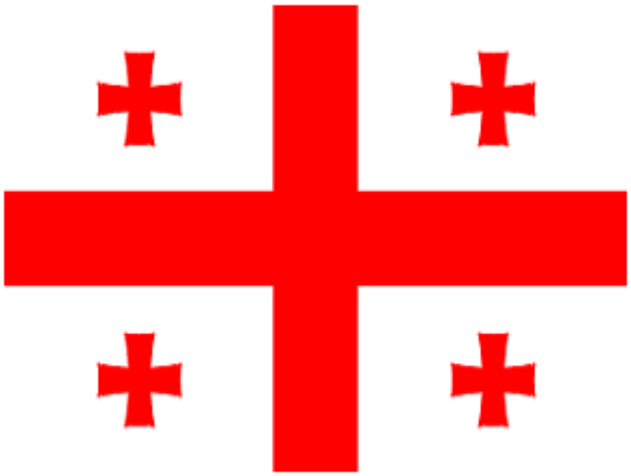
“Real-Time Georgia”

სამთავრობო და სამეწარმეო ოპერაციების დაცვის ორგანიზება



დრ. დევიდ ე. პრობერტი, VAZA International

საქართველოს პირველი IT ინოვაციების კონფრენცია

თბილისი: 2008 წლის 29 და 30 ოქტომბერი

ავტორი: დოქტორი დევიდ ე. პრობერტი საავტორო უფლება: www.vaza.com – ოქტ. 2008
ქართული ვერსიის რედაქტორი: დოქტორი დიმიტრი ყიფიანი, www.orient-logic.com , ნოემბ. 2008

(1) შესავალი: საქართველოს უსაფრთხოება უმნიშვნელოვანეს ფაქტორს წარმოადგენს ამ ახალი დემოკრატიული ერის მომავალი ეკონომიკური ზრდისა და განვითარებისათვის. გასულ წელს საპატიო მოპატიჟება მივიღე ევროგაერთიანებიდან: საქართველოს პარლამენტისათვის უსაფრთხოების გაუმჯობესებასთან და განახლებასთან დაკავშირებით რეკომენდაციების გაცემა, მის IT დირექტორთან, მერაბ გოცირიძესთან თანამშრომლობით.

გარდა ამისა, დოქტორმა დიმიტრი ყიფიანმა (შპს "ორიენტ-ლოჯიკი") მომიწვია, რათა საწარმოთა საინფორმაციო განყოფილებების დირექტორთა და სამთავრობო IT სპეციალისტთა ჯგუფისათვის წარმედგინა ბიზნესის უწყვეტობისა და ავარიულ სიტუაციებში აღდგენის პროცედურების ძირითადი პრინციპები, ასევე, IT უსაფრთხოებასთან, DoS-შეტევებთან ბრძოლისა და კიბერ-ომის პირობებში საინფორმაციო დაცვასთან დაკავშირებული პროგრამა.

ბევრი რამ მოხდა ამ უკანასკნელი 12 თვის განმავლობაში და ჭეშმარიტად მახარებს თბილისში დაბრუნება, კოლეგებთან და ახალ მეგობრებთან ელექტრონული უსაფრთხოების ინფრასტრუქტურის დაგეგმვაზე მუშაობის განახლების მიზნით, რომელიც სახელმწიფოებრივი მდგრადობის საფუძველს წარმოადგენს!

წინამდებარე დოკუმენტი (Security White Paper) მოიცავს პროექტის პრაქტიკულ ზომებს, რომელთა მიღება აუცილებელია საქართველოს IT, გამოთვლითი და კომუნიკაციური ინფრასტრუქტურის განახლებისათვის, სრულად დაცული და ერთიანი Real-Time 21-ე საუკუნის ელექტრონული მთავრობის უზრუნველყოფის მიზნით, რომელიც დაკავშირებულია ე-კომერციულ საწარმოებთან საქართველოში და მსოფლიოში.

ამ დოკუმენტის ძირითად აზრს წარმოადგენს განაწილებული ქსელური სისტემების დაცვა. წარსულ, Web1.0 ერაში, თქვენი მთავარი სერვერების, ინტრანეტის, ელ-ფოსტისა და დოკუმენტაციის დასაცავად აუცილებელი იყო მხოლოდ ორმაგი ფაიერვოლი DMZ-ით (დემილიტარიზებული ზონა) და პროქსი სერვერი. ახლა კი, ახალ, Web 2.0 ერაში, უსაფრთხო პერიმეტრი ნაკლებად არის განსაზღვრული, ყველა

ატარებს ახალ მოწყობილობებს – მე-3 თაობის მობილურ ტელეფონებს, აიპოდებს, მემორი-სტიკებს, ლაპტოპებს, Wi-Fi, Bluetooth, და სხვა უსადენო მოწყობილობებს.

არსებობს გარკვეული პარალელები საქართველოს ისტორიულ მდებარეობასთან, სადაც კავკასია ფიზიკურ დაცვას უზრუნველყოფდა ჩრდილოეთიდან შემოჭრის წინააღმდეგ, ხოლო სამხრეთით – გამოქვაბულების კომპლექსები, როგორიცაა, მაგალითად, ვარძია, აგებული მე-12 საუკუნეში, იცავდა ქვეყანას სამხრეთ საზღვრებიდან შემოჭრის წინააღმდეგ შედარებით დაცული ცხოვრების უზრუნველყოფის მიზნით.

სინამდვილეში, ვარძიის ეს უძველესი არქიტექტურა კვლავაც შეიცავს ანალოგიას დღევანდელ რეალობასთან, ვინაიდან 21-ე საუკუნეში, ნაცვლად კლდოვანი გამოქვაბულების სამგანზომილებიანი ქსელისა, ჩვენ ვიცავთ სერვერების, მონაცემთა ბაზების და საბოლოო მომხმარებლების მოწყობილობების უაღრესად რთულ, მრავალგანზომილებიან ქსელს. ვარძია მტკვარს დაჰყურებს – მშვენიერ მდინარეს, რომელიც მიედინება თბილისში, საქართველოს დედაქალაქში, შემდეგ კი – რუსთავში, კიდევ უფრო ძველი, მე-6 საუკუნის დავით გარეჯის მახლობლად. ასე რომ, ახლა ჩვენ ვიცავთ ელექტრონულ გამოქვაბულებს (სერვერებს), რომლებიც სავსეა მნიშვნელოვანი საინფორმაციო რესურსებით და მე თავს უფლებას ვაძლევ, მოვიხსენიო შემოთავაზებული პროგრამა, რომელიც ითვალისწინებს "Real-Time ელექტრონული საქართველოს – e-GE" შემუშავებასა და სრულ დაცვას –პროექტის **"ვარძია"** სახით - ხიდი მეთორმეტე და ოცდამეერთე საუკუნეებს შორის!

გასულ წელს საქართველოს პარლამენტთან მუშაობისას, სწრაფადვე გახდა ნათელი, რომ ინვესტირება, განხორციელებული IT ინფრასტრუქტურაში, იყო ტრადიციულად მცირე, კერძოდ, უსაფრთხოების, მონაცემთა დარეზერვების, დუბლირების და ISO საერთაშორისო სტანდარტებთან შესაბამისობის მიღწევის თვალსაზრისით. უკანასკნელი თვეების ტრაგიკულმა მოვლენებმა ცხადყო, რომ უაღრესად აუცილებელია მნიშვნელოვანი კაპიტალდაბანდება მთავრობისა და საწარმოების IT და უსაფრთხოების ინფრასტრუქტურაში, ვინაიდან არსებული ქსელები ძალზედ დაუცველი და არამდგრადია კიბერ-თავდასხმებისა თუ სხვა სახის საშიშროებებისადმი.

(2) უსაფრთხოების მიმდინარე მდგომარეობა. საერთაშორისო ბაზარი და დასავლური მთავრობების უმრავლესობა, უკანასკნელი 10 წლის მანძილზე, ინტერნეტის მეშვეობით გადავიდა სრულყოფილად ფუნქციონალურ და უაღრესად უსაფრთხო ფიზიკურ და ვირტუალურ ქსელებზე, რომლებიც უზრუნველყოფენ ე-ბიზნესის უზრუნველყოფას ბაზრის ყველა სექტორში, დაწყებული საფინანსოთი და დამთავრებული სამოგზაურო, საწარმოო, საცალო, სამთავრობო, საგანმანათლებლო და სამედიცინო დარგებით. კარგ სიახლეს საქართველოსთვის წარმოადგენს ის, რომ დასავლური პარტნიორებისაგან ინვესტიციების არსებობის გათვალისწინებით, გადასვლა მომავალი თაობის ქსელებზე არ მოითხოვს დიდძალი მემკვიდრეობის ინტეგრაციას ICT (Information and Communication Technology) სფეროში შედარებით მცირე ინვესტიციების გამო ამ უკანასკნელი 15 წლის განმავლობაში. თუმცა, ICT და უსაფრთხოების პროგრამის მართვა პროფესიონალურ მიდგომას მოითხოვს, რათა უზრუნველყოფილი იქნას მისი სრული ფუნქციონირება მომდევნო 2-3 წლის მანძილზე.

საქართველოში ჩემს მიერ ამ ბოლო დროს მიღებული გამოცდილების საფუძვლად, შემიძლია ვთქვა, რომ უსაფრთხოების არსებული ხარისხი როგორც მთავრობაში, ისე საწარმოებში, ძალზედ არაადექვატურია და გაცილებით ჩამორჩება ISO 27000 უსაფრთხოების სტანდარტებს, რომლებიც საერთაშორისო მასშტაბით არის მიღებული. წინამდებარე დოკუმენტი (White Paper) ასახავს "**ვარძიის პროექტის**" რეზიუმირებულ შემოთავაზებას, რომელიც ითვალისწინებს ტექნოლოგიური და ოპერაციული უსაფრთხოების ინფრასტრუქტურის ინტენსიურ და ეფექტურ განახლებას მისი მდგრადობის უზრუნველყოფისა და, დაახლოებით 2012 წლისათვის, ოპერაციული უსაფრთხოების სტანდარტებთან შესაბამისობის მიღწევის მიზნით.

