შოთა რუსთაველის
საქართველოს ეროვნული
სამეცნიერო ფონდი

დავით აღმაშენებლის სახელობის
საქართველოს ეროვნული
თავდაცვის აკადემია

მოხსენებათა კრებული

„კიბერუსაფრთხოების ახალი გამოწვევები გლობალურ საინფორმაციო სივრცეში“

სეზონური სკოლა

2019 წელი

სარჩევი

დავით გულუა - ასოცირებული პროფესორი.
დავით აღმაშენებლის სახელობის ეროვნული თავდაცვის აკადემია

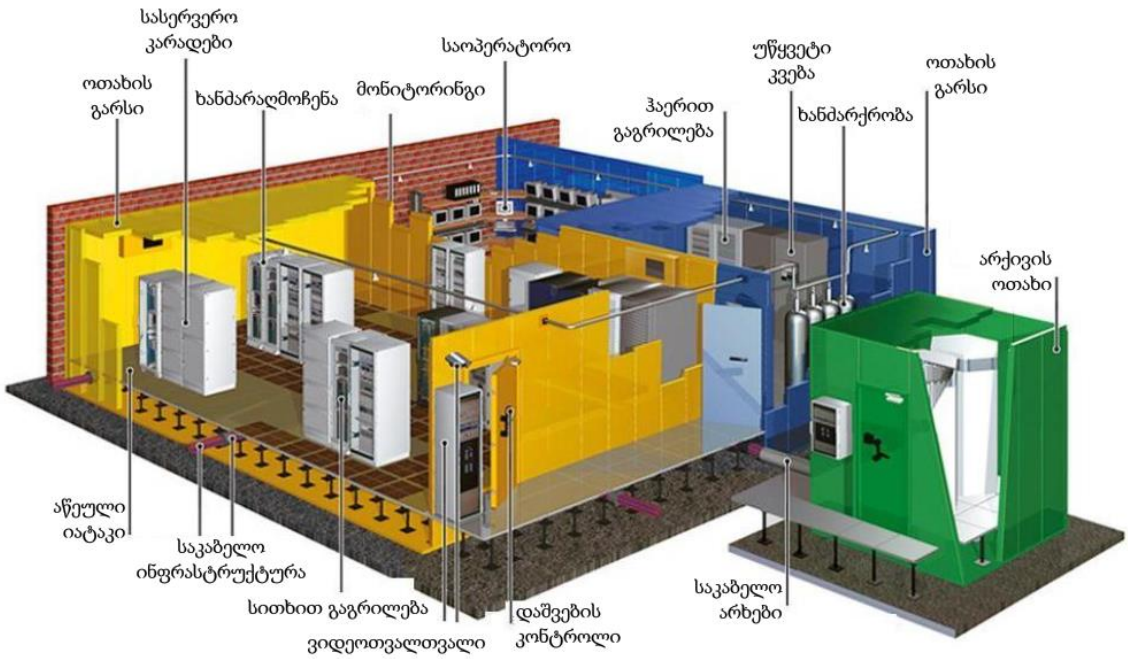
კრიტიკული ინფორმაციული ინფრასტრუქტურის უსაფრთხოება. მონაცემთა ცენტრების აღჭურვა და მართვა

მონაცემთა ცენტრი თანამედროვე ინფორმაციული სისტემების მთავარ სამუშაო პლატფორმას წარმოადგენს. ბიზნეს-კრიტიკული ინფორმაციის მოცულობის სწრაფი ზრდისა და მისი საიმედო შენახვა-დამუშავების აუცილებლობიდან გამომდინარე, თანამედროვე მონაცემთა ცენტრებს უაღრესად მაღალი დონის მოთხოვნები წაეყენებათ, რომელთა შორის უმთავრესებს ინფორმაციასთან შეუფერხებელი წვდომა, მისი დამუშავების მაღალი ეფექტურობა და შენახვის პრაქტიკულად 100%-პროცენტიანი საიმედობა წარმოადგენენ.

თანამედროვე მონაცემთა ცენტრები ორი მიმართულებით ვითარდება. ძველი, ტრადიციული ამოცანებისთვის (დიდი მოცულობის გამოთვლების შესრულება სამეცნიერო და ტექნოლოგიური ამოცანებისთვის) უმჯობესდება ძველი და იქმნება ახალი დატა-ცენტრები. თითოეული მათგანი ერთი დიდი, ე.წ. სუპერკომპიუტერის მომსახურებაზეა გათვლილი და მაღალი წარმადობით გამოირჩევა[1]. ამგვარი დატა-ცენტრების არქიტექტურას (ფიზიკური, საინჟინრო და აპარატული კომპონენტების განლაგება და მათ შორის კომუნიკაცია) საკუთარი სპეციფიკა გააჩნია, რომლის განხილვაც ჩვენი ნაშრომის ფარგლებში არ შედის. აღვნიშნოთ მხოლოდ, რომ კონკურენცია წარმადობის რეკორდების დასამყარებლად წლიდან წლამდე მძაფრდება და სადღეისოდ (2016 წლის ივნისის მონაცემებით) 100 პეტაფლოპსიანი თამასის დაძლევამდე დიდი დრო აღარ რჩება. პირველ სურათზე ნაჩვენებია დატა-ცენტრი, რომელიც ემსახურება Mare Nostrum-სუპერკომიუტერს. იგი განთავსებულია ბარსელონაში, ყოფილი კათოლიკური ტაძრის ფარგლებში და რწმენის და ცოდნის სიმბოლურ ერთიანობას განასახიერებს.

სურათზე მოცემულია სტანდარტული მონაცემთა ცენტრის ფიზიკური სქემა.

[1] https://www.top500.org/ - სუპერკომპიურების რეიტინგ-ლისტი

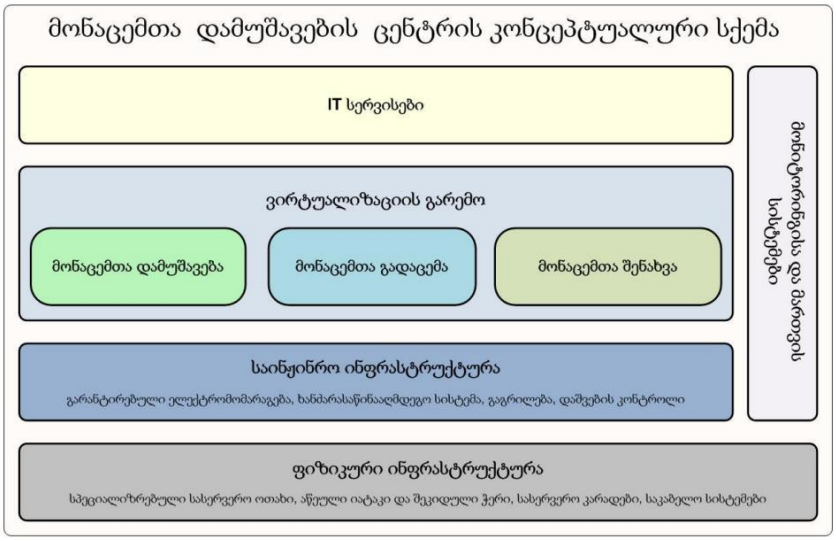


მონაცემთა ცენტრის ფიზიკური სქემა

როგორც სურათიდან ჩანს, მონაცემთა ცენტრის შემადგენლობაში, გარდა ძირითადი დარბაზებისა, შედის არქივის ოთახიც, სადაც გრძელვადიანი არქივები ინახება. დამატებით, როგორც წესი, მცირე ფართზე აწყობენ საოპერატოროს, საიდანაც ადმინისტრატორებს მონიტორინგის საშუალებათა ფართო ნაკრების გამოყენება შეუძლიათ. ზოგადად, მონაცემთა ცენტრის ეფექტური არქიტექტურა უშუალოდ სერვერთა დარბაზში IT-პერსონალის მხოლოდ მინიმალური დროით, აპარატურის მოდიფიცირების დროს ყოფნას გულისხმობს.

ახლა განვიხილოთ თანამედროვე მონაცემთა ცენტრის ფუნქციონალური არქიტექტურა, რომელიც ხუთი ძირითადი ინფრასტრუქტურული კომპონენტის ერთობლიობას წარმოადგენს. ესენია:

- ფიზიკური ინფრასტრუქტურა;
- საინჟინრო ინფრასტრუქტურა
- მონაცემთა გადაცემის ინფრასტრუქტურა;
- მონაცემთა შენახვის ინფრასტრუქტურა;
- მონაცემთა დამუშავების ინფრასტრუქტურა.



