Resursu klasifikācijas un risku analīzes piemērs virtuālai iestādei

RESURSU KLASIFIKĀCIJA

Informācijas resursu klasifikācija

Komentāri: Informācijas resursu klasifikācijas kārtība ievietota no IT drošības noteikumu vadlīniju **5.punkta** .

- *Iestāde veic visu informācijas resursu klasifikāciju ar mērķi novērtēt resursa saturošās informācijas nozīmību pēc konfidencialitātes, vērtības un pieejamības. Informācija var būt **publiska** un **ierobežotas** pieejamības.*
  - ***Informācijas konfidencialitātes** līmeni nosaka izejot no kaitējuma, kas varētu tikt nodarīts iestādei ja informācijai piekļūst personas, kas nav pilnvarotas.*
  - ***Publiska informācija (P)** – nav svarīga konfidencialitātes aspektā, tā ir brīvi pieejama iestādes darbiniekiem, jebkurai personai vai organizācijai, kas to ir pieprasījusi. Šīs informācijas izplatīšana neietekmē iestādi negatīvā veidā.*
  - ***Ierobežotas pieejamības informācija (I)** – ir svarīga konfidencialitātes aspektā, tās pazīmes noteiktas Informācijas atklātības likuma 5., 6., un 7. pantā. Šī informācija ir pieejama tikai iestādes darbiniekiem, kuriem ir piešķirtas šādas tiesības.*

- ***Informācijas vērtības** līmeni nosaka atkarībā no kaitējuma, kas varētu būt nodarīts iestādei, ja netiktu nodrošināta informācijas resursu integritāte, pēc šādas skalas:*
  - *V1 - augstas vērtības informācija,*
  - *V2 - vidēja vērtības informācija,*
  - *V3 - zema vērtības informācija.*

- ***Informācijas pieejamības** līmeņus nosaka atkarībā no iestādes darbības jomas, ņemot vērā kaitējumu kas varētu tikt nodarīts iestādei vai tās klientiem, ja netiktu nodrošināta resursu pieejamība. Informācijas pieejamības līmeni nosaka pēc šādas skalas:*
  - *P1- informācija pieejama 24 stundas diennaktī, 7 dienas nedēļā,*
  - *P2 - informācija pieejama iestādes darba laikā.*
  - *Resursi, kuriem nav piešķirts neviens no konfidencialitātes, vērtības vai pieejamības līmeņiem tiek uzskatīti par **neklasificētiem**. (tiem nav jāveic riska analīze)*

- *Informācijas klasifikācijas tabula (V- informācijas vērtība, K – informācijas konfidencialitāte, P- informācijas pieejamība)*

Galveno Informācijas resursu klasifikācija, kuri glabājas IT sistēmās (no virtuālās iestādes apraksta)

Komentāri: Izmantojot resursu klasifikācijas kārtību (IT drošības noteikumu vadlīniju **5.punkts**) tiek izveidota tabula, kurā apkopo un novērtē atbilstoši aprakstam Informācijas resursus, kuri aprakstīti Virtuālajā iestādē.

Nr.	Resurss	Informācijas sistēma	Informācijas vērtība (V)	Informācijas konfidencialitāte (K)	Informācijas pieejamība (P)
1	2	3	4	5	6
1	Lietvedība	Lietvedības dokumentu uzskaites sistēma	V2	P/I	P2
2	Personāla daļa	Personāla daļas dokumenti elektroniskā formā	V1	I	P2
3	Juridiskā daļa	Iestādes juridisko dokumentu uzskaites sistēma	V1	P/I	P2
4	Grāmatvedība	Grāmatvedības sistēma	V1	I	P2
5	Iestādes resursi	Iestādes darbības nodrošināšanai nepieciešamie dokumenti	V2	P/I	P2
6	IT daļa	Iestādes darbinieku IT sistēmu pieejas tiesību saraksts, u.c. informācija, kura nepieciešama IT sistēmu darbībai	V1	I	P1
7	Valsts informācijas sistēma	Valsts informācijas sistēma, ar kuru iestāde apmainās ar informāciju	V1	I	P2
8	Iestādes interneta tīmekļa vietne	Informācija par iestādi interneta tīmekļa vietnē	V2	P	P2

Resursu aizbildņa noteikšana

Komentāri: Katram Informācijas resursam jānosaka atbildīgais (Resursu aizbildnis – IT drošības noteikumu vadlīnijas **punkts 2.6, 4.2**) . Resursu aizbildnis šajā piemērā tiek noteiks atsevišķi Resursu saturam un funkcionēšanai atbilstoši darba pienākumiem.