ზოგ სამთავრობო სამსახურში, სააგენტოსა და საწარმოში დანერგილია უმაღლესი კლასის ICT სიახლეები, ზოგში კი ინფრასტრუქტურა და შესაბამისი საშუალებები საბჭოთა ერაშია ჩარჩენილი – მდგომარეობა იგივეა, რაც თითქმის 20 წლის წინ იყო. გარდა ამისა, არსებული სამთავრობო და ბიზნეს ინფრასტრუქტურა არაადექვატურად არის ურთიერთდაკავშირებული, არც საკმარისი საერთაშორისო კავშირები თუ სიხშირული დიაპაზონი არსებობს იმისათვის, რომ უზრუნველყოფილი იქნას საქართველოს გლობალური სავაჭრო ეკონომიკის მხარდაჭერა. არსებულ ქსელებში უამრავი გაუმართაობაა, რასაც ემატება ICT სფეროს დაბალი კვალიფიკაცია

მთავრობისა და მსხვილი კომერციული საწარმოების გარეთ. აქედან გამომდინარე, განათლება და ტრენინგი უსაფრთხოების სფეროში, ისევე, როგორც ესტონეთში, უნდა წარმოადგენდეს ე-საქართველოს მთავრობის სამწლიანი პროექტის ერთ-ერთ პრიორიტეტულ მიზანს.

და ბოლოს, ისტორიული და პოლიტიკური მიზეზებისა და უკანასკნელი 15 წლის განმავლობაში ICT სფეროში უაღრესად მცირე ინვესტირების გამო, მთავრობისა და საწარმოების გამოყენებითი პროგრამების უსაფრთხოების არსებული დონე ხშირად მიუღებელი ხდება. უაღრესად მნიშვნელოვანი პროგრამები მთავრობასა თუ საფინანსო და კომერციულ საწარმოებში ხშირად ღიაა კიბერ-თავდასხმებისათვის უსაფრთხოების საშიშროებებიდან გამომდინარე, რომლებიც ქვემოთაა ჩამოთვლილი, მათ შორის – მომსახურეობის გაწევის განაწილებული უარყოფა (Ddos), ვირუსების/Trojan თავდასხმები, უსადენო ქსელებისა და მარშრუტიზატორების ჰაკირება, ინფორმაციის პოტენციური დაკარგვა მინიმალური დარეზერვების გამო და თავდასხმა საბოლოო მომხმარებლის ICT მოწყობილობების სუსტი დაცულობის შედეგად.

(3) **უსაფრთხოების საშიშროებები**: ტექნოლოგიური და ოპერაციული: ქვემოთ ჩამოთვლილია ის 10 მთავარი საშიშროება, რომელიც რეალურად არის მოსალოდნელი საქართველოს მთავრობისა და მსხვილი კომერციული საწარმოებისათვის:

I. **10 მთავარი საშიშროება**: i) მომსახურეობის გაწევის განაწილებული უარყოფა ii) SQL მონაცემთა ბაზის ჰაკირება; iii) მიზანმიმართული ტროას ცხენები (Targeted Trojan Horses); iv) ვებ-საიტებისა და ინტერნეტის IP მისამართების ფალსიფიცირება; v) დაცული ინფორმაციის მოპარვა; vi) დესტრუქციული ვირუსები; vii) პაროლის, კოდის გასაღებისა და ID მოპარვა; viii) კომპიუტერის სერვერებისა და ქსელის სისტემების ფიზიკური განადგურება (ხანძარი, დაბომბვა, ტერორისტული აქტი); ix) საერთაშორისო ინტერნეტ კავშირის დაკარგვა; x) მტრისა და ტერორისტების მიერ ინფორმაციის არაკანონიერი გზით მიღება და სამთავრობო და სამხედრო ICT და web-რესურსების გასაიდუმლოებული კონტროლი. სინამდვილეში, არსებობს ელექტრონული და ტექნოლოგიური უსაფრთხოების საშიშროების მრავალი სხვა დონე, მაგრამ ზემოაღნიშნული 10 მთავარი საშიშროება, ალბათ, ყველაზე მეტად მიესადაგება საქართველოს სიტუაციას.

II. **კონტრქმედებები:** საქართველოში აუცილებელია უსაფრთხოების კონტრქმედებების დივერსიფიცირებული ელექტრონული ძალების ფორმირება ამ 10 მთავარი საშიშროების გამოვლენისა და პრევენციის მიზნით. ზოგი მათგანის დანერგვა შესაძლებელია ორიოდ კვირაში, ხოლო ბიზნესის უწყვეტობისა და ავარიულ სიტუაციაში აღდგენის პროგრამის სრულად განხორციელება მოითხოვს რამდენიმე თვეს კომპიუტერული განახლებისათვის პერსონალის საფუძვლიან ტრენინგთან ერთად. შედარებით მეტი დრო სჭირდება უსაფრთხოების საერთაშორისო სტანდარტების, მათ შორის ISO27000 სტანდარტის დაკმაყოფილებას, ასევე, NATO-სა და ASIS-ის ბიზნესის უწყვეტობისა და ავარიულ სიტუაციაში აღდგენის "საუკეთესო პრაქტიკის" დანერგვას.

III. **ოპერაციული უსაფრთხოების საშიშროებები**: უსაფრთხოების პროფესიონალებს შორის ზოგადად არის მიღებული, რომ უსაფრთხოების პრობლემების 40% წარმოიქმნება არა ტექნოლოგიური ჰაკერობის ან ელექტრონული ქურდობის შედეგად, არამედ სუსტი ოპერაციული იმპლემენტაციის, ადამიანის, ზოგჯერ თვით ICT პერსონალის მიერ დაშვებული შეცდომებისა და ჩადენილი ქურდობის გამო. ოპერაციული უსაფრთხოების უმთავრეს რისკებს საქართველოს მთავრობისათვის წარმოადგენს შემდეგი:

i) მნიშვნელოვანი ინფორმაციის დაკარგვა დარეზერვების პროცედურების უხარისხო დანერგვის ან განხორციელების გამო;

ii) მონაცემთა ერთიანობა – ინფორმაცია ან მონაცემთა ბაზები შეიძლება მალულად იქნას შეცვლილი პერსონალის ან კრიმინალების მიერ;

iii) სისტემური გაუმართაობა და მონაცემთა დაკარგვა ბუნებრივი მოვლენების გამო, როგორიცაა მიწისძვრა, ხანძარი ან წყალდიდობა;

iv) დოკუმენტებისა და არქივების დაკარგვა ისეთი ფიზიკური მოწყობილობების დაკარგვის გზით, როგორიცაა მემორი-სტიკები, ლაპტოპები, მობილური ტელეფონები ან ნებისმიერი სხვა მოწყობილობები, რომლებსაც შეუძლიათ ინფორმაციისა და საკონტაქტო მონაცემების შენახვა;

v) პაროლების, დაშიფრვის გასაღების, აქსეს-ბარათების და შენობის გასაღების ქურდობა პერსონალის ან ვიზიტორების (სტუმრების) მიერ.

კვლავ და კვლავ, ოპერაციული რისკების სია პოტენციურად დაუსრულებელია, მაგრამ მთავარი ის არის, რომ ქვემოთ მითითებულ ტექნოლოგიურ გადაწყვეტილებებთან ერთად აუცილებელია ოპერაციული უსაფრთხოების ტრენინგის უწყვეტი პროგრამების განხორციელება, რომლებიც უნდა წარმოადგენდეს საქართველოსათვის შემუშავებული უსაფრთხოების ნებისმიერი პროგრამის აუცილებელ ნაწილს.

(4) ტექნოლოგიური გადაწყვეტილებები: საბედნიეროდ, დღეს Symantec და Hewlett Packard კომპანიები გვთავაზობენ მზა ტექნოლოგიურ გადაწყვეტილებებს, რომლებსაც ძალუძთ უსაფრთხოების რისკების უაღრესად ფართო სპექტრისაგან – მათ შორის ზემოაღნიშნული რისკებისაგან – დაცვის უზრუნველყოფა.
ახლა უსაფრთხოების 10 მთავარ საშიშროებას რიგ-რიგობით განვიხილავთ:

i) **მომსახურეობის გაწევის განაწილებული უარყოფა** – უცხო ინვაზიური ბოთნეთების ინვაზიის წინააღმდეგ რაიმე სახის ინდივიდუალური გადაწყვეტილება არ არსებობს, მაგრამ შეტყობინებების სათაურების შემოწმება რეალურ დროში ღრმა პაკეტურ შემოწმებასთან ერთად "თავდასხმის" ადრეულ სიგნალს უზრუნველყოფს და ოპერატორებს აძლევს ამ თავდასხმის ალტერნატიულ მიმართულებებზე სწრაფად გადამისამართების შესაძლებლობას, სერვერებისა და მონაცემთა ბაზების დისტანციურ სარეზერვო რეჟიმში გადართვის მეშვეობით. IP მისამართის ხელახალი შეყვანა ალტერნატიულ დიაპაზონზე დომეინების DNS–ის ხელახალ განსაზღვრასთან ერთად, ასევე, შესაძლო გადაწყვეტილებას წარმოადგენს.

ii) **SQL მონაცემთა ბაზის ჰაკირება** – სამწუხაროდ, მრავალი თავდასხმა SQL სერვერზე ხდება იმის გამო, რომ დეფოლტურ ადმინ-პაროლებს არასოდეს ცვლიან! ნებისმიერ შემთხვევაში, მონაცემთა ბაზის ჰაკირების ეს ფორმა წარმოადგენს ერთ-ერთ უადვილეს და ყველაზე გავრცელებულ გზას როგორც სამთავრობო, ისე ბიზნეს ინსტალაციებზე. სწორედ ამ გზით ხდებოდა საკრედიტო ბარათების მონაცემებისა და, შესაძლოა, სამხედრო მონაცემთა ბაზების ჩანაწერების მასიური მოპარვა. ამ შემთხვევაშიც, უსაფრთხოების პროგრამული უზრუნველყოფის მსხვილი ვენდორების მიერ