მონაცემთა ცენტრის ფუნქციონალური არქიტექტურა

მონაცემთა ცენტრის აგების პროცესი (მოცემული სქემის მიხედვით) ხორციელდება ქვევიდან ზევით. მუშაობის მონიტორინგის წარმოება შესაძლებელია ყველა დონეზე, გარდა ფიზიკურისა. ტერმინი „ვირტუალიზაციის გარემო“ ხაზს უსვამს იმ გარემოებას, რომ თანამედროვე მონაცემთა ცენტრების აპარატული უზრუნველყოფა მეტწილად ვირტუალიზებულია, თუმც ფიზიკურ სერვერებზე და მონაცემთა საცავებზე მომუშავე ინფორმაციული სისტემებიც საკმაოდ ბევრია შემორჩენილი.

მომდევნო თავებში ჩამოთვლილი კომპონენტების დეტალურ ანალიზს შევასრულებთ.

მონაცემთა ცენტრის ფიზიკური ინფრასტრუქტურა

ფიზიკურ ინფრასტრუქტურაში იგულისხმება სასერვერო ოთახი, აწეული იატაკი (ფალშპოლი), შეკიდული ჭერი, სასერვერო კარადები, კაბელური სისტემა. თითოეული ამ კომპონენტის დანიშნულებას მონაცემთა ცენტრის აპარატურის მოხერხებულად განთავსების უზრუნველყოფა წარმოადგენს, რომ ნებისმიერი ცვლილების განხორციელება, რომელიც ინფრასტრუქტურის, სისტემის თუ ქსელის ადმინისტრატორთა მიერ დაიგეგმება, სწრაფად და უპრობლემოდ განხორციელდეს.

სასერვერო ოთახი (დარბაზი), როგორც წესი, გარეშე პირთაგან მოშორებულ, კარგად დაცულ ადგილას ეწყობა. სასურველია მისი გამართვა მრავალსართულიანი შენობის მე-2 ან მე-3 სართულზე, რათა, ერთი მხრივ, საჭიროებისას მისი ევაკუაცია შედარებით ადვილად განხორციელდეს, ხოლო

მეორე მხრივ - წყალდიდობის შემთხვევაში დატბორვის რისკი მინიმალური იყოს. მწირი დაფინანსების არსებობისას მონაცემთა ცენტრებს ჩვეულებრივი ოთახების (დარბაზების) გადაკეთების ხარჯზე აწყობენ, თუმცა ხანძარმედეგობის, წყალგაუმტარობის, ვანდალიზმისა და აფეთქების წინააღმდეგ მდგრადობის, ელექტრომაგნიტური და რადიაციული დაცვის უზრუნველსაყოფად სპეციალური გადაწყვეტები („სოლიუშენები“) არსებობს უსაფრთხოების სხვადასხვა დონეებით, საბაზისოდან მაქსიმალურამდე.

მონაცემთა ცენტრის საინჟინრო ინფრასტრუქტურა

უმთავრეს ინფრასტრუქტურულ კომპონენტს, რომელიც მონაცემთა ცენტრის საიმედო მუშობას განაპირობებს, საინჟინრო ინფრასტრუქტურა წარმოადგენს. იგი შემდეგი კომპონენტებისგან შედგება:

- გაგრილების და ვენტილაციის სისტემა;
- უწყვეტი ელექტრომომარაგების სისტემა;
- ხანძარსაწინააღმდეგო სისტემა;
- ცენტრში დაშვების კონტროლი;
- სტრუქტურირებული საკაბელო სისტემა.

თითოეული ჩამოთვლილი კომპონენტისთვის შეიძლება შედგეს კომბინაცია „ფასი/საიმედობა“, რის შემდეგაც მათი კომბინირებით განისაზღვრება საინჟინრო ინფრასტრუქტურის 4 დონე, საიმედობის განსხვავებული მაჩვენებლებით:

- პირველი დონე (Tier 1) საბაზო დონეს წარმოადგენს და გაგრილებისა და ელექტრომომარაგების სისტემების დუბლირებას არ ითვალისწინებს. ბუნებრივია, ნებისმიერი კომპონენტის ავარიული ან გეგმიური გათიშვა მთლიანი დატა-ცენტრის გაჩერებას გამოიწვევს.
- მეორე დონეზე (Tier 2) ელექტრომომარაგების და გაგრილების სისტემების დუბლირება ხორციელდება. ამ დონის დატა-ცენტრს გააჩნია დიზელ-გენერატორი, თუმცა დენით მომარაგება და გაგრილება ერთადერთი მაგისტრალით ხორციელდება, რაც დატა-ცენტრის გაჩერების გარკვეულ ალბათობას მაინც ტოვებს. სტატისტიკური მონაცემებით, მეორე დონის დატა-ცენტრის უქმობის დრო წელიწადში საშუალოდ 22 საათს შეადგენს.
- მესამე დონის (Tier 3) მონაცემთა ცენტრში ყველაფერი დუბლირებულია, მათ შორის ელექტრომომარაგების და გაგრილების მაგისტრალური ხაზებიც, ამიტომ ასეთი ცენტრი წელიწადში საშუალოდ სულ 2 საათით თუ შეიძლება გაითიშოს.
- მეოთხე დონის (Tier 4), ყველაზე მაღალმდგრად მონაცემთა ცენტრებში გაგრილების და ელექტროკვების მინიმუმ 2 აქტიური მაგისტრალი მუშაობს.

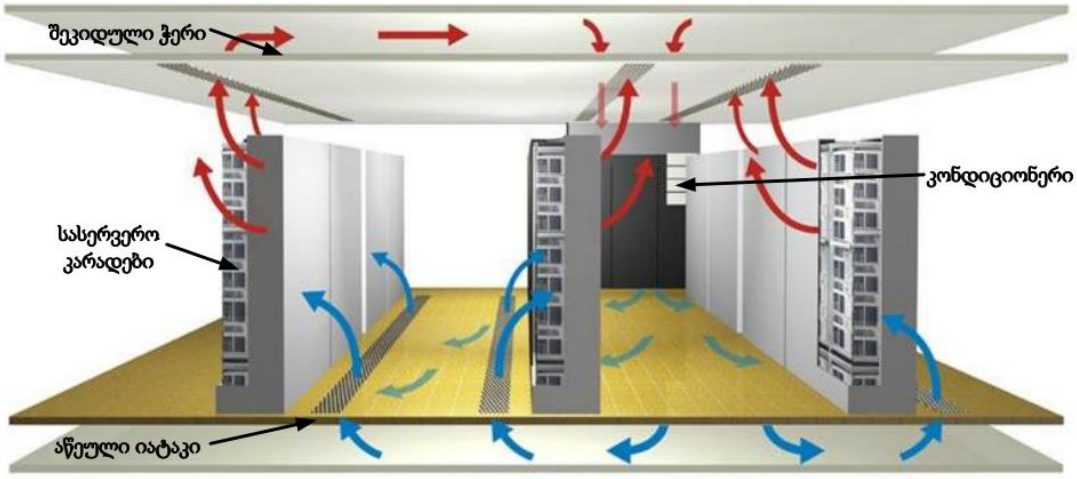
ამგვარი ცენტრის გაჩერების ალბათობა უკიდურესად მცირეა და წელიწადში საშუალოდ 25 წუთს შეადგენს.

გაგრილების სისტემა Emerson - მონაცემთა ცენტრის უწყვეტი მუშაობის ერთერთი გარანტი

მონაცემთა ცენტრების საიმედო მოქმედების ერთერთ წინაპირობას ავარიებისა და კატასტროფებისადმი მდგრადობა წარმოადგენს. მიწისძვრა, წყალდიდობა, ხანძარი, ტერაქტი და სხვა გარე ფაქტორები ვერ უნდა ახერხებდნენ ინფორმაციული პროცესების შეფერხებას ან გაჩერებას. ამ მიზნის მისაღწევად ის ორგანიზაციები, რომელთაც შესაბამისი ფინანსები გააჩნიათ, ფიზიკურად დაშორებულ, სარეზერვო მონაცემთა ცენტრებს (Backup Data Center) აგებენ. ამ დროს ორი ან მეტი ფიზიკური დატა-ცენტრი ერთ ლოგიკურ დატა-ცენტრად არის ქცეული და ერთერთის მწყობრიდან სრული გამოსვლაც კი ინფორმაციული სისტემების მუშაობაზე გავლენას ვერ ახდენს.

