ევროკავშირი
საქართველოსთვის

რუსული პროგრამული უზრუნველყოფის გამოყენების რისკები

ციფრული საქართველოს რუსული ოკუპაცია

10/9/24

IRC
Innovations and reforms Center

GITAC

სტატიის შესახებ

სტატია მომზადდა ა(ა)იპ ინოვაციებისა და რეფორმების ცენტრის მიერ.

სტატიის მიზანი

საქართველოში მოქმედი ბიზნესების ინფორმირება რუსული ICT პროდუქტების საფრთხეებთან დაკავშირებით.

ავტორები

- დავით შავგულიძე
- ირაკლი ლომიძე

რეფერენსი

სტატიაში გამოყენებული იქნა "***ICT მიწოდების ჯაჭვის უსაფრთხოების"*** სიღრმისეული კვლევა[1], რომელიც მომზადდა 2024 წელს, საქართველოს ინფორმაციის და ტექნოლოგიების ანალიზის ცენტრის (GITAC) მიერ, ევროკავშირის მიერ დაფინანსებული პროექტის **„უსაფრთხოების სექტორის ანგარიშვალდებულების გაძლიერება სამოქალაქო საზოგადოების ეფექტური ზედამხედველობით"** ფარგლებში, რომელსაც ინოვაციებისა და რეფორმების ცენტრი (IRC) ახორციელებდა.

ეს სტატია შექმნილია ევროკავშირის მხარდაჭერით. მის შინაარსზე სრულად პასუხისმგებლები არიან ავტორები და შესაძლოა, რომ იგი არ გამოხატავდეს ევროკავშირის შეხედულებებს.

[1]https://shorturl.at/arRn4

რატომ არის მნიშვნელოვანი პროგრამის წარმომავლობა, რომელსაც იყენებთ?

დღევანდელ ურთიერთდაკავშირებულ სამყაროში ტექნოლოგია ყოველდღიური ცხოვრების ძირითადი ნაწილია როგორც ბიზნესისთვის, ასევე ინდივიდებისთვის. ფინანსების მენეჯმენტიდან და კოლეგებთან კომუნიკაციიდან დაწყებული მომხმარებელთა მონაცემებისა და პროექტების ვადების დამუშავებამდე, პროგრამული სისტემები გადამწყვეტია კომპანიების გამართული მუშაობისთვის და მოქალაქეების ციფრული ცხოვრებისთვის. თუმცა, ყველა **პროგრამული უზრუნველყოფა არ არის უსაფრთხო.**

ქართული კომპანიებისა და მოქალაქეებისთვის რუსული პროგრამული უზრუნველყოფისა და აპარატურის გამოყენება საფრთხის შემცველია. რუსეთის სახელმწიფოს მიერ დაფინანსებულ აქტორებს აქვთ კიბერშეტევების მრავალწლიანი გამოცდილება საქართველოში. რუსეთში შემუშავებული პროგრამული უზრუნველყოფა შეიძლება იყოს გამოყენებული კიბერ ჯაშუშობის, მონაცემთა გაჟონვისა და საოპერაციო შეფერხებისთვის. ამ სტატიაში ჩვენ განვიხილავთ, **თუ რატომ შეიძლება იყოს რუსული პროგრამული უზრუნველყოფა საფრთხის შემცველი, რა რისკები მოაქვს მას კომპანიებსა და მოქალაქეებისთვის და როგორ შეიძლება ევროკავშირის კიბერუსაფრთხოების რეგულაციები და სტანდარტები დაეხმაროს საქართველოს ციფრულ ინფრასტრუქტურის დაცვას.**

1. რუსული პროგრამული უზრუნველყოფის გამოყენების რისკები

რუსული პროგრამული უზრუნველყოფის თანდაყოლილი საფრთხეები

რუსული პროგრამული გადაწყვეტილებები[2] პოპულარულია საქართველოსა და პოსტსაბჭოთა სივრცეში. პროდუქტები, როგორიცაა 1C (ERP სისტემა), Bitrix24 (პროექტის მენეჯმენტისთვის) და Yandex Cloud (ღრუბლოვანი გამოთვლითი პლატფორმა) ჩვეულებრივ გამოიყენება ბიზნესისა და მოქალაქეების მიერ მათი ყოველდღიური ოპერაციებისთვის. მიუხედავად იმისა, რომ ეს პროგრამები შეიძლება ჩანდეს როგორც ხელმისაწვდომი და მოსახერხებელი გადაწყვეტილებები, მათ აქვთ ფარული საფრთხეები:

- **მიწოდების ჯაჭვის შეტევები:** რუსული პროგრამული უზრუნველყოფა შესაძლოა გამოყენებული იქნეს მიწოდების ჯაჭვის შეტევებისთვის. კერძოდ, **ჰაკერებმა შესაძლოა ჩააშენონ მავნე კოდი (ვირუსი, ტროიანი, გამომძალველი პროგრამა, ჯაშუშური პროგრამა და ა.შ) შესყიდული ლეგიტიმური პროგრამული უზრუნველყოფის განახლებებში (update)**. როდესაც მომხმარებლები დააინსტალირებენ ამ განახლებებს, ისინი გაუცნობიერებლად გაუშვებენ მავნე პროგრამას, რომელსაც **<u>შეუძლია მონაცემების მოპარვა, ფაილების დაშიფვრა ან კრიტიკული სისტემების გამორთვა.</u>**

რა რისკების წინაშეა ბიზნესი?

<u>ქართული ბიზნესისთვის, განსაკუთრებით მცირე და საშუალო საწარმოებისთვის (SME), რისკები რეალურია და არა თეორიული.</u> ილუსტრაციისთვის, განვიხილოთ შემდეგი გავრცელებული რუსული პროგრამული სისტემები:

- **1C:** საქართველოში ფართოდ გამოიყენება ფინანსური მენეჯმენტისა და მარაგების კონტროლისთვის. ეს ERP სისტემა ამუშავებს სენსიტიურ ბიზნეს მონაცემებს, როგორიცაა ფინანსური ჩანაწერები, შესყიდვების ხელშეკრულებები და მომწოდებლის შესახებ ინფორმაცია. გამომდინარე ინფორმაციის მნიშვნელობიდან, **აღნიშნული სისტემა წარმოადგენს კარგ / მომგებიან სამიზნეს რუსული ჰაკერული დაჯგუფებებისა და სახელმწიფოს სპეცსამსახურებისთვის**.
- **Bitrix24:** პროექტების მართვის, კოლაბორაციის, მომხმარებლებთან ურთიერთობის მართვის (CRM) პლატფორმა პოპულარულია დაბალი ხარჯებისა და სიმარტივის გამო. თუ სისტემა იქნება კომპრომეტირებული, აღნიშნულმა შესაძლოა გამოიწვიოს ორგანიზაციის კომერციული საიდუმლოს შემცველი ინფორმაციის გაჟონვა ან თუნდაც, მიმდინარე პროექტების შეფერხება.
- **Yandex Cloud:** ღრუბლოვანი საცავის პლატფორმა, რომელზეც ორგანიზაციამ შეიძლება განათავსოს თავისი ბიზნეს ინფორმაცია ან სერვისები. **ღრუბლოვანი სისტემებიდან ინფორმაციის მიტაცება უფრო დიდი რისკია და გავლენა შესაძლოა უფრო დამანგრეველი იყოს ქართული კომპანიისთვის**.

[2]სტატიაში განხილული რუსული პროგრამული უზრუნველყოფის მაგალითები შეირჩა მათი პოპულარულობის გათვალისწინებით და არ წარმოადგენს ამომწურავ სიას.

ჩვენი ბიზნესი ვის აინტერესებს?

<u>ხშირ შემთხვევაში მცდარია მოსაზრება, რომ ჩვენი ბიზნესი / კომპანია არავის აინტერესებს და არ წარმოადგენს შემტევის სამიზნეს.</u> პრაქტიკა ცხადყოფს, რომ **მიწოდების ჯაჭვის შეტევები (როდესაც პროგრამული უზრუნველყოფის გამოყენებით შეაღწევენ პროგრამის მომხმარებელთან) შეიძლება იყოს გამოყენებული ერთი ორგანიზაციიდან სხვა ორგანიზაციაზე გასასვლელად**. SolarWinds-ისა და NotPetya-ს სახელებით ცნობილი კიბერშეტევები არის მაგალითები იმისა, თუ როგორ შეიძლება მიწოდების ჯაჭვის შეტევამ გამოიწვიოს მილიარდობით მოცულობის ზიანი.