შემოთავაზებული გადაწყვეტილებები უზრუნველყოფს SQL ბაზების უსაფრთხოებას და დაცვას რისკებისაგან.

iii) **Targeted Trojan Horses (მიზანიმამრთული ტროას ცხენები)** – ეს ვირუსი სულ უფრო და უფრო დახვეწილი ხდება და ბოთნეთის გაერთიანების ფარგლებში პერსონალური კომპიუტერების დაინფიცირების უმთავრეს წყაროს წარმოადგენს. აღნიშნული ინფექცია, სავარაუდოდ, შემოდის კომპიუტერული თამაშებიდან და კომპიუტერული მოწყობილობების საშინაო გამოყენების შედეგად, რომლებიც რეალურად მხოლოდ სამთავრობო ან ბიზნეს მიზნებისთვისაა განკუთვნილი. Admin Logon ოფციონის დაბლოკვა საუკეთესო პირველი საფეხურია, ასევე, აუცილებელია ლოკალური და დისტანციური შეღწევის უზრუნველყოფა დაწესებულების საკატალოგო სერვისის გამოყენებით. კიდევ ერთ პრობლემას საქართველოს მთავრობისათვის წარმოადგენს კრიმინალების, მტრის აგენტების ან ტერორისტების მიერ გაშვებული ტროას პროგრამული უზრუნველყოფის ლატენტური "აგენტი-რობოტები", რომლებიც ფილტრავენ და გადასცემენ ქსელში არსებულ ამა თუ იმ საიდუმლო ინფორმაციას ვირუსის ავტორის მიერ განსაზღვრულ დროს – ფიზიკური თუ უსადენო ქსელური კავშირების მეშვეობით. ასეთი ვირუსების დადგენა შესაძლებელია მხოლოდ მონაცემთა, სკრიპტებისა და IP მარშრუტიზებული მისამართების უაღრესად დეტალური მრავალმხრივი გამოძიების საშუალებით, გარდა ამისა, აუცილებელია ყოველგვარი კომუნიკაციისა და დოკუმენტების რუტინული ანტივირუსული სკანირება რეალურ დროში.

iv) **დაცული ინფორმაციის ქურდობა** – ტექნიკური თვალსაზრისით, ეს შეიძლება დაკავშირებული იყოს ტროას ცხენის დანერგილ პასიურ ან ლატენტურ ვირუსთან. ასეთი ვირუსების რუტინული გამოვლენა შესაძლებელია უსაფრთხოების სტანდარტული პროგრამული უზრუნველყოფის მეშვეობით, მაგრამ ყოველივე ეს უნდა განხორციელდეს პროფესიონალურად განსაზღვრული უსაფრთხოების პოლიტიკის ფარგლებში, იქნება ეს საქართველოს პარლამენტში, სამინისტროებში თუ კომერციულ საწარმოებში.

v) **ვებ-საიტებისა და ინტერნეტ IP მისამართების ფალსიფიცირება** – როგორც ჩანს, სულ უფრო და უფრო იზრდება ვებ-საიტების, SPLOGS (სპამის ბლოგების) და IP მისამართების ფალსიფიცირების შემთხვევები. ხშირია

ბრენდული საიტების ფალსიფიცირება, მხოლოდ მცირედი ცვლილებებით ID და პაროლის შესაყვან მონაცემთა ველებში. ისევ და ისევ, ამგვარი ფალსიფიკაციისაგან დაცვას უზრუნველყოფს მზა პროგრამული უზრუნველყოფა, მაგრამ, საბოლოო მომხმარებლები ყურადღებით უნდა იყვნენ საეჭვო ი-მეილებისა და ვებ-გვერდების შემთხვევაში და არ უნდა გასცენ კონფიდენციალური პირადი, სამთავრობო თუ ბიზნეს ინფორმაცია, ვიდრე 100%-ით არ დარწმუნდებიან, რომ ყველაფერი წესრიგშია.

vi) **დესტრუქციული ვირუსები** – ბევრი დესტრუქციული ვირუსი ვრცელდება შენიღბული "exe" ფაილების მეშვეობით და ხშირად ჩანერგილია JPG ან GIF ფორმატის გრაფიკული ფაილების კოდში, ან შესრულებადი სკრიპტის ამა თუ იმ ფორმით. თუმცა, მათ მიერ გამოწვეული ზიანი შეიძლება ძალზედ დიდი იყოს, - პირველ რიგში ინფიცირდება ქსელში ჩართული ყველა სერვერი, შემდეგ კი თანმიმდევრობით იშლება ყოველგვარი ინფორმაცია ბაიტურ დონეზე, გარდა ამისა, ვირუსი იმეილით იგზავნება ქსელის საკონტაქტო სიაში მითითებულ ყველა მისამართზე. ამ შემთხვევაშიც, Symantec-ის მიერ შემოთავაზებული გადაწყვეტილებები უზრუნველყოფს რეალური დროის პროაქტიურ დაცვას ამგვარი ვურუსული საშიშროებისაგან.

vii) **პაროლების, შიფრის კოდების, წვდომისა და ბიომეტრული ID კოდების ქურდობა** – პერსონალური მონაცემების ქურდობის ეს ფორმები უაღრესად საშიშია, რადგან კრიმინალს შეუძლია განასახიეროს მთავრობის ან საწარმოს ხელმძღვანელის როლი და შეაღწიოს უაღრესად მნიშვნელოვან და კონფიდენციალურ ინფორმაციაში. აუცილებელია ტექნიკური დაცვის კომბინაცია გაუმჯობესებულ ოპერაციულ პროცედურებსა და პერსონალის ტრენინგთან ერთად, განსაკუთრებით სამხედრო ან სადაზვერვო ჯგუფებში.

viii) **სერვერებისა და ქსელის სისტემების ფიზიკური განადგურება (მიწისძვრა, ხანძარი, დაბომბვა, ტერორისტული აქტი)** – როგორც ცნობილია, საქართველო და მთელი კავკასია მდებარეობს ისეთ რეგიონში, რომელშიც სერიოზული მიწისძვრების დიდი ალბათობა არსებობს. ამდენად, ICT სისტემების დამონტაჟებისას გათვალისწინებული უნდა იქნას მათი მდგრადობა მცირე მიწისძვრებისადმი მაინც, ვიბრაციის ჩამქრობი სპეციალური ფუნდამენტებისა და არმირებული ჭერების მეშვეობით. ფიზიკური განადგურების შემთხვევაში რისკი მნიშვნელოვნად მცირდება, თუ

ყოველგვარი მონაცემები, იმეილები და ინფორმაცია დარეზერვებულია დისტანციურ შემნახველ მოწყობილობებში, რომლებიც განთავსებულია რამდენიმე კილომეტრის დაშორებით, ამა თუ იმ საიდუმლო შეუმჩნეველ ადგილას, შესაძლოა მიწისქვეშ.

ix) **საერთაშორისო ინტერნეტ კავშირების დაკარგვა და ჰაკირება** – თავისი ბუნებით, ინტერნეტ კომუნიკაციები შეიძლება მარშრუტიზებული იქნას ნებისმიერი ქსელური კავშირით. VoIP და მონაცემთა სხვა მატარებლების განვითარება ქმნის დამატებით რისკებს და ზრდის სუსტი მხარეების რიცხვს. ნებისმიერი საიდუმლო სამთავრობო თუ ბიზნეს ინფორმაცია ყოველთვის დაშიფრული უნდა იყოს საკმარისად მძლავრი ალგორითმითა და გასაღებით. საქართველოში, ასევე, აუცილებელია ინვესტირება ალტერნატიული მარშრუტებისა და მაღალსიჩქარული საერთაშორისო ფართო დიაპაზონის IP კომუნიკაციებში, რათა შემცირებული იქნას აგენტების თვალთვალის, ჰაკერობისა და მომსახურეობის გაწევის უარყოფის რისკები.

x) **აგენტების მიერ ინფორმაციის დისტანციურად მოპოვება; სამთავრობო და სამხედრო ICT და ვებ-რესურსების საიდუმლო თვალთვალი** – ეს რისკი შეიძლება საკმაოდ არარეალურად ჟღერს, მაგრამ, სინამდვილეში, დაცული საშუალებები ერთხელ მაინც ყოფილა "გატეხილი" განვითარებულ ქვეყნებშიც კი, ზოგი მათგანი კი მუდმივ თავდასხმას ექვემდებარება. საქართველოს შემთხვევაში უნდა ვივარაუდოთ, რომ DdoS და მასთან დაკავშირებული თავდასხმები მრავალი თვისა და წლის განმავლობაში განხორციელდება და რომ მიზანში ამოღებული იქნება როგორც მთავრობა, ისე კომერციული საწარმოები. შემოთავაზებული NATO-ს უსაფრთხოების მონაცემთა ცენტრის განხორციელება ნამდვილად შეუწყობს ხელს მრავალმხრივი გამოძიების ტექნიკური რესურსების გამოყოფას ამგვარი კიბერ-თავდასხმების რისკის შემცირების მიზნით, ასევე, უსაფრთხოების სპეციალისტების კვალიფიკაციის ამაღლებას შესაბამისი ტრენინგების შედეგად.