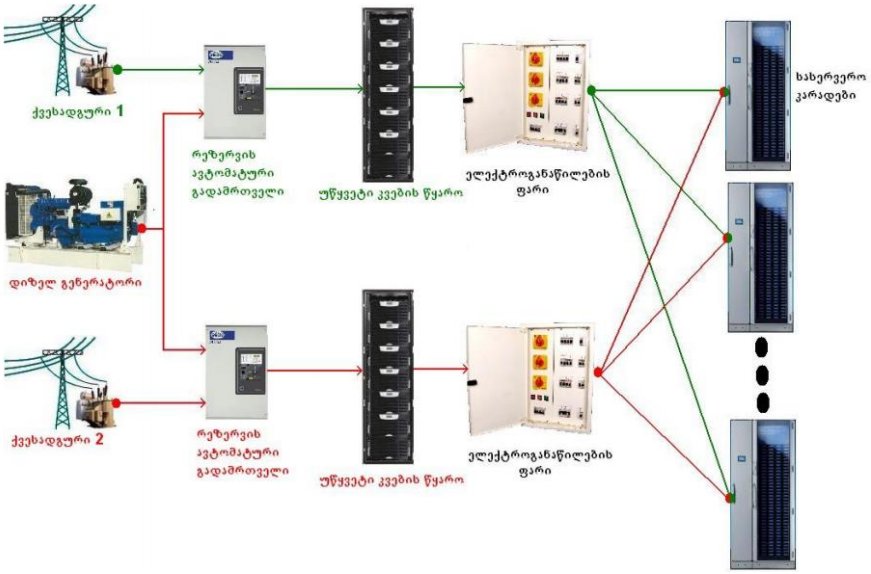
შევეხოთ გაგრილების სისტემებს, რომლებიც სასერვერო დარბაზში ტემპერატურის, ტენიანობის და მტვრის კონცენტრაციის რეგულირებაზე აგებენ პასუხს. მონაცემთა ცენტრების უმრავლესობა დარბაზის გასაგრილებლად ჰაერის კონდიცირების მეთოდს იყენებს. ნაკლებად კრიტიკულ დატა-ცენტრებში ჩვეულებრივი საყოფაცხოვრებო კონდიციონერებიც კი შეინიშნება, თუმცა იქ, სადაც მეტი საიმედობაა მოთხოვნილი, სპეციალური აპარატურა გამოიყენება.

ჰაერით გაგრილება შემდეგი სქემით მუშაობს: ეწყობა ცივი და ცხელი ჰაერის სამოძრაო კორიდორები. ცივი ჰაერი აწეული იატაკის ქვემოთ მოძრაობს და სავენტილაციო არხების გავლით მიეწოდება სასერვერო კარადებს, საიდანაც 6-8 კილოვატი სითბო „გამოაქვს“ (თითოეული კარადიდან). გაცხელებული ჰაერი შეკიდულ ჭერში დამონტაჟებული გამწოვების გავლით ისევ კონდიციონერს მიეწოდება გასაგრილებლად.



ჰაერით გაგრილების სქემა მონაცემთა ცენტრში

დიდი ოდენობით სერვერული აპარატურის გამოყენებისას ჰაერით გაგრილება დასმულ ამოცანებს ვერ პასუხობს, რადგან აპარატურით სრულად დაკომპლექტებული სერვერთა კარადა ხშირად 20 კილოვატამდე სითბოს გამოყოფს. ასეთ დროს წყლით გაგრილების ბევრად უფრო ეფექტურ მეთოდს იყენებენ, რომელსაც 40 კილოვატამდე სითბოს გამოტანა შეუძლია.



უწყვეტი ელექტრომომარაგების სქემის ნიმუში

უწყვეტი ელექტრომომარაგების გარეშე ვერცერთი მონაცემთა ცენტრი ვერ იმუშავებს. ამ ამოცანას დატა-ცენტრში ორი მოწყობილობა ემსახურება: დიზელ-გენერატორი და უწყვეტი ელექტროკვების წყარო (UPS). პირველის დანიშნულებას ქალაქის ელექტროკვების გათიშვისას სასერვერო დარბაზის აპარატურისა და

გაგრილების სისტემების ელექტროკვებით უზრუნველყოფა წარმოადგენს, ხოლო მეორე ვალდებულია „დაიჭიროს“ ელექტრომომარაგება ქალაქსა და დიზელ-გენერატორს შორის ავტომატური გადართვის რამდენიმეწამიან მონაკვეთში, აგრეთვე იზრუნოს ელექტროპარამეტრების მუდმივობაზე და ძაბვის ვარდნების კონტროლზე.

დიდ დროს ვერ დავუთმობთ ხანძარსაწინააღმდეგო და ქრობის ელექტრონულ სისტემებს, რადგან მათი მუშაობა მონაცემთა ცენტრში, ჩვეულებრივი საოფისე ოთახების ანალოგიურია.

მონაცემთა დამუშავების, შენახვის და გადაცემის ინფრასტრუქტურა

მონაცემთა საიმედო დამუშავება, შენახვა, გადაცემა და დაცვა მონაცემთა ცენტრის მთავარ მისიას წარმოადგენს. პირველ ამოცანას სერვერები ემსახურებიან, მეორეს - მონაცემთა საცავები, მესამეს - ქსელური აპარატურა, ხოლო მეოთხეს - სპეციალიზებული აპარატული უზრუნველყოფა.

სერვერთა არჩევანი მრავალფეროვანია. დასამუშავებელი ამოცანების მიხედვით ორგანიზაციას შეიძლება დასჭირდეს როგორც მინიმალური კონფიგურაციის, ასევე მაღალი სიმძლავრის სერვერების შეძენა და გამართვა. გასაცემია პასუხიც კითხვაზე: რას უნდა უზრუნველყოფდეს სერვერი, ინფორმაციის დამუშავების მაღალ სიჩქარეს, თუ ინფორმაციულ ნაკადებთან პარალელური მიმართვის ოპერაციათა დიდ რაოდენობას?

სანამ უშუალოდ სერვერებს შევეხებოდეთ, აღვნიშნოთ, რომ ყველა გამოთვლით სისტემას (კომპიუტერს) სამ ძირითად კლასად ყოფენ:

- დიდი ეგმ-ები ანუ მეინფრეიმები (Mainframes) - მაგ. IBM z series
- მინიკომპიუტერები (MidRange systems) - მაგ. DEC VAX, HP AlphaServer, Oracle SUN SPARC, IBM Power Systems
- მიკროკომპიუტერები (x86-Systems) – თანამედროვე სერვერული და პერსონალური გამოთვლითი სისტემების უმრავლესობა.

მეინფრეიმები გამოთვლითი ტექნიკის ისტორიის გარიჟრაჟზე, გასული საუკუნის 50-იან წლებში ეგმ-ის ერთადერთ სახეობას წარმოადგენდა, რომელსაც 60-იანი წლებიდან მინიკომპიუტერები, ხოლო 80-იანებიდან მიკროკომპიუტერები შეემატა. 90-იანი წლებისთვის პირველი ორი კლასის კომპიუტერებს მესამის ხარჯზე გადაშენებას უწინასწარმეტყველებდნენ, თუმცა მათ (განსაკუთრებით კომპანია IBM-ის მეინფრეიმებმა) მოახერხეს ბაზარზე დარჩენა და დღესაც მცირე, მაგრამ სტაბილურ სეგმენტზე მუშაობენ. სხვა მხრივ კი, მონაცემთა ცენტრების სერვერთა აბსოლუტური უმრავლესობა მიკროკომპიუტერულ, ე.წ. x86-არქიტექტურის ბაზაზე მუშაობს.

მაღალმწარმოებლურ, ე.წ. High-end-სერვერებს რამდენიმე ცნობილი კომპანია (IBM, HP, DELL და სხვები) უშვებს. მათი შეძენის აუცილებლობა მხოლოდ დიდ სახელმწიფო (სამინისტროები, საწარმოები) და კერძო (ბანკები, მსხვილი კორპორაციები) დაწესებულებებს გააჩნიათ. მსგავსი მოწყობილობები (იხილეთ სურათები 7,8,9) დიდი მოცულობის რესურსებს (პროცესორები, ოპერატიული მეხსიერება, ქსელური გამტარობა) შეიცავენ, რაც მათ ფასზეც აისახება.

