispravnosti postupka provedbe.

Ponovna procjena preostalog rizika sastoji se od procjene preostalog rizika nakon koraka ublažavanja rizika i utvrđivanja je li prihvatljiva razina ili trebaju li se provoditi dodatne mjere za daljnje smanjenje ili uklanjanje preostalog rizika, prije nego što organizacija može pravilno obavljati posao.

Postoje dvije uznemirujuće činjenice koje svaka velika organizacija mora prihvatiti. Prvo, da gotovo sigurno posjeduje komercijalno osjetljive informacije koje bi, ukoliko padnu u pogrešne ruke, mogle pokazati duboku štetu budućnosti poduzeća. I drugo, sofisticirani cyber-napad koji cilja ove podatke gotovo su uvijek uspješni. Nema jedinstvenih rješenja, najbolja opcija organizacije za otkrivanje i odvraćanje iscrpljivanja podataka od strane naprednih napadača je sveobuhvatna dubinska obrana, određena temeljitom procjenom cyber rizika. Stoga je potrebna identifikacija računalnih sredstava, njihovih ranjivosti i prijetnji onima koji su izloženi, kao i vjerojatnost nastanka i utjecaja istih, kako bi se odredile odgovarajuće kontrole za prihvaćanje, smanjenje, prijenos ili izbjegavanje pojave rizika. Stoga je važnost formalne metode za izradu analize rizika i ranjivosti.

Analiza rizika informacijske sigurnosti proučavana je iz perspektive revizije kroz duže vrijeme. Najčešći je pristup razvijanju skupa kontrolnih popisa za provjeru postojećih sigurnosnih elemenata i na temelju prosudbe revizora utvrditi rezultate procjena. Za potrebe ove studije primijenjena je metodologija zasnovana na matriksu, koja je predložena za analizu rizika informacijske sigurnosti. Model matričnog pristupa omogućio je razvoj kvantitativne analize u širokom opsegu.[49]

Ova metodologija korelira sredstva, ranjivosti, prijetnje i kontrole organizacije i određuje važnost različitih kontrola koje odgovaraju imovini organizacije. Sredstva organizacije definiraju se kao vrijednosti koje mora zaštititi. Imovina može biti opipljiva, poput podataka i mreža, i nematerijalna, poput reputacije i povjerenja. Proces evaluacije ogledao se u matrici rizika koja pokazuje identificirane elemente rizika i njihove odnose.

9.1. Identificiranje realnih prijetnji

Cyber-analiza rizika štiti organizaciju koja usvaja IT kao dio svoje vizije i misije od širokog spektra prijetnji osigurati kontinuitet poslovanja, minimizirati štetu i povećati povrat ulaganja i mogućnosti. Svaki proces koji podržava informacijski sustavi i mreže su važan dobitak organizacije.[50] Identifikacija prijetnji trebao bi pomoći menadžmentu da stvori kontrole kako

[49] Goel, S., Che, V. (2005). Information security risk analysis a matrix based approach. Dostupno na: http://www.albany.edu/~GOEL/publications/goelchen2005.pdf (15.1.2020.)
[50] Marcus, R., & John, B. (2000). Access Control Systems and Methodology Information Security Management Handbook, Four Volume Set: Auerbach Publications.

bi umanjio vjerojatnost i utjecaj rizika povezanih s ranjivostima i postojeće prijetnje informacijskoj sigurnosti.

Identifikacija i klasifikacija informatičke imovine koja postoji u ustanovi

1) primjena metodologije za procjenu rizika koja je dizajnirana za definiranje ranjivosti i postojećih sigurnosnih prijetnji i procjena rizika prema definiranoj skali.
2) predlaganje mehanizama upravljanja i kontrole koji umanjuju identificirane prijetnje i ranjivosti koje se nalaze u provedena analiza rizika,
3) priprema izvješća s preporukama u kojima su prikazani nalazi kako bi se omogućila definicija opisa sustav informacijske sigurnosti prilagođen stvarnosti organizacije.

Postojeći programi procjene rizika koriste suprotan način razmišljanja da bi razvili teoretska rješenja za minimiziranje prijetnji kršenjem sigurnosti uz minimalni trošak. Procjena rizika omogućava odrediti odgovarajuće protumjere u skladu s tri različite obrambene strategije povezane sa sigurnosnom politikom organizacije.

9.2. Odnos između prijetnji i rizika

Učinkovito upravljanje rizikom mora nužno znati situacije koje mogu utjecati na organizaciju, to jest:

- što treba zaštititi,
- koji se resursi smatraju kritičnim, i
- hoće li poduzete mjere očuvanja ili sprečavanja smanjiti negativan utjecaj.

Prijetnje su povezane s potencijalnim uzrocima koji mogu negativno utjecati na informacije, u mjeri u kojoj bi imovina mogla biti pogođeni posjeduju slabosti ili nedostatke u kontrolama koje ih štite. Potonji se koncept sažima u pojmu ranjivost koja, kada se iskorištava prijetnja, izlaže organizaciju riziku.

Taj će rizik nastati iz analiza njihove vjerojatnosti pojave i utjecaja na zaštićena dobra. Drugim riječima, nijedan sustav ne može biti ranjiv ako ne prijeti i ne postoji uvjet prijetnje za stavku, predmet ili sustav, ako nije izložen i ranjiv na potencijal radnju koja predstavlja takvu prijetnju. Odnosno, nema prijetnje ili neovisne ranjivosti jer se one uzajamno uvjetuju situacije definirane konceptualno neovisno u metodološke svrhe i za bolje razumijevanje rizika.

Općenito, pojam prijetnje odnosi se na latentnu opasnost ili vanjski faktor rizika sustava; izraženo matematički kao vjerojatnost da premašuje razinu pojave određenim intenzitetom, pod određenim uvjetima i za datu izloženost vrijeme. Ta se shema neprestano mijenja zbog ugradnje nove imovine, pojave prijetnji i ranjivosti otkriće zahtijeva stalnu pažnju profesionalaca posvećenih informacijskoj sigurnosti i predstavlja stalni izazov postići učinkovitu zaštitu informacija.

Prijetnja je svaki element koji, korištenjem ili iskorištavanjem ranjivosti, ugrožava sigurnost informacija ili računalnog sredstva.

Prijetnje proizlaze iz postojanja ranjivosti, bez obzira na to utječu li ili ne na sigurnost sustava. U redu na prijetnje identitetu u određenom računalnom okruženju, nakon što su poznati rizici i resursi koje treba zaštititi, te kako njihova šteta ili neuspjeh može utjecati na organizaciju, potrebno je identificirati svaku od prijetnji i ranjivosti koje mogu prouzrokovati štete za resurse[51]Kao što je već spomenuto, postoji izravna veza između prijetnje i ranjivost do te mjere da ako ni jedan ne postoji drugi. Postojeće prijetnje obično se dijele prema njihovim opsegu:

1) Okolišna katastrofa (Fizička sigurnost).
2) Prijetnje sustavu (logička sigurnost).
3) Mrežne prijetnje (komunikacije).
4) Prijetnje ljudima (insajderi-autsajderi).