Nr.	Resurss	Informācijas sistēma	Resursu aizbildnis (saturs)	Resursu aizbildnis (funkcionēšana)
1	2	3	4	5
1	Lietvedība	Lietvedības dokumentu uzskaites sistēma	Lietvedis/e	IT administrators/e
2	Personāla daļa	Personāla daļas dokumenti elektroniskā formā	Personāla daļas vadītājs/a	IT administrators/e
3	Juridiskā daļa	Iestādes juridiskie dokumenti	Juridiskās daļas vadītājs/a	IT administrators/e
4	Grāmatvedība	Grāmatvedības sistēma	Grāmatvedis/e	Ārpakalpojuma sniedzējs
5	Iestādes resursi	Iestādes darbības nodrošināšanai nepieciešamie dokumenti	Lietotāji	IT administrators/e
6	IT daļa	Iestādes darbinieku IT sistēmu pieejas tiesību saraksts, u.c. informācija, kura nepieciešama IT sistēmu darbībai	IT drošības pārzinis/e	IT administrators/e
7	Valsts informācijas sistēma	Valsts informācijas sistēma, ar kuru iestāde apmainās ar informāciju	Lietotāji	IPS (par datu komunikāciju) un VIS pārzinis (par VIS darbību)
8	Iestādes interneta tīmekļa vietne	Informācijas ievietošana iestādes interneta tīmekļa vietnē	Sabiedrisko attiecību daļas darbinieki	Ārpakalpojuma sniedzējs

RISKU NOVĒRTĒJUMS

Risku pašnovērtējums

Katrs struktūrvienības vadītājs iesniedz IT drošības pārzinim iespējamo risku (apdraudējumu) sarakstu, kas iever brīvā formā aprakstītus riskus un iespējamās sekas, ja kaut kas tāds notiktu. Paraugā doti iespējamie riski, kas tiešā veidā nav nevienā iestādē izmantojami.

- Lietvedis/e –lietvedības programma ik pa brīdim strādā ļoti lēni, apgrūtina iestādes normālu darbību un dokumentu apriti.
- Personāla daļas vadītājs/a - darbinieku personāla lietu kopijas elektroniskā formā atrodas uz servera, iespējama piekļūšana no iekšējā tīkla,
- Juridiskās daļas vadītājs/a – iestādei būtiski juridiski dokumenti glabājas uz darbinieka datora. Lai nenotiktu iespējama informācijas noplūde, tiek netiek turēti uz failu servera,
- Galvenais/ā grāmatvedis/e – grāmatvedības programmas atjaunināšana notiek ar aizkavēšanos, nav iespējams savlaicīgi sagatavot atskaites.
- IT daļas vadītājs/a:
    - iestādes failu serverim un elektroniskā pasta serverim nav '*hardware backup*', līdz ar to iekārtu bojājuma rezultātā iestādes darbība tiks traucēta līdz tiks atjaunota iekārtu darbība,
    - nepieciešami līdzekļi antivīrusu programmu licenču atjaunošanai, citādi darbinieku datori netiks aizsargāti pret ārējiem uzbrukumiem,
    - datu rezerves kopiju atjaunošanai uz datora cietā diska ir par maz brīvas vietas,
    - ilglaicīgas elektroenerģijas pārtraukuma gadījumā iestādes serveri izslēgsies pēc noteikta laika, darbinieku darba stacijas izslēgsies uzreiz.

Komentāri. Riski pamatā ir saistīti ar iekārtu un komunikāciju atteikumiem, kas izraisa iestādes apgrūtinātu darbību vai darbības apturēšanu. Daži riski izriet no nesakārtotiem organizatoriskiem jautājumiem (grāmatvedības programmas atjaunināšana). Iekārtu atteikums var novest pie informācijas bojājuma vai zuduma (Integritātes zudums), ir aprakstīti arī sociālie riski – darbinieka kļūda vai ļaunprātīga rīcība, kā arī trešo personu ļaunprātīga rīcība.