7. HP SuperDome (Power-at-once) – უწყვეტი წარმოების სერვერი

8. DELL PowerEdge R920 High-end Server

9. IBM x3850 X5 High-end Server

შედარებით ხელმისაწვდომ მოწყობილობებს საშუალო და მცირე სერვერები წარმადგენენ, რომლებიც High-end-სერვერთა მსგავსად საკარადე (Rack-mountable) ან დასადგამი (Standalone) ფორმ-ფაქტორებით გამოდიან ბაზარზე.

საიმედობის თვალსაზრისით სერვერულ კომპიუტერულ ინფრასტრუქტურაში განსაკუთრებულ ყურადღებას იქცევს ე.წ. Blade-სისტემები (Half-Blade, Full-Blade). ისინი რომლებიც შედგება რამდენიმე პატარა სერვერისა (Blade Server ითარგმნება, როგორც სამართებლის სიგანის სერვერი) და მათი კონტეინერისგან (Enclosure), რომელიც ელექტროკვების, ქსელის ინტერფეისებისა და კონდიცირების სისტემებს ცენტრალიზებულად განაგებს. საჭიროების შემთხვევაში შესაძლებელია სერვერების „ცხლად“ ჩანაცვლება, მთლიანი ენქლოჟერის გათიშვის გარეშე.

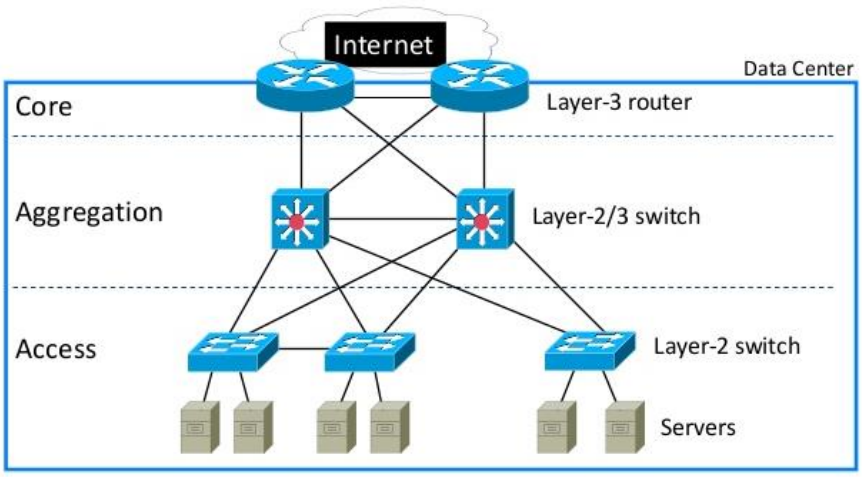
მონაცემთა საცავი (Data Storage) ინფორმაციის შენახვის საშუალებას წარმოადგენს და სერვერული სისტემებისგან დამოუკიდებლად აიგება. ყველაზე დიდი მოცულობის და კრიტიკული მონაცემების შესანახად Storage Area Network, იგივე SAN-ტექნოლოგიას იყენებენ, რომელიც ხისტი ან SSD-დისკებით

დაკომპლექტებულ მონაცემთა საცავებსა და სერვერებს ერთმანეთთან აკავშირებს, როგორც წესი, ოპტიკურბოჭკოვანი კავშირის არხების (Fibre Channel) გამოყენებით.

ნაკლებ ინტენსიურად გამოსაყენებელი ინფორმაციის (სარეზერვო ასლები, არქივები) შედარებით იაფ მოწყობილობებს იყენებენ. მათგან ყველაზე ეფექტურია ქსელური მონაცემთა საცავი (NAS – Network Area Storage). ფართოდ გამოიყენება აგრეთვე არაქსელური გარე ხისტი მეხსიერება (DAS - Direct Attached Storage) და იაფი ლენტურ-კასეტური მასივები (Tape Storage) გრძელვადიანი არქივების შესანახად.

მონაცემთა ცენტრის ქსელური ინფრასტრუქტურა ორი ძირითადი ტიპის მოწყობილობებისგან შედგება: ქსელის კვანძებისა და საკომუნიკაციო კომპონენტებისგან. პირველს ვაკუთვნებთ მარშრუტიზატორებს (Router) და კომუტატორებს (Switch), ხოლო მეორეს - მეტალის (სპილენძის) და ოპტიკურ კაბელურ სისტემებს.

ქსელის აწყობა მონაცემთა ცენტრში ერთერთ ყველაზე საპასუხისმგებლო და შრომატევად საქმეს წარმოადგენს. საკმარისია გავიხსენოთ, რომ სწორედ მონაცემთა ცენტრებს აწვებათ ინტენსიური ქსელური ტრაფიკის ნაკადები და იმ მოწყობილობათა ჩამონათვალი, რომელთაც ამ ნაკადების სწრაფად და უდანაკარგოდ ტრანსპორტირება ევალებათ, საკმაოდ დიდია. შევეხოთ კომუტატორების (სვიჩების) იერარქიული სისტემას, რომლის ყველაზე დაბალ საფეხურზე ე.წ. „წვდომის“ (სართულის) სვიჩებს (Access switch) ვხედავთ. სართულის სვიჩი, როგორც წესი, ერთ ან მეტ შიდა ქვექსელს ემსახურება და უშუალოდ მონაცემთა ცენტრში ე.წ. გამანაწილებელ სვიჩთან (Distribution switch) მიდის ყველა სხვა „კოლეგის“ მსგავსად. და ბოლოს, გამანაწილებელი სვიჩი ერთი მხრივ და სერვერებთან კავშირის სვიჩები (Server Access Switch, Top-of-Rack-Switch) მეორე მხრივ გადაიკვეთებიან მონაცემთა ცენტრის მთავარი, ყველაზე ძვირადღირებული კომუტატორ(ებ)ის (Core switch) ფარგლებში, სადაც ინფორმაციული ტრაფიკის ყველაზე მაღალ დონეზე გადამისამართება ხორციელდება.



მონაცემთა ცენტრის ქსელის ზოგადი არქიტექტურა

მოკლედ შევეხოთ სპეციალიზებულ მოწყობილობებსაც, რომელთა დანიშნულებას სპამთან ბრძოლა, ბრანდმაუერის (Firewall) ფუნქციების შესრულება, ვებ-გვერდების და აპლიკაციების ფილტრაცია, ორგანიზაციის ქსელში უკანონო შემოღწევათა დაფიქსირება და პრევენცია (IDS/IPS), ანტივირუსული დაცვა და სხვა მრავალი მნიშვნელოვანი ფუნქცია წარმოადგენს. სადღეისოდ აღწერილ ამოცანებს ხშირად ერთი მოწყობილობა (UTM – Unified Threat Management, იგივე Next-generation Firewall) ასრულებს, რომელიც, ცხადია, საკმაოდ ძვირი ჯდება და მონაცემთა ცენტრში ერთერთ ყველაზე „საპატიო“ ადგილას, ქსელის პერიმეტრზე თავსდება. NG Firewall-ებს აწარმოებენ ფირმები CheckPoint, FortiGate, Barracuda, Sophos და სხვები.

მონაცემთა მართვის საიმედობის უზრუნველყოფა

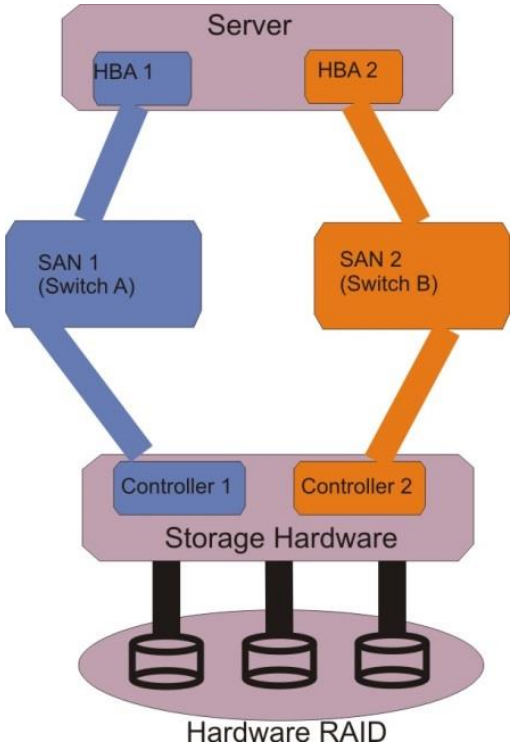
ინფორმაციული პროცესების წარმოება წარმოუდგენელია სარგებლიანობისა და საიმედობის მაღალი დონის გარეშე. სადღეისოდ ბიზნეს-პროცესები იმდენად მჭიდროდ დაუკავშირდა ელექტრონულ-გამოთვლით სისტემებს, რომ საქმიანობის „ქაღალდზე“ წარმოება შეგვიძლია ისტორიას ჩავაბაროთ. შესაბამისად, ინფორმაციული ინფრასტრუქტურის ნებისმიერი შეფერხება თუ გაჩერება შეიძლება სერიოზულ პრობლემად ან სულაც კატასტროფად იქცეს ორგანიზაციისთვის.