Cyber rizik predstavlja sve veću prijetnju kako javnim tako i privatnim institucijama zbog potencijalno katastrofalnih učinaka na organizacijske informacijske sustave, reputacijski rizik i potencijalni gubitak povjerenja potrošača i dionika. Pojavom interneta i odgovarajućim širenjem informatičke tehnologije, tvrtke, neprofitne i vladine jedinice općenito su bile nespremne za prepoznavanje i rješavanje ovog rizika, ali prijetnja se s vremenom povećavala i u učestalosti i u ozbiljnosti i prirodi napadi su se također promijenili.

U mnogim ranim slučajevima počinitelji cyber napada i kampanja informacijskog ometanja prekidali su poslovne operacije samo radi vlastitog zabave ili su proboj u infrastrukturu korporativne informacijske tehnologije (IT) smatrali izazovom. Oni bi prkosili web

[51] Creasey, J., Glover, I. (2013). Cyber security incident response guide. Dostupno na: http://www.crestapproved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf (15.1.2020.)

stranicama ili rušili servere kako bi se pogoršali ili jednostavno izazovali druge cyber profesionalce kako bi dokazali da mogu to učiniti, a ne da profitiraju.[52]

Međutim, kako je internet rastao i e-trgovina procvjetala, pristup zaposlenika podacima kompanija povećavao se, a daljinski pristup internim računalnim sustavima postao je uobičajen, cyber napadači su se razvijali, postajali su sofisticiraniji i njihovi učinci postaju sve razorniji.[53] Trenutne cyber prijetnje i napadači sve su više usredotočeni na profit od posljedica njihovih napada i iskorištavaju ili podatke koje nezakonito dobivaju za privatni dobitak ili zahtijevaju isplate žrtvovanog poduzeća za vraćanje usluge, pristupa ili web stranica natrag u operativnu funkcionalnost.

Cyber rizik jedinstven je među ostalim operativnim rizicima poduzeća zbog svoje mobilne lokacije, opsega prijetnji i velikog utjecaja. Širenjem poslovnih usluga, sustava i podataka dostupnih putem interneta, cyber prijetnje poduzećima (javnim i privatnim) neizmjerno su porasle. Nadalje, tvrtke su sada shvatile da rizikuju stvaranje obveza iz bilo kojeg cyber događaja koji bi mogli utjecati na povezane usluge i proizvode (npr. krađa adresa e-pošte s Epsilona u travnju 2011. utjecala je i na korisnike brojnih drugih tvrtki, poput hotela Hilton, Citibank itd. bacio je reputacijski rizik ne samo na prvobitno poduzeće već i na njihove klijente, te je stvorio i povećanu potencijalnu pravnu odgovornost).

Efekat obrušavanja koji cyber-napadi mogu proizvesti može utjecati na dobavljače, krajnje korisnike i samu organizaciju, pa čak može imati i potencijal destabilizacije velikih razmjera gospodarstva ako bi meta cyber napada bila sistemski važna (poput sistemski važnih financijskih ustanove, komunalni operateri, postrojenje za pročišćavanje vode, prometna mreža itd.). Uz to, tehnike cyber špijunaže brzo se razvijaju, čineći poslovne tajne poduzeća također ranjivim na krađe konkurenata.

Kao i s mnogim drugim opasnostima s kojima se suočavaju tvrtke, osiguravajuća društva koja su se specijalizirala za pretpostavku rizika i udruživanje rizika, vidjela su potencijalnu financijsku priliku u ispunjavanju potreba upravljanja rizikom od cyber rizika pružajući police osiguranja dizajnirane za zaštitu ili naknadu štete od financijskih posljedica ovih Interneta - povezane prijetnje. Nekoliko osiguravajućih društava počelo je nuditi politike povezane s povezivanjem koje pokrivaju cyber informacije i kršenja sigurnosti.

[52] Hallam-Baker, P. (2008). Famous for Fifteen Minutes: A History of Hacking Culture. Dostupno na: http://www.csoonline.com/article/217058/famous-for-fifteen-minutes-a-history-of-hacking-culture (15.1.2020.)
[53] Rhemann, M. (2011) Cyber Trends. Dostupno na: http://trendsdigeststore.com/CyberTrends.aspx (15.1.2020.)

U početku, dok su osiguratelji probno ulazili na ovo novo tržište, bilo je teško generirati podatke o elektroničkim gubicima. Iako je pokrivenost internetskim osiguranjem još uvijek u povojima (u usporedbi s drugim vrstama osiguranja), osiguravajuće tvrtke u posljednjih nekoliko godina poboljšale su svoju sposobnost točnijih cjenovnih politika i predviđanja mogućih gubitaka. Te tvrtke, uključujući AIG, Chubb, Fidelity, Marsh i Lloyds iz Londona, napisale su pravila koja mogu zaštititi ili prenijeti različite aspekte rizika cyber prostora.[54]

Prijetnja od cyber rizika za poduzeća je sve veća. Federalni istražni biro (FBI) u SAD-u, sveučilišta i druge istraživačke organizacije duboko su se udubile u pitanja koja se odnose na cyber-sigurnost kao prijetnju vladama i privatnim korporacijama.

Zajedničko istraživanje instituta za računalnu sigurnost iz 2002. godine / FBI o cyber riziku otkrilo je da je 90 posto ispitanika otkrilo kršenja računala u protekloj godini, s prosječnim gubitkom većim od 2 milijuna USD po organizaciji. U tada relativno novom dobu informacijske tehnologije i Interneta, većina tvrtki nije bila adekvatno pripremljena za suočavanje s tim vrstama skupih gubitaka.

Do 2008. godine, međutim, istraživanje Instituta za računalnu sigurnost / FBI utvrdilo je da se prosječni gubitak smanjio na oko 300 000 dolara, što sugerira da su tvrtke i sigurnosni softver koji koriste postale sofisticiraniji u nastojanju da se nose s povećanom prijetnjom kriminalne cyber aktivnosti.