(5) ოპერაციული გადაწყვეტილებები: უსაფრთხოების დამცავი ფარის განვითარებისა და შენარჩუნების ერთ-ერთ უმნიშვნელოვანეს კომპონენტს წარმოადგენს უსაფრთხოების პოლიტიკების დანერგვა და კომუნიკაცია უსაფრთხოების იმ ტექნოლოგიურ გადაწყვეტილებებთან ერთად, რომლებიც ზემოთაა აღნიშნული.

i) **ბიზნესის უწყვეტობის პროგრამა**: მნიშვნელოვანი ინფორმაციის დაკარგვის პრევენცია შესაძლებელია, თუ განხორციელდება მონაცემთა ცენტრის განახლება მონაცემთა რეალურ დროში დუბლირების მეშვეობით და უფრო გრძელვადიანი დარეზერვებით ლენტურ დრაივებზე. მონაცემთა შენახვის არქიტექტურა უკანასკნელი 10 წლის მანძილზე მნიშვნელოვნად გაუმჯობესდა, შესაბამისად შემცირდა ღირებულება/გიგაბაიტზე. დისკური მასივების, კლასტერებისა და ვირტუალიზაციის პლატფორმათაშორისი პროგრამული უზრუნველყოფის მიმდინარე თაობა ქმნის ინფორმაციის ეფექტურად და ეკონომიურად დარეზერვების შესაძლებლობას როგორც ლოკალურად, ისე დისტანციურად.

ii) **ციფრული ხელმოწერები**: ერთ-ერთ უმთავრეს ამოცანას ყველა ბიზნეს-საწარმოსათვის, მაგრამ, განსაკუთრებით, სამთავრობო და საფინანსო დაწესებულებებისათვის, წარმოადგენს, მაგალითად, ქვეყნის კანონმდებლობაში, მნიშვნელოვან გეგმებში, თუ საბანკო ანგარიშებში მალული ცვლილებების შეტანის პრევენცია. მოკლედ, ინფორმაციის უსაფრთხოება დაკავშირებულია საწყისი მონაცემების ერთიანობასთან. დღეისათვის არსებული ოპერაციული გადაწყვეტილებები მოიცავს მზა ციფრულ ხელმოწერებს, დაშიფრულ ფაილებს, რომლებიც დაკავშირებულია კერძო/სახელმწიფო გადაწყვეტილებებთან, ასევე, ბიომეტრულ წვდომას თითების ანაბეჭდებით, თვალის ბადურას სკანირებას და ელექტრონული წვდომის სისტემების სხვა ფორმებს.

iii) **აღდგენა ავარიულ სიტუაციებში**: ბოლო დროს საქართველოში განვითარებულმა მოვლენებმა ცხადყო, რომ აუცილებელია შესაბამისი დაგეგმვა პოტენციური ავარიული სიტუაციების შემთხვევებისათვის. ასეთი შემთხვევები შეიძლება გამოწვეული იქნას როგორც ბუნებრივ (მიწისძვრა, ხანძარი, წყალდიდობა), ისე პოლიტიკურ (ომი, ტერორისტული აქტი) მიზეზთა გამო. ელექტრონულ ინფრასტრუქტურას სულ უფრო და უფრო ხშირად იღებენ მიზანში მტრის აგენტები, ხოლო გამანადგურებელი კიბერ-თავდასხმები სამთავრობო, სამხედრო

და საფინანსო ICT ინფრასტრუქტურაზე, როგორც წესი, ხდება ფიზიკურ ინვაზიამდე, მის დროს ან მას შემდეგ. **მე კიბერ-ბრძოლის საკითხი საქართველოს მთავრობის გადაწყვეტილების მიმღებ პირებთან და კომერციულ საინფორმაციო ხელმძღვანელებთან ერთად განვიხილე 2007 წლის სექტემბერში, ხოლო 2008 წლის აგვისტოს მოვლენებმა ტრაგიკულად დაადასტურა ამგვარი პროგნოზები.** ისეთ ორგანიზაციებს, როგორიცაა ASIS International, ხელთ აქვთ ბრწყინვალე დოკუმენტაცია, რომელიც მოიცავს ავარიულ სიტუაციაში მომზადების სახელმძღვანელოს და ბიზნესის უწყვეტობის პრინციპებს. ამდენად, სრულყოფილი სარეზერვო სისტემების დამონტაჟებასა და დისტანციური მონაცემთა ცენტრების შექმნასთან ერთად იმპერატიულ მოთხოვნას წარმოადგენს პერსონალის საფუძვლიანი მომზადება ევაკუაციის, ავარიულ რეჟიმზე გადასვლის პროცედურებსა და ტექნიკურ საკითხებში, რათა უზრუნველყოფილი იქნას კომუნიკაცია და წვდომა კრიტიკულად მნიშვნელოვან ინფორმაციაში ავარიული სიტუაციების დროს და შემდეგ.

iv) **ელექტრონული აქტივების მენეჯმენტი**: დღეისათვის, პერსონალისა და გადაწყვეტილების მიმღებთა უმრავლესობა ატარებენ პორტატულ მოწყობილობებს მნიშვნელოვანი და ზოგჯერ კონფიდენციალური ინფორმაციით. სამწუხაროდ, ასეთი მოწყობილობები ზოგჯერ იკარგება ან გამიზნულად იქურდება, მათ შორის, მემორი-სტიკები, ლაპტოპები, პორტატული დისკები, მობილური ტელეფონები და PDA ("ჯიბის კომპიუტერები"). ცალკეულ ოპერაციულ პროცედურებს არ ძალუძთ მონაცემთა დაკარგვის პრევენცია, მაგრამ, ასეთი მოწყობილობები ყურადღებით უნდა იმართებოდეს ოპერაციული პროცედურებისა და პოლიტიკების შესაბამისად. ეს, შეიძლება, მოიცავდეს, RFID (Radio Frequency IDentification) მარკირება, დაშიფრული დისკური დრაივები და შეზღუდვები პორტატული მოწყობილობების გატანაზე სამთავრობო, სამხედრო და საფინანსო დაწესებულებებიდან. საკვირველია, რომ ასე ხშირად ხდება ამგვარი მოწყობილობების "დაკარგვა" მატარებლებში, ტაქსებში თუ თვითმფრინავებში და ეს მოწყობილობები ხშირ შემთხვევებში უმნიშვნელოვანეს და კონფიდენციალურ ინფორმაციას შეიცავენ!

v) **შენობის ფიზიკური უსაფრთხოება**: დასავლეთის სამთავრობო ოფისების, ბანკებისა და მაღალპროფილური კორპორატიული ოფისების უმეტესობა დაფარულია რეალური დროის CCTV (Closed Circuit TeleVision) სისტემებით, ასევე,

შესვლა/გამოსვლის უსაფრთხოება ხშირად დაკავშირებულია RFID ბარათებთან და ბიომეტრული წვდომის მოწყობილობებთან. წარსულში ამ მოწყობილობებს ცალკე ქსელებში ამუშავებდნენ შენობის დაცვის თანამშრომლები, მაგრამ IP წვდომის ქსელების ევოლუციამ გამოიწვია ფიზიკური და ICT უსაფრთხოების მოთხოვნილებების სწრაფი კონვერგენცია. ახლა, ფართო დიაპაზონის IP CCTV გამოსახულებები, სახანძრო სიგნალიზაციის სისტემები და წვდომის კონტროლი ამუშავებს იგივე მაღალსიჩქარულ IP LANS/WANS-ს და იგივე მონაცემთა ცენტრის მოწყობილობებს იყენებს მულტიმედია-შენახვისათვის, ანალიზისა და დარეზერვებისათვის. ამგვარად, მომავალი 3 წლის დაგეგმვისათვის, ჩემი რეკომენდაცია ითვალისწინებს იმას, რომ საქართველომ სერიოზული ყურადღება უნდა მიაქციოს ინტეგრირებული სისტემების განვითარებას ICT და ფიზიკური შენობისა და საიტის უსაფრთხოებისათვის. ეს, მაგალითად, უზრუნველყოფს სტუმრებისა და პერსონალის გაკონტროლების შესაძლებლობას RFID და პერსონალური ბიომეტრიული მონაცემების მეშვეობით, რაც, თავის მხრივ, მნიშვნელოვნად შეამცირებს ელექტრონული აქტივების, მნიშვნელოვანი მონაცემებისა და დოკუმენტების გაქურდვის რისკს.

vi) **CERT:** "სასწრაფო კომპიუტერული დახმარების ბრიგადა" – აუცილებელია ეფექტური CERT-ის შექმნა, რომელიც შეიძლება პირდაპირ იყოს დაკავშირებული NATO-ს კიბერ-თავდაცვის ცენტრთან. როგორც კი უსაფრთხოებისათვის მნიშვნელოვანი შემთხვევა გამოვლინდება, CERT-ის მიერ შესრულდება წინასწარ დაგეგმილი პროცედურა, რათა მინიმიზებული იქნას დეზინტეგრაცია საქართველოს მთავრობასა და მსხვილ საწარმოებში. CERT-ის დანერგვა და ფუნქციონირება უშუალოდ იქნება ინტეგრირებული ბიზნესის უწყვეტობისა და ავარიულ სიტუაციებში აღდგენის გეგმებთან.

vii) **ტრენინგი უსაფრთხოების საკითხებში**: თანმიმდევრული ტრენინგის არარსებობისას, მრავალი ტექნოლოგიური გადაწყვეტილება მხოლოდ ნაწილობრივ თუ იქნება ეფექტური, რადგან, როგორც უკვე აღინიშნა, უსაფრთხოების გაუმართაობების 40% მაინც გამოწვეულია ბუნებრივი მიზეზებითა და ადამიანის ინტერვენციის შედეგად. ამდენად, **"ვარძიის პროექტის" პროგრამებში ჩვენ განუწყვეტლივ ვამახვილებთ ყურადღებას უსაფრთხოების ქართველი სპეციალისტების კვალიფიკაციის ამაღლების აუცილებლობაზე,** რომლებსაც შეუძლიათ იმუშავონ თბილისში დაფუძნებულ IT

კონტრაქტორებთან, როგორიცაა, მაგალითად, შპს "ორიენტ-ლოჯიკი". ინვესტირება IT უსაფრთხოების დარგში იქნება ე-საქართველოს წარმატების ერთ-ერთი მნიშვნელოვანი კრიტერიუმი.