Riska analīze

Komentāri. Risku analīzes kārtība ievietota no IT drošības noteikumu vadlīniju **6.punkta** , paplašinot Resursu apdraudējumu un Resursiem radīto kaitējumu skalu no 3 vērtībām līdz 5, kas ļauj precīzāk aprēķināt risku.

- *Risku analīzi veic ar mērķi izvērtēt resursu apdraudējumus un iespējamās sekas apdraudējuma iestāšanās gadījumā.*
- *Risku pārvaldīšanu veic ņemot vērā informācijas klasifikāciju un risku pārvaldīšanas pasākumus nosaka samērojot drošības pasākumu izmaksas ar iespējamiem zaudējumiem.*
- *Atbildīgais par risku analīzes veikšanu ir resursu turētājs, kurš organizē risku analīzi, piesaistot struktūrvienību vadītājus.*
- *Struktūrvienību vadītāju pienākums ir nodrošināt pēc iespējas pilnīgu un precīzu risku identificēšanu un novērtēšanu.*
- *Risku analīzi veic ne retāk kā vienu reizi gadā.*
- *Resursu apdraudējuma varbūtību nosaka izmantojot skalu:*
    - *1 – maza apdraudējuma varbūtība,*
    - *2 – neliela apdraudējuma varbūtība,*
    - *3 – vidēja apdraudējuma varbūtība,*
    - *4 – ievērojama apdraudējuma varbūtība,*
    - *5 – liela apdraudējuma varbūtība.*

- *Resursiem radīto kaitējumu no katra apdraudējuma nosaka izmantojot skalu:*
    - *1 – mazs kaitējums,*
    - *2 – neliels kaitējums,*
    - *3 – vidējs kaitējums,*
    - *4 – ievērojams kaitējums,*
    - *5 – liels kaitējums.*

- *Risku aprēķināšanu veic - risks= (apdraudējuma varbūtība x resursa apdraudējuma kaitējums). R=AVxRK .*
- *Tabulā apkopo iespējamos resursu apdraudējumus, atzīmējot ietekmi uz (K- konfidencialitāti, P – pieejamību, I – integritāti, AV - apdraudējuma varbūtību, RK - resursiem radīto kaitējumu , R - aprēķināto risku).*

Komentāri: Lai noteiktu apdraudējuma iestāšanās varbūtību, jānosaka tā raksturs. Drošības apdraudējumus nosacīti var sadalīt vairākās grupās: (apdraudējuma iedalījums katrā iestādē būs citādāks)

1. Iestādei specifiski apdraudējumi - tos var novērtēt tikai iestādes struktūrvienību vadītāji, (tieši saistīti ar iestādes darbu, izmantotām iekārtām un tehnoloģijām)
2. Daba - fiziski apdraudējumi (fiziska nopostīšana, dabas stihija, ugunsgrēks, plūdi utt.),
3. Vide - tehniski apdraudējumi (datorvīrusi, energoapgādes pārtraukumi, iekārtu bojāšanās, programmatūru nepilnības u.c.),
4. Cilvēki - sociāli apdraudējumi (personāla nekompetence, kļūdas, paroļu zaudēšana, aizmāršība, ļaunprātība utt.).

Risku novērtējumu tabula

Nr.	Apdraudējums	Apraksts	varbūtība Apdraudējuma	Radītais kaitējums	Aprēķinātais risks	Komentāri
1	2	3	4	5	6	
	Iestādes specifiski apdraudējumi					
1	Nestrādā (lēni strādā) lietvedības programma	Saistīts ar lielu daudzumu elektronisku dokumentu apstrādi, to reģistrāciju un iestādes darbinieku iepazīstināšanu ar tiem. Tas apgrūtina iestādes efektīvu darbību, savlaicīgu ienākošo un izejošo dokumentu apriti.	3	4	12	Lietvede vairākkārtīgi ir informējusi gan iestādes vadību, gan IT administratoru.
2	Iespējama nesankcionēta piekļuve iestādes darbinieku personas lietām	Tā kā dati atrodas uz kopējā failu servera, tad, izmantojot sistēmas ievainojamības vai ļaunprātīgi lietojot svešus pieejas datus (parole, lietotājvārds), pastāv iespēja piekļūt informācijai.	1	5	5	
3	Iestādei svarīgu dokumentu	Visi iestādes līgumi un cita juridiska satura informācija	2	5	10	Precedentu vēl nav bijis.