წინა ქვეთავებში აღწერილი თითოეული მოწყობილობა თუ კავშირის საშუალება კარგად გამართული მონაცემთა ცენტრის ფარგლებში აუცილებლად მადუბლირებელ ანუ რედუნდანტულ კომპონენტებს უნდა შეიცავდეს. ეს წესი ეხება როგორც საინჟინრო მოწყობილობებს (რაზეც პირველ თავში უკვე ვისაუბრეთ), ასევე სერვერებს, მონაცემთა საცავებს, ქსელურ და სპეციალიზებულ აპარატურას. ქვემოთ რამდენიმე მაგალითს განვიხილავთ.

სერვერებსა და მონაცემთა საცავებს შორის რედუნტანტული კავშირების უზრუნველსაყოფად შემდეგი ღონისძიებები ტარდება:

- ყოველი სერვერი და მონაცემთა საცავი ოპტიკური კავშირის მინიმუმ ორი ადაპტერით (HBA - Host Bus Adapter) აღიჭურვება
- სერვერებსა და მონაცემთა საცავებს შორის განთავსდება მინიმუმ ორი ოპტიკური კომუტატორი (SAN-Switch)
- ყოველი სერვერი და მონაცემთა საცავი ერთმანეთს მინიმუმ ორი ოპტიკური კომუტატორის გავლით უკავშირდება.

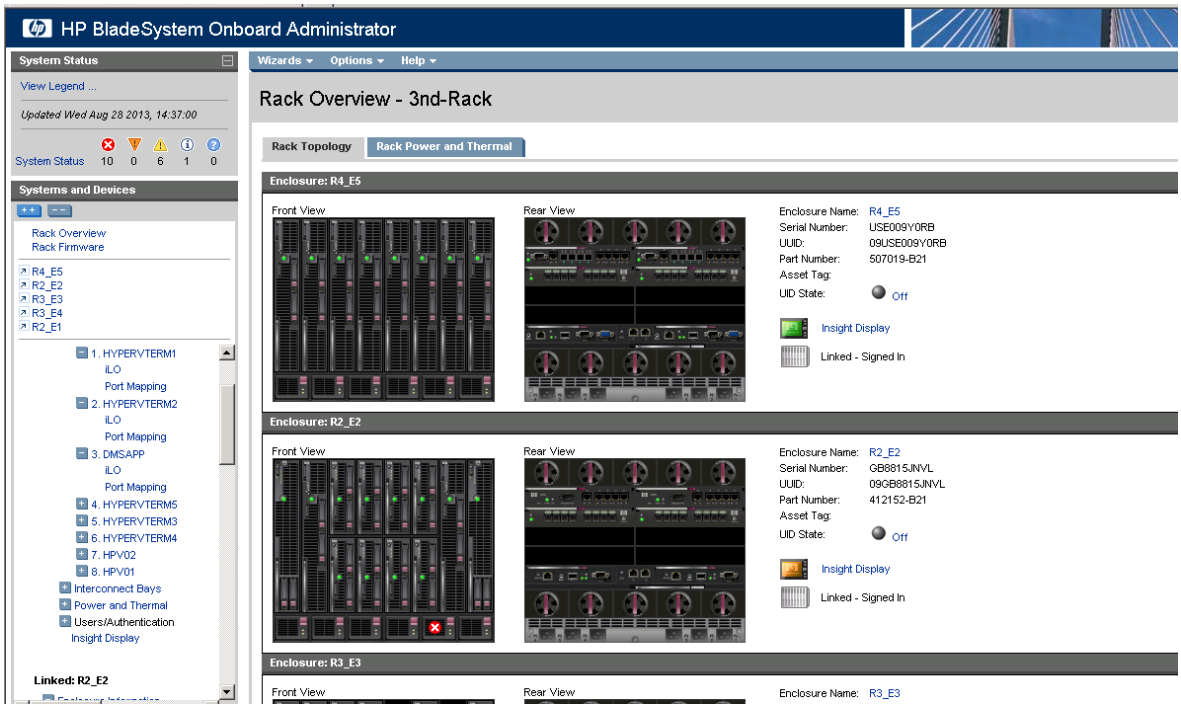
თითოეულ მოწყობილობაზე სხვადასხვა ტიპის კავშირის ინტერფეისები არსებობს (FC, iSCSI, Management, LAN), რომლებიც მრავალფეროვანი კომუნიკაციის აწყობის საშუალებას იძლევიან. საიმედო კავშირის სქემატური ნიმუში მოცემულია სურათზე.



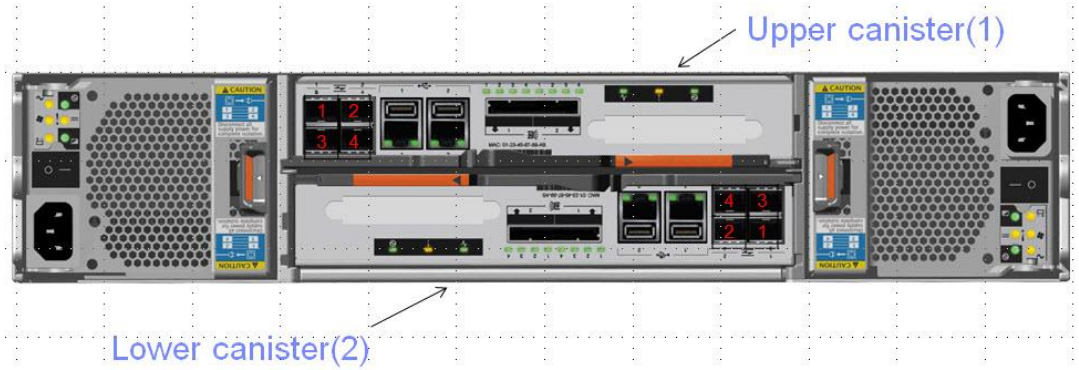
რედუნდატული კავშირები სერვერებსა და მონაცემთა საცავებს შორის

პრაქტიკულ მაგალითად გამოგვადგება კომპანია HP-ს ბლეიდ-სერვერთა და მონაცემთა საცავების მართვის სისტემა. იგი კლიენტ-სერვერის პრინციპით მუშაობს, სადაც კლიენტებს აღნიშნული კომპანიის ბლეიდ-სერვერები, მონაცემთა საცავები, SAN-სვიჩები და ჩვეულებრივი ქსელური კომუტატორები წარმოადგენენ, რომელთაც მართვის სპეციალურ აპარატულ მოდულებს (iLO – Integrated Light-out) უდგამენ. iLO-მოდულებს ცალკე, ქსელური, ე.წ. მენეჯმეტ-ადაპტერები ემსახურება, რომელთა საშუალებითაც შესაძლებელია მოწყობილობათა დაშორებული მართვა მაშინაც კი, როცა ისინი გამორთულია.