რა შეიძლება მოხდეს?

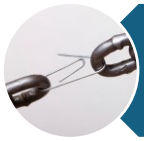
მაგალითისთვის, **თუ თქვენ წარმოადგენთ სადისტრიბუციო კომპანიას, რომელმაც დანერგა რუსული ERP სისტემა, მათ შორის საწყობების ავტომატიზაციის მოდულებითა და მომხმარებლების მართვის სისტემით,** თქვენს წინაშეა შემდეგი რისკები:

- მარტივად გაჟონოს თქვენი კომპანიის სასაქონლო მარაგების შესახებ ინფორმაციამ;
- გაჟონოს კომპანიის კლიენტების, მათი შეკვეთებისა და სხვა ბიზნეს გარიგებების შესახებ ინფორმაციამ;
- საქართველოზე მიტანილი მსხვილმასშტაბიანი კიბერშეტევის დროს, გააჩერონ თქვენი ციფრული სისტემებიც, როგორც ქვეყანაზე ზემოქმედების ერთ-ერთი კომპონენტი.
- კომპანია მონაწილეობას ვერ მიიღებს ევროკავშირის შესყიდვებსა და პროექტებში.

უსაფრთხოების კონტროლები დამეხმარება?

ხშირად, კომპანიები, **რომლებიც გვთავაზობენ რუსულ პროგრამულ უზრუნველყოფას, ასევე, გვთავაზობენ უსაფრთხოების სისტემებსა და მომსახურებას. <u>მცდარია მოსაზრება,</u>** რომ:

რუსული ანტივირუსული პროგრამა საიმედოა და დაგვიცავს



ISO/IEC 27001 ინფორმაციული უსაფრთხოების მართვის სისტემის სტანდარტს თუ ავიღებთ, დაცული ვიქნებით რუსული მიწოდების ჯაჭვის კიბერშეტევებისგან

„უსაფრთხოების კონტროლებს დავნერგავთ და ვერ გაგვტეხავენ“

სერვისის მომწოდებელი კომპანია სანდოა, ვინაიდან უსაფრთხოება და ციფრული ტრანსფორმაცია განსხვავებული მიმართულებებია

2. რაში დაგვეხმარება ევროკავშირთან ჰარმონიზაცია?

ევროკავშირის ჰარმონიზაციის პროცესის მეშვეობით ქართული სახელმწიფო სექტორის, ბიზნესებისა და მოქალაქეების კიბერუსაფრთხოება შესაძლოა მნიშვნელოვნად გაძლიერდეს. ევროკავშირს გააჩნია ქმედითი და დახვეწილი კანონმდებლობა პერსონალური მონაცემების დაცვისა და ინფორმაციული უსაფრთხოების მიმართულებით. ევროკავშირის კონტექსტში, მნიშვნელოვანია შემდეგი რეგულაციები:

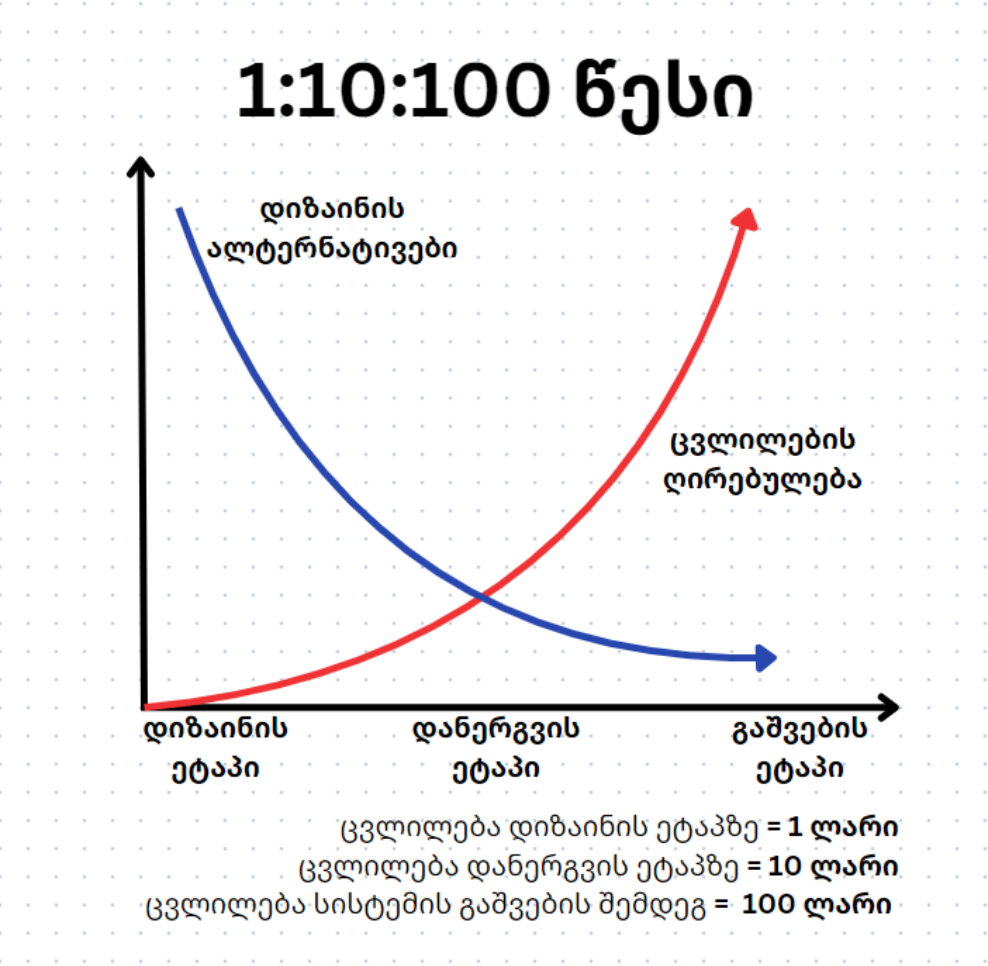
- **<u>მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR)</u>** – დირექტივა ავალდებულებს პერსონალური მონაცემების დამმუშავებლებს დაიცვან მონაცემთა დამუშავების წესები. აღნიშნული გულისხმობს პერსონალური მონაცემების მოპოვების, დამუშავების, შენახვისა და გადაცემის წესების ერთობლიობას, რაც საბოლოო ჯამში ქმნის წინაპირობას, რომ **პირადი ცხოვრება იქნება ხელშეუხებელი და მომხმარებლის ინტერესები იქნება დაცული. რეგულაცია დაიცავს საქართველოს მოქალაქეების პერსონალურ მონაცემებს და არ დაუშვებს მათ გადაცემასა და უკანონო დამუშავებას რუსეთის ფედერაციის ტერიტორიაზე.**
- **<u>ქსელისა და ინფორმაციული უსაფრთხოების დირექტივა (NIS2)</u>** - დირექტივა აყალიბებს ყოვლისმომცველ კონტროლებს ეროვნული კრიტიკული ინფორმაციული ინფრასტრუქტურის დასაცავად. რეგულაციაში მნიშვნელოვანი აქცენტი კეთდება **მიწოდების ჯაჭვის კიბერუსაფრთხოებაზე,** რაც გულისხმობს **ორგანიზაციების მიერ შესყიდული პროგრამული და აპარატურული უზრუნველყოფის წარმომავლობისა და მათი მწარმოებლების სანდოობისა და უსაფრთხოების შეფასებას**. შედეგად, რეგულაცია დაეხმარება ქართულ ბიზნესებს გაზარდ
- **<u>ციფრული საოპერაციო მედეგობის აქტი (DORA)</u>** - რეგულაცია აყალიბებს კიბერუსაფრთხოების მოთხოვნებს ფინანსური სექტორის მიმართ, რაც სხვა დანარჩენთან ერთად, არეგულირებს მიწოდების ჯაჭვის რისკების მართვის ჩარჩოს. რეგულაცია ხელს უწყობს **ფინანსურ ორგანიზაციებს გაზარდონ ხილვადობა შესყიდული პროგრამების, სერვისებისა და აპარატურის წარმომავლობისა და სანდოობის შესახებ.** შედეგად, რეგულაცია დაეხმარება საქართველოს ფინანსურ სექტორს წინსწრებით შეაფასონ შესყიდული ICT პროდუქტების რისკები და მათი სანდოობა.