	zaudējums vai tie kļūst pieejami trešajām personām	glabājas iestādes jurista/es portatīvā datora cietajā diskā. Ja dators pārstāj darboties, pastāv iespēja pazaudēt informāciju elektroniskā formā. Tā kā jurists/te bieži strādā arī ārpus iestādes, pastāv risks, ka dators var tikt pazaudēts vai nozagts.				
4	Grāmatvedis/e nevar laikā sagatavot finanšu atskaites, jo nav atjaunināta grāmatvedības programmatūra.	Likumdošanas izmaiņu gadījumā programmas izstrādātāji veic nepieciešamās izmaiņas un uzstāda tās pēc iestādes pieprasījuma.	2	4	8	Pēc pēdējām izmaiņām par PVN, netika savlaicīgi uzlikts programmas atjauninājums, līdz ar to mēneša atskaite tika sagatavota ar novēlošanos.
5	Kaitīga vai ļaundabīga koda (vīrusu u.c.) darbība uz iestādes darba stacijām un serveriem.	Antivīrusu programmatūra nav atjaunota, tomēr strādā, bet nespēj atpazīt jaunākos vīrusus.	4	4	16	
6	Nav iespējams atjaunot datus no rezerves kopijām	Datu apjoms, kuru nepieciešams saglabāt kā rezerves kopijas, pieaug, un uz cietā diska, kur tās glabājas, ir palicis maz vietas.	2	5	10	
	Daba					
7	Plūdi	Ēkas elektrības sadales skapis atrodas pagrabstāvā. Ja tas applūdīs, visa ēka paliks bez elektroenerģijas padeves.	1	5	5	
8	Ugunsgrēks		1	5	5	Māja ir ar daudziem birojiem, ir ēkas kopīgais ugunsdrošības un evakuācijas plāns
	Vide					

9	Vīrusi, ļaundabīga programmatūra	Iespējama datorā atrodošās informācijas (ieskaitot resursu pieejas lietotājvārdu un paroļu) sabojāšana, nodzēšana vai nokļūšana trešo personu rokās.	2	4	8	Ik pa laikam uz darbinieku darba stacijām tiek atrasts kāds ļaundabīgs kods vai vīruss.
10	Darba stacijas bojājums	Ja darbinieka darba stacija (dators) sabojājas, nav iespējams to uzreiz aizvietot ar rezerves datoru, iestādei nav pieejamas uz vietas datoru rezerves daļas.	1	4	4	
11	Lietotāji, Grāmatvedības vai E-pasta iestādes servera bojājums.	Serveris nebūs pieejams līdz bojājums netiks novērsts. Cietā diska bojājumu gadījumā iespējams informācijas neatgriezenisks zudums, ja neizdodas to atjaunot no rezerves kopijām.	2	5	10	Vismaz reizi gadā kāds serveris pārstāj darboties tehnisku iemeslu dēļ.
12	Interneta pieslēguma pārtraukums	Iestādes darbs netiek būtiski traucēts, nav iespējams nosūtīt e-pastus un lietot internetu. Neilgi pārtraukumi (dažas stundas) interneta darbībā nav kritiski.	2	3	6	
13	Serveru pārkaršana	Vasarā karstajās dienās iespējama serveru pārkaršana, kas būtiski palielina servera atteices iespēju.	1	5	5	
14	Elektroenerģijas padeves pārtraukums	Iestādes darba stacijas un tīkla darbība apstājas, serveri izslēdzas pēc noteikta laika.	2	3	6	
15	Interneta mājās lapa nav pieejama	Ārpakalpojuma sniedzēja vai datu komunikācija darbības pārtraukums.	2	3	6	
16	Nav pieejas Valsts informācijas sistēmai	Valsts informācijas sistēmas vai datu komunikācija darbības pārtraukums. Nebūs iespējama datu apmaiņa, iestādes darbība tiks traucēta. Īsi pārtraukumi (līdz 1 stundai) nav kritiski.	2	4	8	
	Cilvēki					
17	Paroles pazaudēšana	Paroles atjaunošana prasa IT administratora/es darba resursus, līdz paroles atjaunošanai darbiniekam nav iespējams veikt savus pienākumus.	1	2	2	Reizēm ir gadījumi, kad darbinieks aizmirst vai pazaudē paroli