მენეჯმენტ-სერვერის როლს ზემოთ აღწერილ სქემაზე სპეციალური პროგრამა On-board Administrator თამაშობს, რომელთანაც თავს იყრის ყველა iLO-მოდული და მათი ცენტრალიზებული მართვა ხორციელდება. ანალოგიური აპარატული უზრუნველყოფა გააჩნია სხვა მწარმოებელთა მოწყობილობებსაც. მაგალითად, DELL-ფირმის სერვერებსა და მონაცემთა საცავებზე iDRAC-მოდულები გამოიყენება, ხოლო კომპანია IBM-ის კვანძებზე ინტეგრირებულ მოდულებს კვანძის კანისტრები (Node Canister) ეწოდებათ.



on-Board Administrator-ის ინტერფეისი



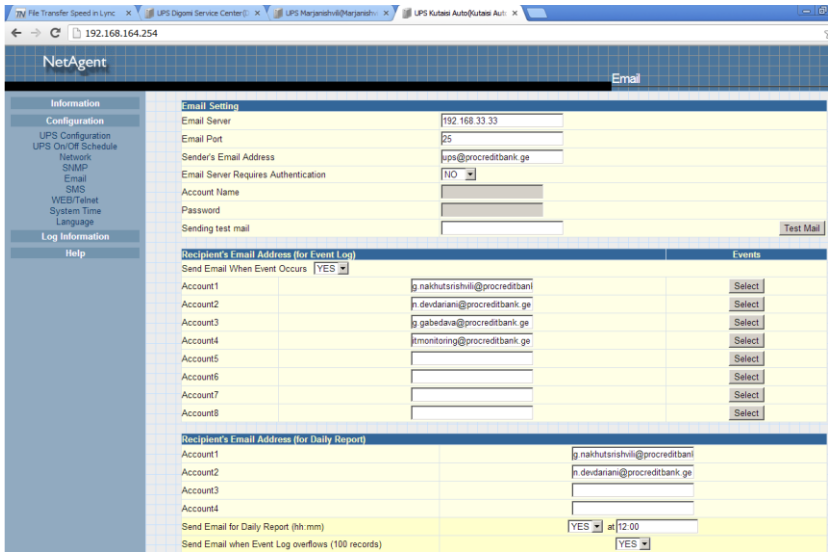
მონაცემთა საცავი IBM Storwize v7000 - Node Canister

კანისტრა მრავალფეროვანი კავშირის ინტერფეისებს შეიცავს (FC - ოპტიკური, LAN - ქსელური, SAS - დისკური და USB). როგორც სურათიდან ჩანს, ყოველ მოწყობილობაზე მინიმუმ ორი ამგვარი მოდულის ინტეგრირება შეიძლება, რაც კავშირის საიმედობას ამაღლებს (დისკური კლასტერის სახით).

ორგანიზაციის IT-ინფრასტრუქტურის სარგებლიანობის და საიმედობის უზრუნველყოფის აპარატული და პროგრამული საშუალებები

საინჟინრო ინფრასტრუქტურის სამართავად სადღეისოდ მდიდარი აპარატული და პროგრამული საშუალებების ნაკრები არსებობს. პროგრამული, ხშირ შემთხვევაში ვებ-ბაზირებული ინსტრუმენტების საშუალებით ადმინისტრატორებს შეუძლიათ დააკვირდნენ და გააკონტროლონ მონაცემთა ცენტრის დარბაზში ტენიანობის, ტემპერატურის და მტვრიანობის პარამეტრები. მოქმედებს შეტყობინებების (ნოტიფიკაციების) სერვისები, როცა ცნობები ნორმიდან გადახვევის შესახებ ადმინისტრატორს სატელეფონო ზარის, ელექტრონული წერილის ან ყველაზე ხშირად მოკლე ტექსტური შეტყობინების ფორმით მიუვა.

იგივეს თქმა შეიძლება დიზელ-გენერატორებისა და უწყვეტი კვების წყაროების შესახებაც. მე-16 სურათზე მოცემულია კომპანია NetAgent-ის UPS-ის მართვის ვებ-ბაზირებული პროგრამის ინტერფეისის ფრაგმენტი.



მონაცემთა ცენტრის UPS-ის მართვის ინტერფეისი

ქსელური მოწყობილობების, სერვერებისა და მონაცემთა საცავების მართვის საკითხებზე საუბრისას უნდა გავითვალისწინოთ, რომ ისინი 24-საათიან რეჟიმში ხელმისაწვდომნი უნდა იყვნენ. ლოკალურად, სერვერთა დარბაზში მართვის ოპერაციათა განხორციელების ყველაზე კომფორტულ ინსტრუმენტს **კარადის**

(რეკის) კონსოლი წარმოადგენს. იგი სერვერულ დარბაზში უზრუნველყოფს ერთ მონიტორის გამოყენებას რამდენიმე სერვერის სამართავად პროგრამული გადართვის მეშვეობით, რისთვისაც სერვერები სპეციალურ **KVM Switch ტიპის კომუტატორს** იყენებენ (მაგალითად 8-პორტიანი MasterView შეიძლება დავასახელოთ). KVM-სვიჩის დეშიფრაცია შემდეგია: Keyboard, Video, Mouse. კომუტატორში **შედის** კაბელთა სამეულები ყოველი კომპიუტერიდან (გრაფიკული ადაპტერის, კლავიატურის და მაუსის პორტები) და გამოდის ერთი სამეული მონიტორის, კლავიატურისა და მაუსისთვის.

ჩვენ განვიხილეთ თანამედროვე მონაცემთა ცენტრების აგებისა და მართვის ამოცანათა ყველაზე მნიშვნელოვანი ნაწილები. მომავალში, „ღრუბლოვანი“ ტექნოლოგიების ინტენსიურ განვითარებასთან ერთად, მონაცემთა ცენტრების მნიშვნელობა კიდევ უფრო გაიზრდება. გაიზრდება მონაცემთა ცენტრების ფარგლებში მომუშავე სერვისების რაოდენობა, წარმოიქმნება ახალი სერვისების დანერგვისა და მათთან შეუფერხებელი წვდომის უზრუნველყოფის ამოცანები. შესაბამისად, მომავალში მონაცემთა ცენტრების აგების და მართვის სფეროში ახალ კონცეპტუალურ და ტექნიკურ სიახლეებს უნდა ველოდოთ.

სერვერული სისტემების დაპროექტება და აგება კორპორაციულ ქსელებში

თანამედროვე ინფორმაციული ტექნოლოგიების განვითარება კომპიუტერული ქსელების წინაშე ახალ ამოცანებს აყენებს. კორპორაციული ინფორმაციის მოცულობისა და ქსელებში ინფორმაციული ნაკადების ზვავისებრი ზრდის გამო ქსელში ინფორმაციის ტრადიციული მეთოდებით შენახვა, დამუშავება და გადატანა დანახარჯების მკვეთრ ზრდას იწვევს, ხოლო მთლიანი ქსელის ფუნქციონირების ეფექტურობა მკვეთრად ეცემა.

გასული საუკუნის ბოლოდან ინფორმაციულ ტექნოლოგიებში კორპორაციული ქსელების დაპროექტების და აგების ახალი მეთოდები მკვიდრდება, რომელთა განვითარების პიკსაც დღევანდელობა წარმოადგენს. უფრო ზუსტად, ახალი მეთოდოლოგია 80-იანი წლების დასაწყისში დროებით „დავიწყებული“ მეინფრეიმულ-სუპერკომპიუტერული არქიტექტურისა და რესურსების ვირტუალიზაციის ტექნოლოგიის ხელახალი აქტუალიზაციის შედეგია. პერსონალური კომპიუტერების განვითარებასთან ერთად თითქოს სუპერკომპიუტერების საჭიროება მოიხსნა, მაგრამ ინფორმატიკის ახალმა რეალობებმა ისინი ხელახლა დააბრუნა ასპარეზზე, ოღონდ მნიშვნელოვნად შეცვლილი სახით.

მოცემული ნაშრომი ეხება თანამედროვე კორპორაციული ქსელების უმნიშვნელოვანეს ნაწილს, სერვერულ ინფრასტრუქტურას, რომელიც ნებისმიერი დიდი ქსელის „გულს“ წარმოადგენს და მის გამართულ მუშაობაში მთავარ როლს თამაშობს. მეორე მხრივ, სწორედ სერვერები შეიცავენ კომპიუტერული ქსელის

ყველაზე ძვირადღირებულ რესურსებს და შესაბამისად, ყოველი სერვერული კომპონენტი თავის ღირებულებას მაქსიმალურად უნდა პასუხობდეს, რაც მათი დატვირთვების ეფექტურ განაწილებას მოითხოვს. მოცემულ ნაშრომში აღნიშნულ საკითხს ასევე მნიშვნელოვანი ადგილი უჭირავს.

ნაშრომის პრაქტიკული ნაწილი რეალური კორპორაციული ქსელის მოდერნიზების პროცესში დასმულ ამოცანებს და მათი გადაწყვეტისთვის გამოყენებულ მეთოდებს ეხება. ნაშრომის ავტორი ამ პროცესის აქტიური მონაწილე იყო. ძირითადი აქცენტები თანამედროვე ინფორმაციული ტექნოლოგიების უმნიშვნელოვანეს მიმართულებებზე: ვირტუალიზაციასა და კლასტერულ არქიტექტურაზე კეთდება. განხილულია მეთოდებიც, რომელთა საშუალებითაც სერვერული სისტემების ძველი არქიტექტურის ახალ ტექნოლოგიებზე მორგება ხდება შესაძლებელი.