3. უსაფრთხოების რეკომენდაციები, რომელთა შესრულება შეუძლიათ ქართულ კომპანიებსა და მოქალაქეებს

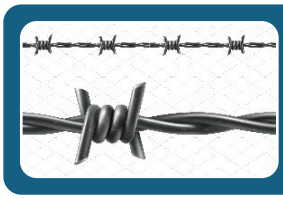
რუსული პროგრამული უზრუნველყოფის რისკებისგან უკეთ დასაცავად, ქართულ კომპანიებსა და მოქალაქეებს შეუძლიათ რამდენიმე პროაქტიული ნაბიჯის გადადგმა:

რეკომენდაციები ქართულ კომპანიებს

ბიზნესის კონკურენტუნარიანობის მიღწევისა და შენარჩუნებისთვის **ციფრული ტრანსფორმაცია გარდაუვალია**. ხშირ შემთხვევაში, მნიშვნელოვანი პროგრამული უზრუნველყოფის (მაგალითად, ERP) **დანერგვა ძალიან ძვირია და დიდ დროს მოითხოვს.** ამ პროცესში აუცილებლად უნდა გავითვალისწინოთ ფორესტერის 1:10:100 წესი, რომელიც ამბობს, რომ დიზაინის ფაზაზე ცვლილების ღირებულება 1$-ია, დანერვის ფაზაზე იგივე ცვლილება 10$ ღირს, ხოლო გაშვებულ პროდუქტში იგივე ცვლილების განხორციელება 100$ დაჯდებოდა. შესაბამისად, თუ ფიქრობთ, რომ **დღევანდელი საჭიროებებისთვის საკმარისია იაფი და მოქნილი რუსული სისტემა, რომელსაც მომავალში ჩაანაცვლებთ სანდო და დახვეწილი დასავლური სისტემებით,** ეს მიდგომა გაცილებით ძვირი და მეტად კომპლექსური იქნება.



ყოველივე ზემოხსენებულის გათვალისწინებით, რამდენიმე პრაქტიკული რეკომენდაცია ბიზნესისთვის:



საქართველოს კიბერსივრცის ციფრული ოკუპაცია

- *საქართველოს ფიზიკური ტერიტორიის 20% ოკუპირებულია რუსეთის ფედერაციის მიერ.*
- *ნუ დაუშვებ საქართველოს ციფრული სივრცის ოკუპაციის რუსული პროგრამების გამოყენებით.*

ევროკავშირის ბაზართან თავსებადობა

- **ნუ შეისყიდით რუსულ პროგრამულ უზრუნველყოფას**, თუ თქვენ გეგმავთ ევროკავშირის ბაზარზე გაფართოებას.

სისტემის დანერგვის დრო და ხარჯები

- **ნუ შეისყიდით რუსულ პროგრამულ უზრუნველყოფას,** მხოლოდ იმიტომ რომ იაფია. მომავალში სისტემის ჩანაცვლება ბევრად უფრო რთული და ძვირი დაგიჯდებათ.

კიბერუსაფრთხოების კონროლები

- **ნუ შეიყიდით რუსულ პროგრამულ უზრუნველყოფას,** იმის იმედით, რომ უსაფრთხოების კონტროლებით შეძლებთ რისკების თავიდან არიდებას. არ არსებობს ქმედითი მექანიზმი, რომელიც მცირე და საშუალო ბიზნესს დაიცავს მიწოდების ჯაჭვის შეტევებისგან.

პარტნიორების სანდოობა

- **ნუ ითანამშრომლებთ ისეთ კომპანიებთან, რომლებიც იყენებენ რუსულ პროგრამებს საკუთარ ბიზნეს პროცესებში.** გახსოვდეთ, თანამშრომლობისას გაცვლილი მონაცემები შესაძლოა რუსული მხარის ხელში აღმოჩნდეს.
- **ნუ ითანამშრომლებთ ისეთ კომპანიებთან, რომლებიც რუსულ პროგრამებს წერგავენ, თუნდაც ისინი კიბერუსაფრთხოების სერვისებს გთავაზობდნენ.**

სოციალური კორპორატიული პასუხისმგებლობა (CSR)

- ნუ შეუწყობ ხელს რუსული პროდუქტების დანერგვას და გავრცელებას. ნუ იქნები ციფრული ოკუპაციის ხელშემწყობი.