Istraživanje CSI / FBI iz 2008. također je pokazalo da su tvrtke značajno povećale svoj unutarnji proračun povezan s cyber sigurnošću, što dalje podrazumijeva da kompanije troše više novca, vremena i radne snage kako bi ublažile te rizike. Cyber prijetnje mogu zatvoriti elektroenergetske mreže, ukrasti informacije i intelektualno vlasništvo, otkriti ponude konkurencije i onemogućiti web stranice potrebne za poslovne aktivnosti, uzrokujući značajnu financijsku štetu nepripremljenim poduzećima. U skladu s tim, vjerojatno je da će se kompanije morati nastaviti usredotočiti na ta pitanja sigurnosti cyber rizika jer hakeri i dalje postaju sofisticiraniji što uzrokuje veće gubitke u poslovanju, internetskim uslugama i poslovanju, posebno ako tvrtke postanu više ovisne o internetu za e-trgovinu, mobilnu (ili m-) trgovinu ili jednostavno za svakodnevne operacije, administraciju i terenski kontakt sa zaposlenicima.

[54] Gordon, L., Loeb, M., & Sohail, T. (2003). A Framework for Using Insurance for Cyber Risk Management, Communications of the Association of Computing Machinery, Vol. 46, No. 3, str. 81-85.

Istraživanje CSI / FBI iz 2008. također je pokazalo da su kompanije značajno povećale svoj unutarnji proračun koji se odnosi na kibernetičku sigurnost, što nadalje podrazumijeva da kompanije troše više novca, vremena i rada kako bi ublažile ove rizike (Computer Security Institute, 2008). Cyber prijetnje mogu zatvoriti elektroenergetske mreže, ukrasti informacije i intelektualno vlasništvo, otkriti ponude konkurencije i onemogućiti web stranice potrebne za poslovne aktivnosti, uzrokujući značajnu financijsku štetu nepripremljenim tvrtkama. Prema tome, vjerojatno će se tvrtke morati nastaviti usredotočiti na ta pitanja cyber sigurnosti jer hakeri i dalje postaju sofisticiraniji, uzrokujući veće gubitke u poslovanju, internetskim uslugama i poslovanju, pogotovo jer tvrtke postaju ovisnije o internetu za e-trgovinu. , mobilnu (ili m-) trgovinu ili jednostavno za svakodnevne operacije, administraciju i terenski kontakt sa zaposlenicima.

Iako su određene tehnike ublažavanja rizika zajedničke za oba izvora prijetnji kibernetskim rizikom (npr. Sekuritizacija i zaštita lozinkom osjetljivih informacija ili tehnologija, segmentacija informacija i njezin pristup unutar organizacije itd.), Druge su tehnike prikladnije za jedan izvor rizika a ne drugo. Prijetnje koje predstavljaju svaki izvor rizika mogu biti različite i često zahtijevaju različite pristupe. Nadalje, kako se zemlje u razvoju bore za paritet s razvijenijim zemljama u pogledu elektroničkog pristupa Internetu i tehnološkog i industrijskog razvoja, tvrtke, neprofitne i vladine jedinice i institucije vjerojatno će vidjeti porast cyber prijetnji iz ovih izvora izvan kontrole ili nadležnost zemlje domaćina poduzeća. Raspravljat ćemo zauzvrat svaki izvor rizika.

9.3. Unutarnje prijetnje od cyber rizika

Ironično je da vrlo visok rizik od cyber zločina dolazi iznutra, a ne izvan organizacije. Iako zaposlenik može biti najveće bogatstvo tvrtke, zaposlenici su stalno izloženi ogromnim količinama povjerljivih informacija i po potrebi im se vjeruje s vlasničkim podacima tvrtke, zalihama i imovinom. Ponekad iskušenje za individualni dobitak može biti preveliko. Ili, zaposlenik koji je potrošio vrijeme na razvijanju važnih informacija o vlasništvu tvrtke, može osjećati da ima pravo na tu tvrtku inteligencija kao rezultat vremena provedenog u istraživanju i razvoju, razvoju proizvoda ili aktivnostima prenosa tehnologije. Posljedično, tvrtka može biti izložena krađi podataka ili intelektualnom vlasništvu iznutra, a ne izvana.

Krađa podataka je izraz koji se upotrebljava kada se podaci ilegalno kopiraju ili preuzimaju od poslovne ili druge osobe. Krađa podataka, formula i procesnih informacija zaposlenika može kompromitirati poduzeće jednako lako kao i napad vanjske krađe podataka, no zbog

privilegiranog položaja zaposlenik ima veću mogućnost djelovanja kao počinitelj, jer već ima povjerenja u dozvolu ili zaporku. cyber sustav poduzeća iz opravdanih razloga, dopuštenje da se tada mogu okrenuti protiv svog poslodavca.

U stvari, FBI izvještava da je krađa zaposlenika najbrže rastući zločin u Americi. Američka gospodarska komora procjenjuje da je oko 75 posto zaposlenika kralo od svog poslodavca, pri čemu je otprilike 30 posto bankrota poduzeća izravno rezultat krađe zaposlenika. Većina uključenih pojedinaca zaposlenici su višeg stupnja i prosječno je vrijeme do otkrića približno 18 mjeseci, što daje znatno vrijeme za financijsku štetu.[55] Poduzeća moraju biti oprezna prema internim cyber prijetnjama koliko i prema vanjskim prijetnjama.

[55] Burke, R., Cooper, C. (2010) Risky Business, Psychological, Physical and Financial Costs of High Risk Behavior in Organizations, Gower Publishing, Surrey, England., str. 433.

10. ZLOUPORABA INFORMACIJSKE TEHNOLOGIJE

Riječ 'IT' označava informacijsku tehnologiju i ona se definira kao dio inženjeringa koji doprinosi stvaranju i proučavanju računalnih sustava i računalnih aplikacija, te kao dio telekomunikacija, pomažući pri pronalaženju, pohranjivanju i prijenosu podataka. U ovom su vremenu mnoge nemoguće stvari postale moguće uz pomoć informacijske tehnologije. Zapravo su mnoge organizacije kompjuterizirane i u svakodnevnoj rutini koriste informacijsku tehnologiju na mnogo načina. Upotreba IT-a postala je dio svačijeg života.

Informaciona tehnologija ima mnoštvo normi i pravila koja treba slijediti i poštivati. Ovdje etika informacijske tehnologije stupa na snagu. Etika je reflektivno proučavanje opće prirode moralnih vrijednosti, pravnih i društvenih pitanja. Postoje neka pravila koja treba slijediti i koja su standardna za usmjeravanje i kontrolu ponašanja pojedinca na profesionalnoj razini. Većina profesionalnih organizacija koje se bave računanjem objavila je etički kodeks.

Kompjuterski kriminal vrlo je opsežna tema. Uključuje mnogo zlonamjernih funkcija od strane korisnika računala. Sve se odnosi na loše korištenje informacijske tehnologije radi osobnog interesa ili u stvaranju problematične situacije za druge.