თანამედროვე სერვერული სისტემები. კორპორაციული ქსელის სერვერული სისტემის ზოგადი სტრუქტურა

კორპორაციული სერვერული სისტემა ორ ძირითად ქვესისტემად შეიძლება დავყოთ: საკუთრივ სერვერული და გარემოსთან ურთიერთობის ანუ ქსელური ქვესისტემები.

სერვერული სისტემის ქსელური ქვესისტემა მოიცავს მაგისტრალურ და სხვა ტიპის ქსელურ აპარატურას (რუთერები, მე-3 დონის კომუტატორები, კონვერტირების მოწყობილობები და სხვა), რომლებიც ინტერნეტთან მიერთებას და კორპორაციული ქსელის სხვადასხვა სეგმენტების ურთიერთკავშირს უზრუნველყოფენ. სერვერული სისტემა ქსელის მომხმარებელთათვის განკუთვნილი მრავალფეროვანი სერვისების (ფაილ-სერვისი, მონაცემთა ბაზები, ელექტრონული ფოსტა, ვები და სხვა) განთავსებისა და მართვის ამოცანას ემსახურება.

სტანდარტული სერვერული სისტემა თითოეული სერვისისთვის, როგორც წესი, ცალკე ფიზიკური მანქანის ან მანქანების (სერვერების) გამოყოფას ითვალისწინებს. შეზღუდული რესურსების არსებობისას შეიძლება რამდენიმე სერვისი ერთსა და იმავე სერვერზე იყოს განთავსებული. არსებობს საკმაოდ მოქნილი მეთოდები მონაცემთა საიმედო შენახვისა და ინფორმაციასთან უწყვეტი წვდომის უზრუნველსაყოფად, თუმცა მოცემული მიდგომა მაინც საკმაოდ „ხისტია“ და გააჩნია რიგი ნაკლოვანებებისა, რომელთაგან უპირველესად რესურსების უყაირათო ხარჯვა უნდა მივიჩნიოთ. სერვერული სისტემის პირველადი არქიტექტურა მეტნაკლებად ითვალისწინებს ყოველი სერვერის წინაშე მდგარ სარესურსო მოთხოვნებს, თუმცა ორგანიზაციის ინფორმაციული მოთხოვნების გაზრდის კვალდაკვალ სერვერული სისტემების მათზე მორგება საკმაოდ

შრომატევადი საქმეა და მნიშვნელოვან ფინანსურ და შრომით დანახარჯებათანაა დაკავშირებული.

ბოლო წლებში განვითარებული რამდენიმე ტექნოლოგიის (ვირტუალიზაცია, კლასტერული არქიტექტურა, ინფორმაციის მრავალდონური შენახვა) წყალობით აღნიშნულ ამოცანათა მეტი ეფექტურობით გადაჭრა გახდა შესაძლებელი.

ინფორმაციის საიმედო შენახვა სერვერულ სისტემებში. პროგრამულ-აპარატული უზრუნველყოფა

გარე მეხსიერების ის მოწყობილობები, რომლებიც დღევანდელ გამოთვლით სისტემებში გამოიყენება (ხისტი, ნახევარგამტარული, ოპტიკური), თავისთავად წარმოადგენენ ინფორმაციის საიმედო მატარებლებს ფუნქციონირების მრავალწლიანი გარანტიით, თუმცა ცხადია, მათი პირდაპირი გამოყენება განსაკუთრებით სერვერულ სისტემებში მიუღებელია. კრიტიკული ინფორმაციის (საბანკო და სადაზღვევო მონაცემთა ბაზები, სახელმწიფო და კორპორაციული ინფორმაცია) ერთ ეგზემპლარად შენახვა ინფორმაციის დაკარგვის თუნდაც მინიმალური რისკით გაუმართლებელია. სარეზერვო კოპირების და არქივაციის (იხ. ქვემოთ) ინსტრუმენტები შეიძლება ინფორმაციის კარგვისგან თავდაცვის ერთერთ მოხერხებულ მეთოდად მივიჩნიოთ, მათი გამოყენება მაინც არასაკმარისია ინფორმაციის საიმედო შენახვის პრაქტიკულად გარანტირებული უზრუნველყოფისთვის.

კომპიუტერული აპარატურის მწარმოებლები გვთავაზობენ სხვადასხვა საშუალებს ინფორმაციული სიჭარბის (**Redundancy**) მისაღწევად, რომელთაგან ყველაზე პოპულარულია გარე მეხსიერებაში განლაგებული ინფორმაციის დუბლირების მექანიზმები ეგრეთ წოდებული **RAID**-ტექნოლოგიის გამოყენებით, რომელსაც მოკლედ შევეხებით.

RAID გაიშიფრება როგორც Redundant Array of Independent Disks და დისკური მეხსიერებაში განთავსებულ ინფორმაციასთან მიმართვის დაჩქარების ან მისი შენახვის საიმედობის ამაღლების სხვადასხვა ალგორითმებს შეიცავს. სადღეისოდ არსებობს რამდენიმე **RAID**-არქიტექტურა **(RAID0…RAID6)** ან არქიტექტურათა კომბინაცია (მაგ. **RAID1+0**). ქართულ აიტი-სლენგზე ნახსენები ტერმინები შემდეგნაირად გამოითქმის: მე-10 მასივი - RAID10, მე-5 მასივი - RAID5 და ასე შემდეგ.

RAID5-ის არქიტექტურა ეფუძნება მარტივ ოპერატორს „გამომრიცხავი ან“ (**XOR**), რომელიც ბიტების მიმდევრობათა სიმრავლისგან ე.წ. „პარიტეტული ბლოკების“ („ექსტრაბლოკების“) მიღებისა და მათგან შემდგომ ბიტების რომელიმე საწყისი მიმდევრობის აღდგენის საშუალებას იძლევა. ამასთან, სტანდარტული არითმეტიკული ოპერაციებისგან განსხვავებით, აღნიშნული ოპერაცია არ იწვევს

თანრიგების გადავსებას, რაც მისი გამოყენების ეკონომიურობას და მოხერხებულობას განაპირობებს. პარიტეტული ბლოკების ფორმირებისა და საწყისი ინფორმაციის აღდგენის ნიმუში იხილეთ ნახაზზე.

	Drive 1	Drive 2	Drive 3	Drive 4
Stripe 1	0100	0101	0010	0011
Stripe 2	0010	0000	0110	0100
Stripe 3	0011	0001	1010	1000
Stripe 4	0110	0001	1101	1010

პარიტეტული ბლოკები (აღნიშნულია ყვითელი ფერით)

პარიტეტული ბლოკის ფორმირების მაგალითი (პირველი სტრაიპისთვის)

(0100) XOR (0101) XOR (0010) = (0011)

საწყისი ინფორმაციის აღდგენის მაგალითი (დაკარგულად ითვლება პირველი სტრაიპის პირველი ბლოკი)

(0101) XOR (0010) XOR (0011) = (0100)

RAID5-ის მთავარ ღირსებას თანაფარდობის „ინფორმაციის საიმედო შენახვა - სასარგებლო მეხსიერება“ მაღალი კოეფიციენტი წარმოადგენს. მაგალითად, 10-დისკიანი მასივისთვის სასარგებლო მეხსიერება მთლიანი მეხსიერების 90%-ს შეადგენს (ზოგიერთი წინაპირობის შესრულების შემთხვევაში), რაც დისკების „სარკული“ ასახვის 50%-თან შედარებით მაღალი მაჩვენებელია. თანამედროვე მონაცემთა საცავებში უპირატესობა სწორედ **RAID5**-ს ან მის მოდიფიცირებულ ვარიანტს, **RAID6**-ს ენიჭება.

დისკური მასივის მართვის ალგორითმი შემდეგია: მთელი დისკური მასივი რამდენიმე ფიზიკური ხისტი დისკისგან შედგება, რომლის ნაწილები ერთერთი რომელიმე ტექნოლოგიის (მაგალითად, **RAID5**) მეშვეობით ერთ მთლიან ლოგიკურ დისკად ყალიბდება, ხოლო შემდეგ მმართველი პროგრამით შესაძლებელია შექმნილი ლოგიკური დისკის „დაშლა“ დისკური მასივის ლოგიკურ ტომებად (**LUN – Logical Unit Number**).