18	Cita darbinieka paroles izmantošana	Lai piekļūtu VIS un iestādes tīmekļa lapai, katram resursam atsevišķi ir izdalīts tikai viens lietotājvārds un parole. Parasti ar šiem resursiem strādā viens darbinieks, bet tā prombūtnes laikā (slimība, atvaļinājums) šo pašu paroli un lietotājvārdu lieto darbinieka aizvietotājs.	2	4	8	Nevar izdalīt auditācijas pierakstos, kurš no darbiniekiem ir strādājis ar resursu.
19	Darbinieka kļūda, nekompetence	Kļūdas vai nekompetences dēļ tiek pazaudēti vai sabojāti dati.	1	4	4	
20	Darbinieka ļaunprātība	Darbinieki, kuri izbeiguši darba attiecības, vēl kādu laiku izmanto iestādes piešķirto lietotājvārdu un paroli.	2	5	10	Nav izstrādāta sadarbības kārtība starp personāla daļu, kā savlaicīgi izdzēst bijušo darbinieku lietotāja vārdus.
21	Portatīvā datora zādzība/pazaudēšana		2	5	10	
22	Ielaušanās, zagļi		2	5	10	Pa biroju darba laikā staigā dažādu preču piedāvātāji/ pārdevēji.

RISKU PĀRVALDĪBA

Risku mazināšanas pasākumi

Komentārs: Risku var pieņemt, to var mazināt vai no tā atteikties. Izvēlamies aprēķinātos riskus, kuru vērtību pārsniedz noteiktu līmeni un kuriem ir nepieciešams veikt risku mazināšanas pasākumus (šajā piemērā robežvērtība ir 8 un vairāk). Ja vērtība ir zemāka, var veikt riska mazināšanas

pasākumus, bet lielākoties šie riski tiek akceptēti (pieņemti). Katrā iestādē aprēķinātā riska vērtību, pie kuras tiek plānoti riska mazināšanas pasākumi, var būt atšķirīga.

Nr.	Apdraudējums	Riska mazināšanas pasākums	Aprēķinātais risks	Ieviešanas termiņš	Izmaksas	Izpildītājs
1	2	3	4	5	6	7
1	Nestrādā (lēni strādā) lietvedības programma	Sazināties ar lietvedības programmas izstrādātāju, precizēt nepieciešamās prasības programmas normālai darbībai un, ja nepieciešams, uzlabot konfigurāciju lietotāju serverim.	12	201X.XX.XX	xxxxx.Ls	IT administrators/e
2	Iespējama nesankcionēta piekļuve iestādes darbinieku personas lietām	Risks ir zems, un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	5			
3	Iestādei svarīgu dokumentu zaudējums vai tie kļūst pieejami trešajām personām.	Veikt pieejas tiesību inventarizāciju, visiem resursiem uzlikt paroles nomaiņas pieprasījumu.	10	201X.XX.XX	-	IT administrators/e
4	Grāmatvedis/e nevar laikā sagatavot finanšu atskaites, jo nav atjaunināta grāmatvedības programmatūra.	Ja nepieciešams, pārskatīt līgumu ar ārpakalpojumu sniedzēju, lai atjauninājumi tiktu uzlikti savlaicīgi.	8	201X.XX.XX	xxxxx.Ls	Jurists/e
5	Kaitīga vai ļaundabīga koda (vīrusu u.c.) darbība uz iestādes darba stacijām un serveriem.	Atjaunot antivīrusa licences	16	201X.XX.XX	xxxxx.Ls	IT administrators/e
6	Nav iespējams atjaunot datus no rezerves kopijām	Iegādāties papildu cieto disku rezerves kopijām.	10	201X.XX.XX	xxxxx.Ls	IT administrators/e
7	Plūdi	Risks ir zems un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	5			