Plagijarizam je jedan aspekt. To je prenos drugih ljudi kao vaš vlastiti, bez davanja ikakvog zasluga za njih. Piratstvo je druga tema o kojoj treba razmišljati, jer ljudi ulažu mnogo truda i troše puno novca da bi stvorili ili napravili nešto tamo gdje drugi samo kopiju kopiraju od trenutka kupnje originalnog. Krekeri su u osnovi pažnja koja se probija u računalni sustav i nelegitimno ih koristi. S brzim razvojem informacijske tehnologije, broj krekera također raste. Vrlo je teško doći do svih ovih pitanja i zato imamo neko udruženje koje ima za cilj smanjiti i zaustaviti te probleme.

„Mnoge su profesije osnovale profesionalna društva koja su usvojila kodekse ponašanja. Na primjer, medicinska struka osnovala je AMA (American Medical Association), a pravna struka osnovala ABA (American Advokatska komora) ”(Tavani 2007, str. 100). Ove dvije udruge bave se kodeksom ponašanja svojih članova. Udruženje za računske strojeve (ACM) i Institut inženjera elektrotehnike i elektronike-računalno društvo (IEEE-CS) primjeri su profesionalnih društava prepoznatih od strane računarstva. Udruženje profesionalaca za informatičku tehnologiju (AITP) bavi se razinom ponašanja profesionalaca.

11. ZAŠTITA PRIVATNOSTI I SIGURNOSTI POHRANJENIH PODATAKA

Primjena novih tehnologija (posebno informacijskih i komunikacijskih tehnologija) u svim područjima ljudskih aktivnosti, od gospodarstva, obrazovanja, znanosti do kulture, sporta i više, pokretač je društvenog i ekonomskog razvoja i prosperiteta svake zemlje. Brz i jednostavan način prikupljanja, pohrane, obrade, prijenosa, razmjene, pristupa i korištenja velikih količina svih vrsta podataka i informacija svakodnevna je pojava u gotovo svim segmentima ekonomskih i društvenih aktivnosti.

Sve veći zahtjev i potražnja za informacijama rezultirali su stvaranjem niza baza podataka. Većina pohranjenih podataka odnosi se na osobne (privatne) podatke pojedinaca. Gotovo da nema institucije ili tvrtke koja ne koristi takve baze podataka. Koriste ih vladina tijela, agencije i institucije u svrhu snimanja i izrade različitih analiza, izvještaja i povezanih programa. Prikupljajući podatke o potrošačima, kupcima i dionicima, tvrtke nastoje prilagoditi proizvode i usluge njihovim potrebama i poboljšati svoje poslovanje.[56]

Ljudi su posebno osjetljivi kada bilježe svoje intimne podatke (na primjer, zdravstveni i seksualni život, etničke ili vjerske podatke, socijalni status, podatke o broju socijalnog i zdravstvenog osiguranja, JMBG, broj bankovnog računa, brojeve kreditnih kartica), stoga ih se obvezuje na vlasnici takvih podataka kako bi ih zaštitili i tretirali s pažnjom prilikom obrade, pohrane ili ažuriranja.[57]

Nedavne digitalne multinacionalne tvrtke u različitim nacionalnim i institucionalnim okvirima postavljaju pitanja koja zahtijevaju nove pristupe u međunarodnim poslovnim studijama.

Među narodima raste zabrinutost zbog moći digitalnih korporacija. Budući da internetska digitalna ekonomija postaje univerzalno dostupna, sposobnost vlade da nadgleda, kontrolira ili zaustavlja digitalne aktivnosti ozbiljno potkopana. Iako je infrastruktura internetska i ljudska bića koja upravljaju podliježu zakonskim jurisdikcijama, protok informacija preko granice je teško kontrolirati.

[56] Frančula, Nedjeljko i Lapaine, Miljenko (2009). Information Sources and Cartography. Sveučilište u Zagrebu, Zagreb., str. 12-14.
[57] Sudar-Kulčar, M. (2005) Zaštita privatnosti i sigurnost pohranjenih podataka s osvrtom na izravni (direktni) marketing. Politička misao, vol.42,br.4., str. 102-104.

Sudjelovanje u međunarodnom poslovanju putem interneta zahtijeva od vlada da usvoje međunarodno poslovanje, zakone i propise koji osporavaju njihov suverenitet, a čija je bitna osobina kontrola nad fizičkim prostorom i objektima unutar njega.[58]

Takve zabrinutosti povećale su upravljanje internetom kao kritičnom javnom politikom. Prema Radnoj grupi za upravljanje internetom (WGIG), postoje četiri područja koja su središnja za upravljanje Internetom[59]:

(1) pitanja vezana za infrastrukturu i upravljanje kritičnim resursima;
(2) pitanja koja se odnose na upotrebu Interneta;
(3) pitanja koja su relevantna za Internet, ali imaju utjecaj u mnogo širem obujmu; i
(4) pitanja vezana za razvojne aspekte upravljanja Internetom, uključujući izgradnju kapaciteta u zemljama u razvoju.

Kasnije je dodano peto područje na temelju promatranja upravljanja Internetom u Kini: regulacija sadržaja, središnji fokus kineske pravne, tehničke i samoregulacije Internet mehanizam.

Oko 100 Amazonovih trgovaca bilo je žrtva šestomjesečnog krađe u 2018. Amazon vjeruje da su trgovci bili prevareni u predaji podataka u prijavi na svoje račune. S obzirom na sofisticiranost današnjih phishing e-poruka koje iskorištavaju informacije o pojedincima dostupnim iz prethodnih kršenja različitih tvrtki, lako je vidjeti kako ih se može prevariti.

Novac prodavača Amazona prebačen je na vlastite račune prevaranta, a Amazonovi odvjetnici tražili su dozvolu za pristup izvodima banaka navodnih prevaranta.

Čini se da bi to bio posao za provedbu zakona, ali prevare u Amazonu možda nisu prioritet takvim agencijama. Izgleda da Amazon vjeruje da se ne može osloniti samo na provođenje zakona. Treba li istražiteljima prijevara u privatnim tvrtkama omogućiti pretragu bankovnih zapisa pojedinaca, čak i onih koji pripadaju sumnjivim prevarantima?

[58] Hathaway, M. (2014) Connected choices: how the Internet is challenging sovereign decisions. America Foreign Policy Interests, 36(5)., str. 300–313.
[59] de Bossey, C. (2005). Report of the Working Group on Internet Governance (WGIG). ITU. Dostupno na: https://www.wgig.org/docs/WGIGREPORT.pdf (15.1.2020.)

12. CASE STUDY: AMAZON

Nedavni napredak svjedočio je uspjehu i popularnosti računalstva u oblaku, što predstavlja novi poslovni model i paradigmu računalstva. Značajka pružanja resursa za računanje, pohrane i propusnosti na zahtjev dovela je moderna poduzeća u oblačne usluge.