(6) მოკლევადიანი პროგრამა (6 თვიდან 1 წლამდე): ე-საქართველოს დაცვა, სამთავრობო, საქმიანი, საგანმანათლებლო დაწესებულებებისა და საავადმყოფოების ჩათვლით, წარმოადგენს გრძელვადიან პროგრამას, რომელიც მოითხოვს უწყვეტ ინვესტირებას ეროვნული თავდაცვისა და სამხედრო ინფრასტრუქტურის მსგავსად. ვარძიის პროექტის განხორციელება 3 მთავარ ფაზად დავყავი, რომელთა მიზანია ISO27000 საერთაშორისო სტანდარტების მიღწევა 3-დან 5 წლამდე პერიოდში (2012-დან 2014-მდე).

პირველ რიგში ჩამოვთვლით იმ ქმედებებს, რომელთა განხორციელება დაუყოვნებლივ უნდა დაიწყოს საქართველოს მთავრობის კომპიუტერული და ქსელური რესურსების უსაფრთხოების დაცვის მიზნით. ეს, ასევე, უნდა მოიცავდეს სამხედრო კომუნიკაციებისა და ელექტრონული ქსელების ინტენსიურ გადახედვას. ამ გადაუდებელი ზომების სრული პროგრამის განხორციელება, ალბათ, 3-დან 4 თვემდე ვადას მოითხოვს – 2008 წლის ნოემბერი/დეკემბერი – 2009 წლის იანვარი/თებერვალი.

ა) **კიბერ-უსაფრთხოების განყოფილება**: უსაფრთხოების საბჭომ უნდა შექმნას კომპიუტერული ქსელების წამყვანი სპეციალისტების - როგორც ადგილობრივი, ისე საერთაშორისო - პატარა ჯგუფი. ეს ჯგუფი (არაუმეტეს 7 კაცისა) პასუხისმგებელი იქნება კიბერ-უსაფრთხოების გადახედვაზე ყველა სამინისტროში, პრეზიდენტის სამსახურში, საქართველოს პარლამენტში და სხვა მაღალპროფილურ საფინანსო დაწესებულებებსა და საწარმოებში.

ბ) **მთავრობის უსაფრთხოების სისტემის გადახედვა**: 2007 წლის სექტემბერში ჩემს მიერ სრულყოფილად იქნა განხილული საქართველოს პარლამენტის კიბერ-უსაფრთხოება და ფიზიკური უსაფრთხოების რამდენიმე ასპექტი, ევროგაერთიანების მოთხოვნისამებრ. ასეთივე საფუძვლიანი გადახედვა და რეკომენდაციები ეხება ყველა მნიშვნელოვან სამინისტროს – საგარეო საქმეთა, ფინანსთა, იუსტიციის, შინაგან საქმეთა სამინისტროს ჩათვლით, პრეზიდენტის სამსახურს და, ასევე, სამხედრო უწყებებს. კიბერ-უსაფრთხოების დეტალური

აუდიტი მოითხოვს 2-3 სრულ სამუშაო დღეს, მაგრამ, ჯგუფმა პარალელურად უნდა იმუშაოს, ისე, რომ ყველაფერი შესრულებული იქნას 4-დან 6 სამუშაო კვირაში.

გ) **საკონტროლო სია**: ჯგუფმა უნდა შეადგინოს უსაფრთხოების საკითხების საკონტროლო სიის ტრაფარეტები თითოეული სამინისტროსათვის, რათა უსაფრთხოების სუსტი მხარეები დაუყოვნებლივ იქნას იდენტიფიცირებული, ხოლო შესაბამისი გადაწყვეტილებები – ადგილობრივ ჯგუფებთან განხილული.

დ) ინფორმაციის დარეზერვება: აუცილებელია რეგულარული შემოწმებების ჩატარება იმის დასადასტურებლად, რომ ყოველგვარი სამთავრობო ინფორმაცია, მონაცემთა ბაზები, იმეილები და არქივები სრულად არის დარეზერვებული დაცულ, ცეცხლგამძლე სათავსებში და - დუბლირებული დაცულ მედიაზე.

ე) პროგრამული უზრუნველყოფისა და სისტემების განახლება: სავარაუდოა, რომ კომპიუტერული სერვერებისა და ქსელური აპარატურის უმეტესობა საჭიროებს უსაფრთხოების ამა თუ იმ ფორმით განახლებას, გაფართოებული RAID-ტიპის მეხსიერებით, დამატებითი პროცესორებით, მონაცემთა ცენტრების დიდი ინსტალაციებისათვის ვირტუალიზებული შენახვის ვარიანტის შესწავლით. საჭიროა ადგილობრივი სპეციალისტი-კომპანიების, როგორიცაა "ორიენტ-ლოჯიკი", მოწვევა ჯგუფთან სამუშაოდ, რათა უზრუნველყოფილი იქნას უსაფრთხოების პროგრამული უზრუნველყოფის ყველაზე მოწინავე, ოპტიმალური დაცვის საშუალებების დამონტაჟება მთელს ცენტრალურ ხელისუფლებაში და საქართველოს სამხედრო ინსტალაციებში და მონაცემთა ცენტრების განახლება ჯგუფის რეკომენდაციების შესაბამისად. ზოგადად, ყველა კომპიუტერული სერვერი, ბაზა, მარშრუტიზატორი და ქსელი კოპირებული უნდა იქნას, სისტემური გაუმართაობის პოტენციური ცალკეული წერტილების რიცხვის მინიმიზების მიზნით.

ვ) ქსელური და უსადენო კავშირი: ეს მოიცავს ყველა ფიზიკურ კაბელს, უსადენო ქსელს და თანამგზავრულ ბმულებს, რომლებიც საქართველოს მთავრობის მიერ ამჟამად გამოიყენება კომუნიკაციისათვის როგორც საქართველოს ფარგლებში, ისე საერთაშორისო ქსელურ გეითვეისთან, მაგალითად, შავი ზღვის გასწვრივ, რადიო და თანამგზავრი. საუკეთესო შემთხვევაში, IP მისამართები და სერვერები დუბლირებული უნდა იქნას "გასაიდუმლოებული" ალტერნატიული სარეზერვო მისამართებით, ხოლო დისტანციური სარეზერვო სერვერები აუცილებლად უნდა იქნას გათვალისწინებული მომსახურეობის გაწევის განაწილებული უარყოფის ან სხვა, ფართომასშტაბიანი, გამანადგურებელი კიბერ-თავდასხმის შემთხვევებისათვის.

ზ) ვებ-საიტებისა და სერვერების დარეზერვება: აუცილებელია ყველა ვებ-საიტის დარეზერვება დომეინზე გადართვის სწრაფი (5 წუთზე ნაკლებ დროში) ოფციონის შესაძლებლობით (ალტერნატიული IP მისამართით) ალტერნატიულ ვებ-სერვერზე, რომელიც მდებარეობს საქართველოში, დაცულ ადგილას ან საზღვარგარეთ. ალტერნატიულ ვებ-საიტს, საუკეთესო შემთხვევაში, უნდა ჰქონდეს Ddos დაბალ-დონიანი პაკეტების აღმქმელი პროგრამული უზრუნველყოფა ავტომატური Ddos სიგნალიზაციითა და ფილტრით, რათა უცხო (კიბერ-თავდასხმის) IP პაკეტები რეალურ დროში იქნას დაკავებული და დამუშავებული შეთანხმებული წესების შესაბამისად.

თ) მონაცემთა ბაზების უსაფრთხოება: ზოგ კომერციულ და სამთავრობო SQL მონაცემთა ბაზაში შენარჩუნებულია მათი დეფოლტური პაროლები, რომელთა ჰაკირება და კომპრომეტირება ადვილად არის შესაძლებელი მტრულად განწყობილი ჰაკერებისათვის. კომპრომეტირების შემდეგ, მონაცემთა ბაზა შეიძლება შეიცვალოს, მოპარულ იქნას ან უბრალოდ წაიშალოს. აქედან გამომდინარე, აუცილებელია ყველა სამთავრობო მონაცემთა ბაზის შემოწმება იმის დასადასტურებლად, რომ უზრუნველყოფილია სრულყოფილი ორმაგი ფაიერვოლი ელექტრონული დემილიტარიზებული ზონით (DMZ) და პროქსი IP მისამართებით.

ი) ინფორმაციის მთლიანობა: ზოგჯერ ჰაკერები აღწევენ მონაცემთა ბაზაში და შეაქვთ მცირედი, თუმცა სტრატეგიული ცვლილებები, რომლებიც შეიძლება მაშინვე ვერ იქნას იდენტიფიცირებული ოპერაციული პერსონალის მიერ. ეს განსაკუთრებით საშიშია, თუ ჰაკერი ტროას ცხენის ვირუსს გაუშვებს, რომელიც გარკვეულ მონაცემებს მის საკუთარ კომპიუტერში დააბრუნებს. ეს ხშირად ხდება საბანკო ან საფინანსო სისტემების ჰაკირების დროს. თუმცა, საქართველოს მთავრობის შემთხვევაში, ეს ნიშნავს, რომ მტრის აგენტებს უკვე აქვთ მალულად და უხილავად განხორციელებული სამინისტროების საინფორმაციო სისტემების კომპრომეტირება, რასაც თან სდევს მნიშვნელოვანი და კონფიდენციალური ინფორმაციის გადაგზავნა მათ სერვერებში (მთავარი სიტყვის მითითებით). კიბერ-უსაფრთხოების ჯგუფი პასუხისმგებელი იქნება სამთავრობო მონაცემთა სისტემების ასეთი სახიფათო გზით კომპრომეტირების მდგომარეობის შემოწმებაზე.

ამ გადაუდებელი მოკლევადიანი ზომების მიღება უნდა დასრულდეს მომდევნო 4 თვის განმავლობაში.