8	Ugunsgrēks	Risks ir zems un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	5			
9	Vīrusi, ļaundabīga programmatūra	Izskaidrot darbiniekiem antivīrusa programmas lietošanas nepieciešamību un veikt kontroli.	8	201X.XX.XX	-	IT administrators/e
10	Darba stacijas bojājums	Risks ir zems un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	4			
11	Lietotāji, Grāmatvedības vai E-pasta iestādes servera bojājums.	Serveru galveno mezglu rezerves daļu iegāde, lai bojājumu gadījumā tos varētu nekavējoši nomainīt.	10	201X.XX.XX	xxxxx.Ls	IT administrators/e
12	Interneta pieslēguma pārtraukums	Risks ir zems un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	6			
13	Serveru pārkaršana	Izskatīt iespēju iegādāties kondicionieri.	5	201X.XX.XX	xxxxx.Ls	IT administrators/e
14	Elektroenerģijas padeves pārtraukums	Tā kā informācijas integritāti uz serveriem elektroenerģijas pārtraukums neietekmē, un tas notiek ļoti reti, tad risks ir zems un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	6			
15	Interneta mājās lapa nav pieejama	Tā kā mājas lapai ir informatīvs raksturs, tās nepieejamība ir tikai reputācijas problēma, tāpēc risks ir zems un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	6			
16	Nav pieejas Valsts informācijas sistēmai	Izstrādāt kārtību saziņai ar interneta pakalpojumu sniedzēju un VIS pārzini, lai maksimāli samazinātu iespējamo dīkstāvi.	8	201X.XX.XX	-	IT administrators/e
17	Paroles pazaudēšana	Risks ir zems un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	2			
18	Cita darbinieka paroles	Sazināties ar interneta tīmekļa vietnes uzturētāju un	8	201X.XX.XX	-	IT

	izmantošana	VIS pārzini, un izdalīt katram darbiniekam atsevišķu lietotājvārdu un paroli.				administrators/e
19	Darbinieka kļūda, nekompetence	Risks ir zems un tas tiek akceptēts – nekāda darbība vai izdevumi nav nepieciešami.	4			
20	Darbinieka ļaunprātība	Pēc darba attiecību izbeigšanas slēgt pieeju jebkuram iestādes resursam.	10	201X.XX.XX	-	IT administrators/e
21	Portatīvā datora zādzība/pazaudēšana	Iegādāties neuzkrītošu somu datoram, IT administratoram veikt dokumentu rezerves kopijas arī no portatīvajiem datoriem. Instruēt portatīvo datoru lietotājus par to glabāšanu un pārvietošanu publiskās vietās.	10	201X.XX.XX	-	IT administrators/e
22	Ielaušanās, zagļi	Pie iestādes durvīm uzlikt sarunu ierīci un durvis aprīkot ar kodu atslēgu.	10	201X.XX.XX	xxxxx.Ls	Saimniecības pārzinis

Kopsavilkums

No 22 apskatītiem apdraudējumiem12 apdraudējumiem aprēķinātā riska vērtība ir vienāda vai lielāka par 8 . Šiem apdraudējumiem tiek plānoti un aprakstīti risku mazināšanas pasākumi ar noteiktu izpildes datumu, atbildīgo par izpildi, kā arī uzrādīts iespējamais budžets. 10 gadījumos aprēķinātā riska vērtība ir zemāka par 8, kas ļauj šos riskus pieņemt neveicot nekādas darbības.

Šis dokuments ir domāts kā atsevišķa IT drošības noteikumu sastāvdaļa, kas ir izveidots kā piemērs virtuālas iestādes Resursu klasifikācijai un risku analīzei.

Iestādes IT drošības noteikumus apstiprina iestādes vadītājs, un tie paliek nemainīgi līdz rodas pamatota nepieciešamība tos mainīt. Nepārtraukti notiek izmaiņu pārvaldība, kurā tiek rekomendēts Resursu analīzi un riska analīzi veikt ne retāk kā reizi gadā.

Ar IT drošības noteikumiem un to prasībām jāiepazīstina visi iestādes darbinieki, kuri lieto IT resursus.