Oblak se smatra vrhunskom tehnologijom, a na njega se oslanjaju samo mnoge velike tehnološke, poslovne i medijske kompanije poput Netflixa ili Salesforce.com. Međutim, osim koristi koje imamo, sigurnosna pitanja dugoročno su briga i glavna su prepreka širokoj upotrebi računalstva u oblaku.

Tri su glavna izazova za izgradnja sigurnog i pouzdanog oblaka:

Outsourcing smanjuje i kapitalne izdatke i operativne izdatke za korisnike oblaka. No, outsourcing također ukazuje da korisnici oblaka više ne zadržavaju fizičku kontrolu nad hardverom, softverom i podacima. Da bi se riješio ovaj izazov, očekuje se pouzdan oblak, što znači da korisnici oblaka mogu provjeriti podatke i računati u smislu povjerljivosti, integriteta i drugih sigurnosnih usluga.

Multi-zakupništvo znači da oblak dijeli više kupaca. Virtualizacija dobavljača u oblaku uvelike koristi da optimiziraju raspodjelu resursa i upravljanje njima. Česta, ali rizična situacija je da podaci koji čeznu za različitim kupcima mogu biti pohranjeni u istom fizičkom stroju. Protivnici mogu iskoristiti ovu vulnerabilnost za pokretanje različitih napada poput kršenja podataka / računanja, napada poplava itd.

Ogromni podaci i intenzivno računanje dvije su druge značajke računalstva u oblaku. Stoga, tradicionalni sigurnosni mehanizmi možda neće biti dovoljni za nove sigurnosne zahtjeve zbog nepodnošljivog računanja ili komunikacije nad glavom.

Kratki pregled je jednostavno sigurnosna kopija ili kopija podataka o količini instance. Za snimanje podataka u instanci može se upotrijebiti snimak, sličan vraćanju iz sigurnosne kopije. Kratki pregled obično nije spremljivi oblik za pohranu

EBS je novi oblik pohrane podataka. EBS je virtualno spremanje podataka koje djeluje identično volumenu, ali podaci se mogu proširiti na više fizičkih tvrdih diskova i mogu se brzo i lako premjestiti. Motivacija EBS-a je povećati učinkovitost pohrane u oblaku. Davatelji usluga u oblaku tada mogu prodati ostatak prostora za više klijenata. Uz to se EBS može sastojati od više volumena, slično particijama na disku.

AMI je napredna slika virtualnog stroja koja se može koristiti za stvaranje jedne ili više instanci tog AMI-ja. Ove su slike slične snimkama za pokretanje koje sadrže dodatne informacije o virtualnom stroju. AMI se učitava na EBS kada se stvori instanca. Na primjer, kada korisnik dobije instancu i postavi je da ugosti njegovu ili njezinu web stranicu, sve što treba učiniti je spremiti instancu u obliku AMI, kopirati je u oblak širom svijeta i potom proizvesti duplicirane instance tog slučaja AMI. Svi njegovi stavovi su živi, radni klonovi izvorne slike koji se šire po regijama.

12.1. Cloud Storage na Amazonu

Na Amazonovom oblaku postoje različite vrste skladištenja: AMI (Amazon Machine Image), EBS (Elastic Block Store), snimke i količine. Količina se sastoji od pohranjenih podataka i eventualno praznog prostora. Također, glasnoća može postojati virtualno ili može pretpostaviti puni fizički tvrdi disk.

Kratki pregled je jednostavno sigurnosna kopija ili kopija podataka o količini instance. Za snimanje podataka u instanci može se upotrijebiti snimak, sličan vraćanju iz sigurnosne kopije. Kratki pregled obično nije spremljivi oblik za pohranu.

EBS je novi oblik pohrane podataka. EBS je virtualno spremanje podataka koje djeluje identično volumenu, ali podaci se mogu proširiti na više fizičkih tvrdih diskova i mogu se brzo i lako premjestiti [16]. Motivacija EBS-a je povećati učinkovitost pohrane u oblaku. Davatelji usluga u oblaku tada mogu prodati ostatak prostora za više klijenata. Uz to se EBS može sastojati od više volumena, slično particijama na disku.

AMI je napredna slika virtualnog stroja koja se može koristiti za stvaranje jedne ili više instanci tog AMI-ja. Ove su slike slične snimkama za pokretanje koje sadrže dodatne informacije o virtualnom stroju. AMI se učitava na EBS kada se stvori instanca. Na primjer, kada korisnik dobije instancu i postavi je da ugosti njegovu ili njezinu web stranicu, sve što treba učiniti je spremiti instancu u obliku AMI, kopirati je u oblak širom svijeta i potom proizvesti duplicirane instance tog slučaja AMI. Svi njegovi stavovi su živi, radni klonovi izvorne slike koji se šire po regijama.

12.2. Sigurnost podataka

Cloud korisnici mogu pohraniti osjetljive podatke u oblačne instance. Iz sigurnosne perspektive, cloud tvrtke moraju osigurati povjerljivost usluge. Na primjer, ti bi podaci mogli

biti rezervna baza podataka za financijsku uslugu. Klijent bilo koje usluge u oblaku trebao bi znati rizike povezane sa sigurnošću podataka, npr. Gubitkom podataka i krađom podataka.

Kod pohrane osjetljivih podataka šifriranje je uvijek moćna shema. Naravno, imalo bi smisla šifrirati osjetljive podatke poput brojeva kreditnih kartica koji su pohranjeni u oblaku. Potencijalna slabost šifriranja u oblaku je sigurnost ključeva. U svijetu hakera općenito je poznato da fizički pristup stroju uvijek rezultira igrom. To je zato što napadač ima kontrolu nad strojem.

Jednostavne lozinke u operativnom sustavu neće spriječiti napadača da krade podatke. Proval je neizbježan osim ako je cijeli disk šifriran. Šifriranje cijelog diska znači da je cjelokupni volumen šifriran, uključujući operativni sustav. Iako je potpuna enkripcija diska moguća u svijetu računalstva u oblaku, mnogi klijenti ne kriptiraju svoje podatke zbog performansi i financijskih razloga. Enkripcija diska dodaje dodatne režijske troškove u ukupno pohranjene podatke. Iako se brzina podataka razlikuje od regije do regije, kada klijenti plaćaju terabajtom, manje je podataka. Uz to, mnogim velikim spremištima podataka potreban je brzi pristup. Na primjer, usluga za strujanje videa mora brzo čitati podatka. Šifriranje diska značajno će usporiti taj proces i povećati troškove poslovanja. U tu svrhu, mnogi korisnici oblaka ne kriptiraju svoje sveske.