(7) საშუალოვადიანი პროგრამა (2-დან 3 წლამდე): კიბერ-უსაფრთხოების ჯგუფის მიერ მთავრობის უსაფრთხოების სრულყოფილი აუდიტის ჩატარების შემდეგ მოსალოდნელია, რომ NATO ხელს შეუწყობს კიბერ-თავდაცვის ადგილობრივი ცენტრის შექმნას, რომელიც შეასრულებს საქართველოს ეროვნული CERT-ის, ტრენინგის ცენტრისა და უსაფრთხოების წარმატების საერთო ცენტრის (COE - Centre of Security Excellence) ფუნქციას. რა თქმა უნდა, უსაფრთხოების ნებისმიერი თანმიმდევრული არქიტექტურა, მე-12 საუკუნის ვარძიის გამოქვაბულთა სისტემის მსგავსად, მოითხოვს სრულ განაწილებას, ისე, რომ ვიდრე COE ასრულებს უსაფრთხოების დაცვის ცენტრალური "ტაძრის" როლს, ქსელის ყველა სხვა კვანძი, სერვერი, ბაზა და ენდ-პიონტი, ასევე, საჭიროებს მეთვალყურეობას და სრულ დაცვას რეალურ დროში.

სპეციფიური საშუალოვადიანი საკითხები, რომლებიც მოგვარებული და გაკონტროლებული უნდა იქნას კიბერ-უსაფრთხოების ჯგუფის მიერ:

ა) **მონაცემთა ცენტრის შენახვა და ვირტუალიზაცია**: საქართველოს პარლამენტში შესრულებული სამუშაოების შედეგად მიღებული გამოცდილებიდან ჩანს, რომ გასულ წლებში კიბერ-თავდასხმებისა და კიბერ-ბრძოლის პოტენციური საშიშროება თითქმის არასოდეს ყოფილა სათანადოდ შეფასებული. უნდა გვესმოდეს, რომ საქართველოს მთავრობამ, რომელიც მისი ევროპელი და ამერიკელი მოკავშირეებისაგან ფინანსურ და რესურსულ მხარდაჭერას იღებს, მნიშვნელოვანი ინვესტიციები უნდა განახორციელოს ელექტრონული ქსელისა და კომპიუტერული ინფრასტრუქტურის სრული განახლების მიზნით. შემდეგ ეს შეასრულებს საიმედო და მდგრადი დამცავი ფარის როლს მომავალი ორგანიზებული ჰაკირების და კიბერ-ტერორისტული აქტების წინააღმდეგ. კერძოდ, მნიშვნელოვანი ინვესტიციები დაგეგმილი უნდა იქნას მომდევნო 3 წლის განმავლობაში დუბლირებულ და ვირტუალიზებულ მონაცემთა ცენტრებში, რათა უზრუნველყოფილი იქნას ე-მთავრობისა და ე-ბიზნესის ექსტენსიური პროგრამები.

ბ) **რეგიონალური მთავრობა:** საშუალოვადიან პერიოდში, გადასახედი და განსაახლებელია მთავრობის რეგიონალური ოფისების ელექტრონული უსაფრთხოებისა და თავდაცვის სისტემები, ვინაიდან სწორედ აქედან შემოდის ინფორმაცია ცენტრალური მთავრობის სამინისტროებში.

გ) **ტრენინგი უსაფრთხოების საკითხებში:** შესაბამისმა IT და კომპიუტერულმა პერსონალმა უნდა გაიაროს ინტენსიური ტრენინგი 21-ე საუკუნის კიბერ-უსაფრთხოების გადაწყვეტილებებში კიბერ-თავდაცვის ეროვნული ცენტრის მიერ ადგილობრივ სპეციალისტ-კომპანიებთან, როგორიცაა შპს "ორიენტ-ლოჯიკი", ორგანიზებული ადგილობრივი კურსების საშუალებით.

დ) **უსაფრთხოების სტანდარტები:** აუცილებელია უსაფრთხოების საერთაშორისო ISO/ISF სტანდარტებთან დაკავშირებული თანმიმდევრული ტრენინგების ჩატარება. აღნიშნული სტანდარტები დანერგილი უნდა იქნას მომდევნო 2-3 წლის განმავლობაში.

ე) **ბიზნესის უწყვეტობა:** ბოლო თვეებში განვითარებულმა მოვლენებმა გვიჩვენა, თუ რაოდენ მნიშვნელოვანია წინასწარ შემუშავებული გეგმებისა და სარეზერვო ოფციონების ქონა IT სისტემების გაუმართაობებისა და კიბერ-თავდასხმების შემთხვევებისთვის. კიბერ-უსაფრთხოების ჯგუფი ამ გეგმებსა და ოფციონებს, ცალკეული სამინისტროს დეპარტამენტებთან ერთად, შეიმუშავებს მომდევნო 6-9 თვის განმავლობაში. კერძოდ, ჯგუფმა უნდა უზრუნველყოს კომპიუტერული ბაზების, სერვერებისა და ქსელური კავშირის დუბლირება კრიტიკულად მნიშვნელოვანი სამთავრობო რესურსებისათვის.

ვ) **აღდგენა ავარიულ სიტუაციებში:** ბიზნეს უწყვეტობასთან მჭიდროდ არის დაკავშირებული აღდგენის გეგმები ავარიული სიტუაციების შემთხვევაში, როგორიცაა კიბერ-ტერორისტული თავდასხმები, შესაძლო წყალდიდობები, ხანძრები და მიწისძვრები. ასეთი ავარიული მოულოდნელობებისათვის საქართველოს მთავრობამ სერიოზული ყურადღება უნდა გაამახვილოს თბილისის გარეთ დისტანციური და დაცული მიწისქვეშა კომპიუტერული ობიექტის მშენებლობაზე, რომელიც შეასრულებს ალტერნატიული სამთავრობო პუნქტის ფუნქციას პარლამენტისა და ცენტრალური ხელისუფლების სამსახურების იძულებითი ევაკუაციის შემთხვევაში.

ზ) **მომსახურეობის გაწევის განაწილებული უარყოფა (Ddos):** არსებობს ალბათობა იმისა, რომ Ddos თავდასხმები რამდენიმე თვის, თუ არა წლის მანძილზე გაგრძელდება საქართველოს მტრებთან გაერთიანებულ პირთა მხრიდან. აქედან გამომდინარე, საჭიროა სრულყოფილი დაცვის შეძენა და დანერგვა, გამოყოფილი Ddos ქსელის აპარატული უზრუნველყოფის ჩათვლით, რომელიც რეალურ დროში ამოწმებს და ფილტრავს ყოველი შემოსული მონაცემთა IP პაკეტის სათაურს და სრულ შინაარსს. ასეთი სისტემები საჭირო იქნება ქსელთაშორისი შლუზის (gateway) სახით ყველა სამთავრობო სამინისტროს, საქართველოს პარლამენტის და მთავარი სამხედრო ინსტალაციებისათვის. ასევე, გათვალისწინებული უნდა იქნას ასეთი სისტემების დამონტაჟების სავალდებულო მოთხოვნა ყველა ქართული კომერციული საფინანსო თუ საბანკო დაწესებულებისათვის.

თ) **ე-ბიზნეს საწარმოები**: პირველი GITI კონფერენციის დისკუსიებისა და შედეგების შესაბამისად, მოსალოდნელი უნდა იყოს ის, რომ მომავალ წელს დაიწყება, ხოლო საშუალოვადიან პერიოდში განხორციელდება პირველი მსხვილი ინვესტირება და ერთობლივი საწარმოების შექმნა ე-ბიზნესში. ჩემი პირადი IT გამოცდილების საფუძვლად შემიძლია ვთქვა, რომ ე-ბიზნესი საბოლოო ჯამში შეაღწევს ქართული ბიზნესისა და მეწარმეობის ყველა ასპექტში, დაწყებული ე-მთავრობიდან, დამთავრებული ე-ჯანდაცვით, ე-განათლებით, ე-დაფინანსებით, ე-შოპინგით და გლობალური ე-ვაჭრობით! ეს ელექტრონული სავაჭრო გზები წარმოადგენს 21-ე საუკუნის "აბრეშუმის გზებს", ხოლო სრულად დაცული და უსაფრთხო განაწილებული ქსელის შექმნა არის საქართველოს პირველი ე-ბიზნეს საწარმოების მომავალი მდგრადობისა და წარმატების საწინდარი. ნუ უგულებელყოფთ ინვესტირებას კარგ უსაფრთხოებაში!

(8) შედარებით გრძელვადიანი პროგრამა (4-დან 5 წლამდე): "ვარძიის პროექტის" უსაფრთხოების პრინციპების დანერგვის შემდეგ დროა გავაფართოვოთ რეალური დროის ე-საქართველოს პროგრამა, რათა უზრუნველყოფილი იქნას უსაფრთხო საერთაშორისო კავშირი სხვა ე-მთავრობის ქსელებსა და, ასევე, გლობალურ ე-ბაზართან.

ა) **ე-მთავრობების ურთიერთფუნქციონირების ევროპული პროგრამა – EIF:** მრავალი სამთავრობო საქმიანობა და პროგრამა აღწევს საერთაშორისო საზღვრებს –

საგარეო საქმეთა სამინისტრო, სახელმწიფო გადასახადები, კანონმდებლობა, ფინანსები და, ასევე, საქართველოს საკონსულოებისა და საელჩოების მსოფლიო ქსელი. აქედან გამომდინარე, ძალზედ მნიშვნელოვანი იქნება საქართველოს ე-მთავრობის ქსელისა და პროგრამების პრაქტიკული მშენებლობა განხორციელდეს საერთაშორისო კომპიუტერული და პროგრამული უზრუნველყოფის სტანდარტების შესაბამისად, როგორიცაა IEEE და ISO – საერთაშორისო სტანდარტების ორგანიზაციის სტანდარტები. სხვა შესაძლო ტრანს-ეროვნული კავშირი შეიძლება მოიცავდეს NATO-ს, გაეროს, IMF-ს, მსოფლიო ბანკს და მრავალ სხვა საერთაშორისო სავაჭრო ორგანიზაციას. ყველა ამ შემთხვევაში, უსაფრთხოების რეალურ დროში დაცვის საშუალებები უნდა იქნას შეთანხმებული და განახლებული იმისათვის, რომ უზრუნველყოფილი იქნას საქართველოს დაცვა პროგრამული უზრუნველყოფის ვირუსების და სხვა სადაზვერვო ონლაინ აგენტების ელექტრონული ინვაზიისაგან.