Kada kupci oblaka ne kriptiraju svoje količine, predstavlja se sigurnosni rizik. Nevjerojatni zaposlenik davatelja usluga može se šuškati okolo bez znanja klijenta. Budući da zaposlenik ima fizički pristup primjerku oblaka kupca, ništa ne može spriječiti zaposlenika da zgrabi vitalne podatke i bilo koje druge privatne ključeve. Ovaj zaposlenik to može učiniti jednostavnim kloniranjem virtualnog stroja žrtve i pokretanjem klona na drugom izvanmrežnom hipervizoru.

Zaposlenik može pratiti ponašanje virtualnog stroja i oduzimati svoje vrijeme tražeći vrijedne podatke. Tada lopov zaposlenik može krasti podatke ili pomoću tipki probiti u više oblaka. Pri spremanju podataka u oblak povjerenje je vrlo važan dio privatnosti podataka. „Prijetnja zlonamjernog insajdera dobro je poznata većini organizacija. Ova se prijetnja pojačava za potrošače oblačnih usluga konvergencijom IT usluga i korisnicima pod jedinstvenom domenom upravljanja, u kombinaciji s općim nedostatkom transparentnosti u postupku i postupku pružatelja usluga “. Stoga je pouzdan oblak bitan korak ka uspjehu računalstva u oblaku.

Ključna briga kod šifriranja podataka je određivanje je li šifriranje softvera otvorenog koda ili ne.

Otvaranje softvera za šifriranje ključno je za osiguravanje da se ne stvaraju stražnja vrata ili dodatni ključevi [1]. To je postao veliki problem mnogim uslugama kao što su tekstualne poruke, videokonferencije i e-pošta. Na primjer, Apple ima uslugu pod nazivom "iMessage" koja obrađuje tekstualne poruke u oblaku. Sve su poruke šifrirane od početka do kraja, osiguravajući da nijedan posrednik ne može čitati vaše razgovore. Ono što vam Apple ne kaže jest da su zakonski obvezni čuvati kopiju ključa. Kupci opet vjeruju u davatelja, Apple.

12.3. Rizici u oblaku i zabrinutosti za API

Od svih rizika o kojima izvještavaju vijesti i blogovi na Internetu, mnogi od njih nisu rizici svojstveni oblačnim servisima, što znači da bi se odnosili na sve poslužitelje. Mada, oblak doista povećava rizik od nekih od njih

1. Uskraćivanje usluge (DoS) – potonje postojanje očito je uvijek problem za poslužitelje. Dodatni rizik za korištenje oblaka je da će napadi na druge korisnike oblaka utjecati na vašu porciju. Ako je napad na oblak koji nema veze s vama oborio, također će srušiti vaš poslužitelj ili ga barem usporiti. Dakle, iako vaš poslužitelj možda nije meta napada, treba uzeti u obzir koji uključuje pojam da možda s istim hardverom radite bilo s kim.
2. Kršenja podataka imaju veći potencijal za katastrofe na oblaku. Jedna manjkavost usluge oblaka mogla bi prouzrokovati da se jedno kršenje podataka proširi na kršenje cijelog sustava. Metode jednostavnije od bočnog kanaliziranja mogu izdvojiti ključeve ili prikupiti nešifrirane podatke. Iako neki pojedinci misle da je to značajan rizik računalstva u oblaku, zapravo je realno manji rizik nego što bi bilo stvaranje vlastitog poslužitelja i njegovo servisiranje. U potonjem slučaju treba poduzeti mnoge mjere predostrožnosti, koje su oblačne službe već primijenile.
3. Gubitak podataka pitanje je koje nije jedinstveno za oblak. Gubitak energije potencijalni je scenarij svuda na Zemlji i ponekad je neizbježan. Članci su klevetali usluge oblaka zbog gubitka podataka kada u stvarnosti ti poslužitelji vjerojatno imaju bolju zaštitu od prenapona i pada od one koju biste si mogli priuštiti.

12.4. Otmica usluga i računa

U ovom trenutku svog razvoja oblak je ozbiljno ugrožen uslugom i otmicom računa. To uključuje neovlašteni pristup računima i uslugama klijenata koji koriste oblak i koriste ih. Otmica se može dogoditi na bilo koji način - budući da je oblak jednostavno mreža koja se pokreće na više različitih poslužitelja, tip je za sve iste napade kao i mreže i poslužitelji.

Jednom kada napadač oteli uslugu ili račun, možda će moći prisluškivati aktivnosti ovlaštenih korisnika, lažno predstavljati ovlaštene korisnike, dirati mrežne podatke ili koristiti uslugu ili račun za širenje zlonamjernog softvera, npr. preusmjeravanjem klijenata na zlonamjerne web stranice - sve prijetnje tipične za ne-oblačne mreže i poslužitelje. Međutim, jedinstveno za oblak, napadač može upotrijebiti otetu uslugu ili račun kao bazu operacija za izvođenje daljnjih napada na ostale strojeve u oblaku.

12.5. Primjer Amazona

Posljednjih godina, jedna od tvrtki na području oblačne tehnologije - Amazon.com, Inc., postala je plijen takvog napada. Godine 2010, otmičari su izveli napad preko križnog skripta (XSS) na neko mjesto kako bi stekli njegove vjerodajnice i bili uspješni. Napadači su se zatim infiltrirali u Amazonovu uslugu relacijskih baza podataka (RDS) tako da, čak i ako izgube izvorni pristup, još uvijek imaju povratnu snagu u Amazonov sustav. Od tog trenutka mogli su zabilježiti podatke o prijavi svih koji su kliknuli gumb za prijavu na početnoj stranici Amazona.

Napadači su koristili svoje poslužitelje kako bi zarazili nove strojeve trojanskim konjem Zeusa i upravljali strojevima koji su s njim već zaraženi (Zeus je komad zlonamjernog softvera dizajniran za Windows koji se najčešće koristi za krađu bankovnih podataka putem dohvaćanja obrasca i lozinke. prijavljivanje putem napada čovjeka-u-pregledniku). Računala zaražena zlonamjernim softverom počela su prijavljivati Amazonovu EC2 radi ažuriranja i uputa.

Jedna od najzanimljivijih činjenica o ovom slučaju bila je da nije, strogo gledajući, Amazon nije kriv. Napadači su dobili pristup putem neke druge, ranjivije domene. To otkriva jednu istinu o oblaku: čak i jedan ranjiv sustav može dovesti do ugrožavanja cijele mreže. Nadalje, Amazon je bio samo jedno od nekoliko mjesta koja je pretrpjela ovu vrstu napada u razdoblju od samo nekoliko mjeseci, i nije bilo loše tvrtka: Twitter, Googleov pokretač aplikacija i Facebook svi su doživjeli slične prijetnje.