ბ) **საერთაშორისო ე-ვაჭრობის ქსელური კონცენტრატორი (ჰაბი)**. საქართველოს ე-ბიზნესის პროგრამის ერთ-ერთ უმთავრეს მიზანს წარმოადგენს მისი ეკონომიკური კონკურენტუნარიანობის გაძლიერება საერთაშორისო ბაზარზე. თბილისი დაარსდა აბრეშუმის ფიზიკურ სავაჭრო გზაზე ჩინეთიდან დასავლეთისაკენ, მაგრამ ახლა ასეთი ვაჭრობა, ისეთ ძვირადღირებულ საქონელთან ერთად, როგორიცაა ნავთობი და გაზი, სწრაფად გადადის ინტერნეტზე. საქართველოს ეკონომიკური რეპუტაცია დამოკიდებული იქნება სწორედ ამ 21-ე საუკუნის ელექტრონული სავაჭრო გზების უსაფღთხოებასა და დაცულობაზე, ამიტომ, აუცილებელია უწყვეტი ინვესტირება შემოჭრის დეტექტორულ სისტემებში, გაძლიერებულ სერვერებში, დუბლირებულ ბაზებში, ვირტუალიზაციაში, უსაფრთხოების სფეროს ტრენინგსა და შესაძლო საგანგაშო და ავარიულ სიტუაციებში სამოქმედო გეგმების მომზადებაში.

გ) **ფიზიკური და ელექტრონული უსაფრთხოების ინტეგრაცია:** მომდევნო 5 წლის განმავლობაში, როგორც ნავარაუდევია, ფიზიკური დაცვის საშუალებების უმეტესობა, როგორიცაა CCTV ქსელები და წვდომის კონტროლი, ციფრულ სისტემაზე იქნება გადაყვანილი IP ქსელების მეშვეობით, ხოლო მაღალი რეზოლუციის კამერები, მანქანის სანომრე ნიშნების ავტომატური ამომცნობები (ANPR) და თანამგზავრული გამოსახულებები ინტეგრირებული იქნება ახალი

თაობის უსაფრთხო მონაცემთა ცენტრის პროგრამებში. დღეისათვის მრავალ სამთავრობო და კომერციულ ობიექტებში უსაფრთხოების ინდივიდუალური ორგანიზაციები არსებობს ფიზიკური და IT უსაფრთხოებისათვის. ვიმედოვნებთ, რომ NATO-ს კიბერ-თავდაცვის ცენტრი, ასევე, ხელს შეუწყობს ფიზიკური CCTV და ელექტრონული IT უსაფრთხოების სრულ ინტეგრაციას შედარებით გრძელვადიანი - 3-5 წლიანი - პროგრამის ფარგლებში.

დ) ბიომეტრული ID და RFID აქტივების მენეჯმენტი: წარსულში მე ტექნიკურ დირექტორად ვმუშაობდი უსაფრთხოების გადაწყვეტილებების ერთ-ერთ მსხვილ საერთაშორისო პროვაიდერ-კომპანიაში (ახლა ამ კომპანიას ეწოდება Stanley Security Solutions Ltd.). პროდუქტები მოიცავდა თითების ანაბეჭდების ბიომეტრულ რიდერებს და RFID აქსეს-ბარათებს ისეთი უაღრესად დაცული ობიექტებისათვის, როგორიცაა ციხეები და სპეციალური სამთავრობო დაწესებულებები. ასეთი ბიომეტრული მოწყობილობების ღირებულება თანდათან მცირდება და ხელმისაწვდომი ხდება ყველა ორგანიზაციისათვის, რაც ხელს უწყობს მოწინავე ტექნოლოგიური კონტროლის დანერგვას უნიკალურად პერსონალურ დონეზე. გასულ კვირას მე მონაწილეობა მივიღე Biometrics2008 გამოფენასა და კონფერენციაში, რომელიც ჩატარდა ვესტმინსტერში, ლონდონში. გამოფენაზე წარმოდგენილი იყო ყველა მსხვილი ვენდორის უახლესი გადაწყვეტილებები. ნათელია, რომ ასეთი ბიომეტრული მოწყობილობები საფუძველს შეუქმნის უსაფრთხოების დაცვის ინოვაციურ საშუალებებს საქართველოს ე-მთავრობისა და ე-ბიზნესის პროგრამებისთვის.

ე) საბოლოო მომხმარებლის მოწყობილობებისა და პროგრამების უსაფრთხოება: ამჟამად მთელს მსოფლიოში შეინიშნება ტენდენცია, რომელიც ითვალისწინებს მონაცემთა ცენტრების ვირტუალიზაციას და ქსელური სერვერების, ბაზების, მომსახურეობებისა და პროგრამების განთავსებას "ღრუბლებში". გარდა ამისა, საბოლოო მომხმარებლის პორტატული და ჭკვიანი მოწყობილობების რიცხვი და ტიპები, როგორც მოსალოდნელია, მნიშვნელოვნად გაიზრდება მომავალი 5-10 წლის განმავლობაში. ყველა ეს ტენდენცია გულისხმობს იმას, რომ უსაფრთხოების ტრადიციული პერიმეტრი, რომლის დაცვაც შესაძლებელია, სწრაფად იფანტება! უსაფრთხოების წამყვანი საერთაშორისო ვენდორები, როგორიცაა Symantec (რომელიც თბილისში წარმოდგენილია შპს "ორიენტ-

ლოჯიკის" სახით), უკვე აფართოებენ უსაფრთხოების საკუთარ მზა პროგრამებს ქსელური საფრთხეების ამ ახალი თაობისაგან დაცვის მიზნით.

არსებობს ერთ-ერთი ახალი ორგანიზაცია – Jericho Forum – რომელიც აწარმოებს უსაფრთხოების ბლუპრინტების (სქემების) შემუშავებას ასეთი ღია ქსელური გარემოებისათვის, სადაც არ არის განსაზღვრული ტრადიციული IT პერიმეტრი. მართლაც, ორმაგი ფაიერვოლები (DMZ) ყოველთვის დიდ გამოყენებაში იქნება LAN დონეზე, მაგრამ, გაფართოებული Campus/Metropolitan/Wide Area ქსელების შემთხვევაში უსაფრთხოება უზრუნველყოფილი უნდა იქნას საბოლოო მომხმარებლის თითოეულ ქსელურ მოწყობილობაში, მარშრუტიზატორში, სვიჩში, შემნახველ მოწყობილობასა და პროგრამაში. რეალურ დროში დაშიფრვა, როგორიცაა RSA/PGP ალგორითმები, უზრუნველყოფს ნაწილობრივ გადაწყვეტილებას და, აქედან გამომდინარე, საქართველოს კიბერ-თავდაცვის ცენტრს გამოწვევების უწყვეტი პროგრამა ექნება განსახორციელებელი Real-Time Georgia-ს უსაფრთხოების უზრუნველყოფის მიზნით. ჩვენი ხუთწლიანი "ვარძიის პროექტის" უმთავრესი ამოცანაა უსაფრთხოების მოქნილი და თანმიმდევრული დამცავი ფარის შექმნა ინვაზიური აგენტების, "აგენტი-რობოტებისა" და კიბერ-კრიმინალების წაინააღმდეგ!

(9) მომდევნო პრაქტიკული ზომები (3-დან 6 თვემდე – 2008 წლის ნოემბრიდან 2009 წლის აპრილამდე): ბოლო 10 გვერდზე ჩვენს მიერ განხილული იქნა უსაფრთხოების, გადაწყვეტილებებისა და პროგრამების დივერსიფიცირებული სპექტრი. ახლა, საქართველოს პარლამენტში მიღებული გამოცდილების საფუძვლად, დავუბრუნდეთ საწყისებს და შევაჯამოთ ის პრაქტიკული ქმედებები, რომლებიც საქართველომ უნდა განახორციელოს ე-მთავრობისა და ე-ბიზნესის დაცვის უზრუნველყოფის მიზნით:

ა) მთავრობის უსაფრთხოების პროფესიონალების სრულ-შტატიანი ჯგუფის შექმნა (მაქს. 7 კაცი);

ბ) ყველა სტრატეგიული სამთავრობო IT ობიექტის თანმიმდევრული აუდიტის ჩატარება. ყურადღება, ძირითადად, გამახვილებული უნდა იქნას გაუმართაობის

ყოველი ცალკეული წერტილის იდენტიფიცირებაზე, დარეზერვების დეფიციტზე, მონაცემთა ქურდობის ან ჰაკირების შესაძლებლობებზე;

გ) კიბერ-თავდასხმისა და მომსახურეობის გაწევის უარყოფის შემთხვევების ელექტრონული პროტოკოლების შემოწმება, რომლებიც შეიძლება მოხდა 2008 წლის ივლისის/აგვისტოს/სექტემბრის თვეებში. უნდა ჩატარდეს შესაბამისი IT სისტემების, ქსელების, ქსელთაშორისი შლუზების, მარშრუტიზატორებისა და სერვერების სუსტი მხარეების ტექნიკური სასამართლო გამოძიება;

დ) სამთავრობო დეპარტამენტებთან მუშაობა ცალკეულ შემთხვევებზე იმის დასადასტურებლად, რომ ყოველგვარი მნიშვნელოვანი, სენსიტიური და კონფიდენციალური ინფორმაცია, გეგმა და მონაცემთა ბაზა სრულად დარეზერვებული და დუბლირებულია ლენტურ ან დისკურ მატარებელზე.