12.6. Moguće obrane

Da bi se spriječila takva vrsta kršenja, Cloud Security Alliance (CSA) savjetuje organizacijama da onemoguće korisnicima i uslugama dijeljenje vjerodajnica računa između sebe, te pored toga upotrebljavaju zahtjeve za provjeru više faktora kada je to izvedivo. Međutim, obje ove promjene mogu otežati upotrebu, skuplje i sporije sustave. Multifaktorska provjera autentičnosti autentifikacija zahtijeva najmanje dva od sljedećeg: znanje ili nešto što netko zna; posjedovanje ili nešto što netko ima; i zaključak, ili je nešto jedno. Dakle, multifaktorska provjera autentičnosti puno više opterećuje korisnike i usluge nego jednofaktorska provjera autentičnosti. A ako je korisnicima i uslugama onemogućeno izravno dijeljenje vjerodajnica, pružatelji usluga u oblaku će možda morati izgraditi sigurne kanale (skupo poduzeće) ili angažirati treću stranu za komunikaciju između korisnika i usluga.

12.7. Budućnost sigurnosti u oblaku

12.7.1. PRISM skandal

U lipnju 2013. Edward Snowden otkrio je da Nacionalna sigurnosna agencija (NSA) prikuplja ogromne količine podataka o komunikaciji i pretraživanju od internetskih kompanija poput Microsofta, Yahooa, Googlea i mnogih drugih, uključujući podatke o aktivnostima američkih građana, Snowden je također objasnio da čak i zaposlenici NSA s niskim razinama imaju mogućnost pristupa tim podacima bez naloga. Takav se nadzor održava od siječnja 2007. Možda nije odmah jasno zašto su ove informacije posebno relevantne za oblak. Vlada može prisiliti pružatelje usluga oblaka da instaliraju pozadinu u svojim hipervizorima, ali to mogu učiniti za operativne sustave, pa čak i pojedinačne strojeve.

Međutim, ciljanje stroja jednog pojedinca mnogo je manje vjerojatno, jer je u tom trenutku vlada posebno izdvojila tog korisnika. Umjesto toga, oblak pruža NSA sjajni ocean mrežnih aktivnosti, u koji može baciti mrežu i nadati se da će uhvatiti nešto korisno - mnogo učinkovitije od ciljanja pojedinih strojeva. Kao što je jedan pisac za Porticor rekao: Skeniranje svih podataka s pružatelja usluga oblaka relativno je jednostavno, jer su dostupne ogromne količine podataka s više vlasnika. Porticor preporučuje korisnicima da šifriraju vlastite podatke kako bi se borili protiv takvih upada u privatnost, no dvojbeno je da će se takvo rješenje ikada pokazati široko prihvatljivim, jer postavlja neupitnu ponovnu sponzoriranost za korisnike i zahtijeva određenu stručnost. Primjer PRISM dotiče se mnogih

pitanja u budućnosti sigurnosti u oblaku: održavanja privatnosti, vladine politike i krađe podataka (budući da napadači mogu prikupljati korisničke podatke koristeći NSA tehnike ili čak i same NSA kanale). Korisnici oblačnih usluga često ne razmatraju ove probleme i o njima se ne govori u velikoj mjeri.

Bolji oblak Postoje organizacije koje rade na sigurnijem oblaku, poput CSA. Drugi je Silver Sky, stručni pružatelj sigurnosne zaštite u oblaku i pružatelj „napredne sigurnosne platforme u oblaku“ u industriji“. CTO of Silver Sky, Andrew Jaquith, objašnjava da mnogi CIO-ovi premještaju svoje usluge u oblak kako bi uštedjeli novac, ali ta sigurnost ostaje ključna briga i ti potezi mogu biti nesigurni ili barem užurbani. No s druge strane, on također objašnjava da mnogi pružatelji usluga oblaka postaju jasniji, transparentniji i sigurniji nego ikad prije da bi mogli zaštititi podatke o kupcima. Prema tome, prelazak na oblak, iako na neki način može biti nesiguran, ne najavljuje nečiju propast. Uz sve veću popularnost, čak i neodlučne tvrtke možda neće uskoro imati izbora.

12.7.2. Bolji oblak

Postoje organizacije koje rade na sigurnijem oblaku, poput CSA. Drugi je Silver Sky, stručni pružatelj sigurnosne zaštite u oblaku i pružatelj „napredne sigurnosne platforme u oblaku“ u industriji. CTO of Silver Sky, Andrew Jaquith, objašnjava da mnogi CIO-ovi premještaju svoje usluge u oblak kako bi uštedjeli novac, ali ta sigurnost ostaje ključna briga i ti potezi mogu biti nesigurni ili barem užurbani. No s druge strane, on također objašnjava da mnogi pružatelji usluga oblaka postaju jasniji, transparentniji i sigurniji nego ikad prije da bi mogli zaštititi podatke o kupcima. Prema tome, prelazak na oblak, iako na neki način može biti nesiguran, ne najavljuje nečiju propast. Uz sve veću popularnost, čak i neodlučne tvrtke možda neće uskoro imati izbora.

Jedinstveni oblici proizvoda i usluga ponuđenih putem cloud usluga pokazuju poticaj za suvremenu poslovnu upotrebu. Koristeći usluge Amazon Web Services kao studiju slučaja, mi smo u mogućnosti iskoristiti neke osnovne pojmove i koncepte računalstva u oblaku. Zatim nastavljamo s raspravom o sigurnosti podataka, problemima API-ja, otmici računa i drugim pitanjima sigurnosti. Pokazalo se da su ove opće zabrinutosti posebno zanimljive za sigurnost u oblaku. Glavne razlike između tradicionalnih usluga i oblačnih usluga uspoređuju se sa sigurnosne perspektive. Obuhvaćena je otmica usluga i računa, kao i moguća obrana.

13. ZAKLJUČAK

Upravljanje rizikom prijeko je potrebna temeljna kompetencija koja pomaže organizacijama da tijekom vremena postignu i povećaju vrijednost dionika. Za dobro upravljanje rizikom potrebni su bolji podaci i informacije kako bi organizacije mogle poduzimati mjere na neprekidnom popisu rizika. Timovi za upravljanje rizikom moraju olakšati i potaknuti prikupljanje, analizu i dostavu trenutnih i perspektivnih podataka o riziku. Informacije o prediktivnom riziku mogu rukovodstvu pružiti napredak u donošenju bolje informiranih odluka i pomoći im da poduzmu mjere koje daju pouzdanije rezultate. Evolucija u računalnoj i rizičnoj tehnologiji i razvoj novih tehnologija koje koriste velike podatke, analitiku, mobilne aplikacije, računalstvo u oblaku, planiranje poslovnih resursa (ERP) i sustave upravljanja, rizika i usklađenosti (GRC) također su važni za upravljanje rizikom. Ova tehnička unapređenja nude menadžerima za upravljanje rizicima i onima iz uprave ili izvan organizacije koji su uključeni u poboljšanje postojećih programa upravljanja rizikom s boljim sposobnostima za poboljšanje učinkovitosti upravljanja rizikom. Učinkovit program rizika trebao bi pružiti menadžmentu poboljšanu sposobnost za kontinuirano evidentiranje, procjenu, analizu i reagiranje na rizike koji proizlaze iz promjene internog poslovanja, vanjskog tržišta ili propisa. Neuspješno upravljanje tim promjenama može proizvesti financijske gubitke, negativan publicitet i utjecati na postizanje ciljeva ili misije organizacije. Evolucija informacijske tehnologije utjecala je na svako područje, poput učenja, marketinga, poslovanja, zabave i politike. Upravljanje rizikom jedna je od domena koja je pod velikim utjecajem evolucije, jer se uglavnom temelji na podacima. Informatička tehnologija iz dana u dan olakšava automatizaciju procesa počevši od prepoznavanja rizika i završavajući nadgledanjem. Mnoge organizacije već imaju velike i opsežne baze podataka koje su trenutno u proizvodnji, a mnogi IT odjeli aktivno su uključeni u njihovu bolju integraciju s postojećim aplikacijama kako bi izvukli više vrijednosti iz IT ulaganja. Mnoge baze podataka sadrže točke podataka o riziku koje je također moguće izdvojiti, minirati ili progutati pomoću moćnijih računalnih platformi kako bi se tijekom vremena postigla još veća organizacijska vrijednost. Alati koje glavni službenici za informiranje (CIO) organizacija sada koriste kako bi se olakšali takvi napori uključuju elektronička skladišta podataka (EDW-ovi), „velike podatke“, aplikacije poslovne inteligencije (BI) i informacijsko-analitičke tehnologije. [60]

[60] Mosca, P., Zhang, Y., Xiao, Z., Wang, Y. (2014) Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services. Dostupno na:

LITERATURA

1. Andrijanić, I., Gregurek, M., Merkaš, Z. (2016) Upravljanje poslovnim rizicima, Libertas – Plejada, Zagreb
2. Angeles, R., Nath, R. (2000) An empirical study of EDI trading partner selection criteria in customer-supplier relationships. Information and Management, 37, 241-255.
3. Caraiani G., (2008),,TranzacYii internaYionale: E-business & tipuri de contracte", Editura C.H. Beck, Bucure3ti
4. Center For Retail Research (2010) E-Commerce and Online Retail. Dostupno na: http://www.retailresearch.org/onlineretailing.php (15.1.2020).
5. Dahlin, P. (2007) "Turbulence in Business Networks - ", Doctoral Dissertation No 53, School of Business, Mälardalen University, Sweden.
6. de Bossey, C. (2005). Report of the Working Group on Internet Governance (WGIG). ITU. Dostupno na: https://www.wgig.org/docs/WGIGREPORT.pdf (15.1.2020.)
7. Deeter-Schmelz, D. R., Norman Kennedy, K. (2002) An exploratory study of the Internet as an industrial communication tool, examining buyers' perceptions. Industrial Marketing Management, 31, 145-154.
8. Dehning, B. and Richardson, V.J. (2002) Returns of Investment Technology: A Research Synthesis, Journal of Information Systems, 16, 1, 7-30.
9. Dimovski. V., Škerlavaj. M. (2004) Comunication Technologies as Management Tools: Case of Slovenia", Faculty of Economocs University of Ljubljana, 636.
10. Douglas, K. (2002) Sociological theory. Vol. 20, No. 3, 285-305.
11. European Commission (2004) Education for entrepreneurship: Making progress in promoting entrepreneurial attitudes and skills through primary and secondary education. Dostupno na: .http://europa.eu.int/comm/enterprise/enterprise_ policy/charter (15.1.2020).
12. Gay R, et all (2009) „Marketing online - o abordare orientata spre client", Editura: ALL
13. Hathaway, M. (2014) Connected choices: how the Internet is challenging sovereign decisions. America Foreign Policy Interests, 36(5), 300–313.
14. Hoffman, L., Novak, I., Peterson, T. (1997) et al Services Quality

https://www.researchgate.net/publication/276499055_Cloud_Security_Services_Risks_and_a_Case_Study_on_Amazon_Cloud_Services (16.1.2020.)

15. King, J.; Lampinen, A.; Smolen, A. (2011) Privacy: is there an app for that? In Proceedings of the SeventhSymposium on Usable Privacy and Security, Pittsburgh, PA, USA, 20–22 Frančula, N. i Lapaine, M. (2009). Information Sources and Cartography. Sveučilište u Zagrebu, Zagreb.
16. King, W. R., Grove, V., Hufnagel, E.H. (1989) Using Information and Information Technology for Sustainable Competitive Advantage: Some Empirical Evidence. Information & Management, vol. 27, nr. 2, 87-93.
17. Leek, S., Turnbull, P. W., Naude, P. (2003) How is information technology affecting business relationships? Results from a UK survey. Industrial Marketing Management, 32, 119-126.
18. Miles, P. (2001) Globalization – Economic Growth and Development and Development Indicators. Planet Papers.
19. Miles, P. (2001). Globalization – Economic Growth and Development and Development Indicators. Planet Papers.
20. Mosca, P., Zhang, Y., Xiao, Z., Wang, Y. (2014) Cloud Security: Services, Risks, and a Case Study on Amazon Cloud Services. Dostupno na: https://www.researchgate.net/publication/276499055_Cloud_Security_Services_Risks_and_a_Case_Study_on_Amazon_Cloud_Services (16.1.2020.)
21. Orlikowski, W. (1992) The Duality of Technology: Rethinking the Concept of Technology in Organizations, Organization Science, 3, 3, 398-427.
22. Sethi, V., King, W. R.. (1994) Development of Measures to Assess the Extent to which an Information Technology Application Provides Competitive Advantage. Journal of Management Science, vol. 40, no. 12, 1601-1627.
23. Sudar-Kulčar, M. (2005) Zaštita privatnosti i sigurnost pohranjenih podataka s osvrtom na izravni (direktni) marketing. Politička misao, vol.42,br.4.
24. Vukičević, M., Odobašić, S. (2012) Upravljanje rizicima, Visoka škola za poslovanje i upravljanje s pravom javnosti Baltazar Adam Krčelić, Zaprešić
25. Vukičević, M., Odobašić, S. (2012) Upravljanje rizicima, Zaprešić: Visoka škola za poslovanje i upravljanje s pravom javnosti Baltazar Adam Krčelić