ე) მუშაობა NATO-სა და ევროგაერთიანების მიერ დანიშნულ პროფესიონალებთან კიბერ-თავდაცვის ეროვნული ცენტრის შექმნის მიზნით, რომელიც გააერთიანებს უსაფრთხოების მონიტორინგის, საგანგაშო მდგომარეობების, CERT-ისა და ტრენინგის ცენტრებს საქართველოში.

ვ) სამინისტროებისა და სააგენტოების ინდივიდუალური უსაფრთხოებისა და IT აუდიტის შედეგების საფუძვლად დეტალური საინჟინრო გეგმებისა და მოთხოვნილებების შემუშავება უსაფრთხოების გადაწყვეტილებების მსოფლიოში ცნობილ საერთაშორისო კონსულტანტებსა და ადგილობრივ ვენდორებთან განხილვის მიზნით;

ზ) IT უსაფრთხოების სპეციალისტთა ტრენინგის კურსის ჩატარება ეროვნული კადრების კვალიფიკაციის ამაღლების მიზნით.

10) **რეზიუმე**: Real-Time Georgia-ს წარმატება მოითხოვს მნიშვნელოვანი ინვესტიციების განხორციელებას IT ინფრასტრუქტურის განახლებასა და მისი სრული უსაფრხოების შენარჩუნებაში. წინამდებარე დოკუმენტში – Security White Paper – მოცემულია წინადადება – საქართველოს მთავრობის მიერ "**ვარძიის პროექტის**" 3-5 წლიანი პროგრამის განხორციელება, რაც უზრუნველყოფს ქვეყნის სრულფასოვან დაცვას მომავალი კიბერ-თავდასხმების, კიბერ-დანაშაულების თუ სხვა ელექტრონული ინვაზიებისაგან.

დანართი: უსაფრთხოების რეფერენციები

ქვემოთ მოცემული რეფერენციები უფასოდ არის ხელმისაწვდომი ონლაინ რეჟიმში, ISO/IEC 27000 სტანდარტებთან ერთად, რომელთა შესყიდვა შესაძლებელია ინტერნეტით, შემდეგ მისამართზე: www.iso.org

ა. ASIS International 2005 – ბიზნესის უწყვეტობის გაიდლაინები (მათ შორის, "აღდგენა ავარიულ სიტუაციებში");

b. საინფორმაციო უსაფრთხოების ფორუმი – 2007 წლის ოქტომბერი – უსაფრთხოების გაიდლაინები – www.securityforum.org;

გ. გერმანიის მთავრობა 2004 – IT უსაფრთხოების გაიდლაინები (უსაფრთხოებისა და IT სამინისტრო);

დ. ISO/IEC 27001/27002 გაიდლაინები – 2005 და განახლებები – www.iso.org;

ე. ECD გაიდლაინები საინფორმაციო სისტემებისა და ქსელების უსაფრთხოებისათვის – 2002;

ვ. აშშ კონგრესი – უსაფრთხოება საინფორმაციო ერაში – მაისი, 2002;

ზ. გაერთიანებული სამეფოს მთავრობა – ქსელის დაცვა – 2002;

თ. გაერთიანებული სამეფოს მთავრობა – უსაფრთხოების არქიტექტურა – ვერსია 4.0 – 2002;

ი. გაერთიანებული სამეფოს მთავრობა – რეგისტრაცია და აუთენტიკაცია – ვერსია 4.0 – 2002;

კ. FIEC – ინფორმაციის უსაფრთხოება – IT შემოწმების სახელმძღვანელო – ივლისი, 2006;

ლ. EIF – ევროპის ქსელების ერთობლივი ფუნქციონირების სტრუქტურა პან-ევროპული ე-მთავრობისათვის – 2004;

მ. International Jericho Forum – "უსაფრთხოების დეპარამეტრიზაცია" www.opengroup.org/jericho/.

პერსონალური მადლობები

გულწრფელი მადლობა მინდა გადავუხადო ყველა იმ ადამიანს, რომელიც დახმარებას მიწევდა საქართველოს რესპუბლიკაში მუშაობისას.

კერძოდ, მადლობას ვუხდი ბატონ **მერაბ გოცირიძეს** (პარლამენტის IT მენეჯერს) და მისი IT სპეცუიალისტების არაჩვეულებრივ გუნდს. შემდეგ, მადლობას ვუხდი დოქტორ **დიმიტრი ყიფიანს** და მის გუნდს შპს "ორიენტ-ლოჯიკში" მათი მხარდაჭერისა და მოთმინებისთვის; განსაკუთრებულ მადლობას ვუხდი ბატონებს **სერგეი სანაკოევს**, **ირაკლი აკიმოვს** და მათ ოჯახებს. მადლობა **ნოდარ მოსაშვილს**, ჩემს ზველ მეგობარსა და კოლეგას, რომელმაც პირველმა გამაცნო საქართველო გასული საუკუნის რთულ 90-იან წლებში. ასევე, გულწრფელ მადლობას ვუხდი ჩემს ძველ მეგობარსა და კოლეგას **პაველ ხრაპკინს** (Symantec Europe) მისი თანმიმდევრული რჩევებისათვის როგორც წინამდებარე დოკუმენტთან დაკავშირებით, ისე ჩემი გასული წლის მივლინების დროს. და ბოლოს, მადლობა **ირაკლი გვენეტაძეს** და საორგანიზაციო ჯგუფს, რომელმაც თბილისში მოაწყო ეს კონფერენცია – 1st Georgian IT Innovation Conference!

პროფესიონალური რეზიუმე

დრ. დეივიდ ე. პრობერტი

***VAZA International* – www.vaza.com**

- ***Computer Integrated Telephony (CIT)*** – "ბრიტიშ ტელეკომ"-ის £ 25 მ EIGER პროექტის ხელმძღვანელი 1980-იანი წლების შუა პერიოდში, რომელიც ითვალისწინებდა კომპიუტერების ინტეგრაციას სატელეფონო კომუტატორებთან (PABX's). პროექტის განხორციელებას შედეგად მოჰყვა ***CIT*** პროგრამების წარმატებული შემუშავება და გაშვება ტელესეილისა და ტელემარკეტინგის ოპერაციებისათვის მსოფლიო ბაზარზე;
- ***Blueprint for Business Communities*** – წარმოსახვითი პროგრამა ციფრული აპარატურის კორპორაციისათვის 1980-იანი წლების ბოლოს, რომელიც ითვალისწინებდა "ცოდნის ობიექტივისა" და "საზოგადოებრივი ქსელების" შექმნას. ბლუპრინტი წარმოადგენდა სტრატეგიულ სტრუქტურას ციფრული აპარატურის კორპორაციის დამატებითი მომსახურეობების ქსელური ბიზნესისათვის, რომელმაც მნიშვნელოვანი კონტრაქტები მიიღო სამეწარმეო ქსელებისათვის;
- ***European Internet Business Group (EIBG)*** – ციფრული აპარატურის კორპორაციის ევროპის ინტერნეტ ჯგუფის შექმნა და ხელმძღვანელობა 5 წლის მანძილზე, 1994 – 1999. პროექტები მოიცავდა ინტერნეტის ეროვნული ინფრასტრუქტურის მხარდაჭერას EMEA ქვეყნებში, ასევე, მსხვილი საწარმოების, სამთავრობო და საგანმანათლებლო ინტრანეტის განვითარებას. დევიდი 7 წლის მანძილზე იყო აკადემიური და სამეცნიერო-კვლევითი ქსელის ტრანს-ევროპული საბჭოს (TERENA) წევრი (1991 – 1998);
- ***Supersonic Car (ThrustSSC)*** – მუშაობდა Richard Noble OBE-სა და Mach One Club-ში პირველი მულტი-მედია და ე-კომერციული ვებ-საიტის შექმნისა და მართვის მიზნით მსოფლიოს პირველი Supersonic Car – ThrustSSC – მსოფლიო სიჩქარის რეკორდის დასამყარებლად – 1995 წლის თებერვალი – 1997 წლის ოქტომბერი;
- ***Secure Wireless Networking –*** Madge Networks-ის ბიზნეს-დირექტორი და ვიცე პრეზიდენტი. მან გამოუშვა უსადენო Wi-Fi IEEE802.11a/b/g ინოვაციური და უსაფრთხო ქსელური პროდუქტების სრულყოფილი პაკეტი გაერთიანებული სამეფოსა და ტაივანის მოწინავე ტექნოლოგიურ პარტნიორებთან ერთად;

- ***Networked Enterprise Security –*** დაინიშნა ახალი პროდუქტების დირექტორად (CTO) Blick Group-ის მენეჯმენტის ჯგუფში. მის პასუხისმგებლობაში შედიოდა უსაფრთხოებისა და პროგრამული უზრუნველყოფის 55 ინჟინრისა და პროფესიონალის და უსაფრთხოების მაღალტექნოლოგიური პროდუქტების დივერსიფიცირებული პორტფელის მართვა;
- ***საქართველოს რესპუბლიკა–*** უფროსი მრჩეველი უსაფრთხოების საკითხებში – დაინიშნა ევროგაერთიანების მიერ საქართველოს პარლამენტთან დაკავშირებული ***IT*** უსაფრთხოების, ფიზიკური უსაფრთხოებისა და ბიზნესის უწყვეტობის გეგმებისა და ავარიულ სიტუაციაში აღდგენის ყოველგვარი ასპექტის შესასწავლად და რეკომენდაციების გასაცემად;
- *დრ. დევიდ პრობერტი არის სამეფო სტატისტიკის საზოგადოების წევრი. მას მიღებული აქვს I კლასის ხარისხი მათემატიკაში (ბრისტოლის უნივერსიტეტი) და PhD ხარისხი კემბრიჯის უნივერსიტეტიდან - თვით-ორგანიზებადი სისტემები (სტოქასტური ავტომატების ევოლუცია).*