სწორედ ლოგიკური ტომი წარმოადგენს დისკური მეხსიერების იმ ერთეულს, რომელსაც ფიზიკური თუ ვირტუალური სერვერების ოპერაციული სისტემები ღებულობენ და თავიანთი დისკური სივრცის ნაწილად (ლოკალურ დისკებად) აღიქვამენ. ამგვარად, სერვერს „არ აინტერესებს“, მის განკარგულებაში გადმოსული

ლოგიკური დისკი რეალურად რამდენ ფიზიკურ დისკზეა განთავსებული. იგი მას საკუთარი ფიზიკური დისკივით იყენებს.

მასივის მართვა **RAID**-კონტროლერების საშუალებით ხორციელდება, რომელიც მეტწილად აპარატულია, თუმცა შეიძლება პროგრამულიც იყოს, როცა იაფად გამოსვლის სურვილი არსებობს. კონტროლერი ან ცალკე სქემის სახით არსებობს (უფრო მძლავრი ფუნქციონალით), ან ინტეგრირებულია კომპიუტერის მთავარ პლატაზე.

ინფორმაციის მრავალდონური შენახვის მეთოდები

თანამედროვე კორპორაციულ ქსელებში გამოყენებული ინფორმაციის მოცულობა განუხრელად იზრდება. ინფორმაციის შენახვის ტექნოლოგიების მზარდი პროგრესის მიუხედავად, ახალი მეთოდების შემოღების აუცილებლობა დროის მცირე მონაკვეთებში ხდება საჭირო. სადღეისოდ კორპორაციული ინფორმაციის შენახვის ყველაზე პოპულარულ ტექნოლოგიას შენახვის მრავალდონიანი არქიტექტურა (**Multi Tier Storage**) წარმოადგენს, რომელშიც გარკვეული წესების საფუძველზე თავმოყრილია სხვადასხვა მწარმოებლურობისა და ღირებულების მოწყობილობები ინფორმაციის შენახვისთვის და მათი მმართველი ინტერფეისები. სადღეისოდ აღნიშნულ მოწყობილობათა შემდეგი კლასები შეიძლება გამოვყოთ:

SSD (Solid State Drive) - მყარსხეულიანი დისკური ტექნოლოგია, რომელიც ნახევარგამტარულ ტექნოლოგიას ეფუძნება და საყოველთაოდ ცნობილი ფლეშ-მეხსიერების სინონიმს წარმოადგენს. გამოირჩევა უაღრესად მაღალი მწარმოებლურობით და ასევე მაღალი ფასით;

SAS/FC (Serial Attached SCSI/Fibre Channel) - ხისტ დისკებზე აგებული ტექნოლოგია, რომელშიც ინფორმაცია კავშირის მაღალსიჩქარიანი არხით (მაგალითად, ოპტიკურბოჭკოვანი არხი) გადაიცემა, ხოლო ინფორმაციის შენახვის ღირებულება საკმაოდ დაბალია;

SATA - ხისტ დისკებზე აგებული ტექნოლოგია, რომელშიც კომბინაცია "მწარმოებლურობა/ღირებულება" ყველაზე ოპტიმალურია;

LTO - ლენტური ტექნოლოგია. ყველაზე იაფი და დაბალმწარმოებლური სისტემა ინფორმაციასთან მიმდევრობითი მიმართვით;

Blu Ray - ინფორმაციის შენახვის ოპტიკური ტექნოლოგია დაბალი ღირებულებით და დამაკმაყოფილებელი მწარმოებლურობით.

კორპორაციულ ინფორმაციის სხვადასხვა ტიპის საცავებში განაწილებისას მთავარ ამოცანას მოთხოვნის მიხედვით მისი კლასიფიცირება წარმოადგენს. საჭიროა შესრულდეს ინფორმაციის სასიცოცხლო ციკლის ანალიზი, რომლის დროსაც ირკვევა, რომ დროის კონკრეტულ მომენტში კონკრეტული ინფორმაცია ხშირად ან

ნაკლები სიხშირით იცვლება, ხოლო რაღაც მომენტიდან იგი პრაქტიკულად აღარ არის საჭირო.

ანალიზის პროცესში გასათვალისწინებელია დაგროვილი ინფორმაციის მოცულობაც. სწორედ ეს პარამეტრი განაპირობებს მრავალდონიან ინფორმაციულ საცავებში მონაცემთა მიგრაციის საჭიროებას და სიხშირეს, რისთვისაც სპეციალური პროგრამული უზრუნველყოფა არსებობს. იგი ავტომატურ რეჟიმში ასრულებს ინფორმაციის გადატანას მრავალდონიანი არქიტექტურის ფარგლებში, ინფორმაციის სტატუსის გათვალისწინებით.

თანამედროვე კორპორაციულ ქსელებში ინფორმაციის შენახვის და მართვის ყველაზე ოპტიმალურ სტრუქტურად სამდონიანი არქიტექტურა (**3-Tier Architecture**) ითვლება, რომელშიც ყოველ დონეს საკუთარი აგებულება და ამოცანები გააჩნია.

ინფორმაციის შენახვის სამდონიანი არქიტექტურის ზოგადი სქემა

პირველ, ე.წ. მწარმოებლურობის დონეზე (**Performance Tier, Tier 1**) პირველადი, ყველაზე ხშირად გამოსაყენებელი ინფორმაცია ინახება. მოცემული დონის ფიზიკური შემადგენლობა წარმოადგენს სწრაფქმედი **SAS/FC**-დისკების მასივს ინფორმაციის საიმედო შენახვის **RAID**-ინტერფეისებით. ამავე დონეზე მოიაზრება **SSD**-დისკების გარკვეული რაოდენობაც განსაკუთრებით აქტუალური ინფორმაციული მასივების შესანახად, თუმცა ჯერჯერობით ამგვარი დისკების ხვედრითი წილი კორპორაციულ ინფორმაციულ საცავებში ჯერ კიდევ დაბალია, რასაც მათი სიძვირე განაპირობებს.

მეორე დონე (**Capacity Tier, Tier 2**), რომელსაც "მოცულობითი დონე" ეწოდება, კორპორაციის ძირითადი, შედარებით ნაკლებაქტუალური ინფორმაციული მასივების შენახვას ემსახურება და როგორც წესი, **SATA/RAID**-ტექნოლოგიით ორგანიზებული გარე მეხსიერების მასივების ერთობლიობას წარმოადგენს.

მესამე, არქივაციის დონე (**Archive Tier, Tier 3**) გრძელვადიანი არქივების შესანახადაა განკუთვნილი და ლენტური და ოპტიკური შემნახველი მოწყობილობების საფუძველზეა აგებული. ამასთან, როგორც წესი, პრიორიტეტი ლენტური მეხსიერების აპარატურას ენიჭება, როგორც მეხსიერების დიდი მოცულობის, ასევე მეხსიერების მოწყობილობათა (მეხსიერების კასეტები) დიდი,

ავტონომიური სისტემების აგების შესაძლებლობათა გამო. არქივაციის დონეზე ინფორმაციის ცვლილება ან წაშლა მეტწილად მხოლოდ წინაწარ განსაზღვრულ, გრძელვადიან პერსპექტივაში ხდება.

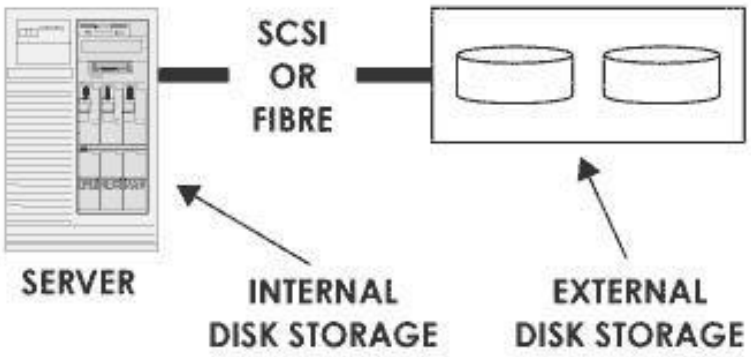
აღწერილ დონეებს შორის ინფორმაციის ავტომატური მიგრაცია, როგორც აღვნიშნეთ, მონაცემთა მართვის წინასწარ განსაზღვრული წესებით სრულდება, შესაბამისი პროგრამული უზრუნველყოფის გამოყენებით.

მონაცემთა საცავები

წინა ქვეთავში განხილური მონაცემთა შენახვის ფიზიკური ინფრასტრუქტურის დანიშნულებაა ინფორმაციის საიმედო და ოპტიმალური შენახვის უზრუნველყოფა და დროული მიწოდება მომხმარებლებისთვის. მეორე მოთხოვნა პირველზე არანაკლებ მნიშვნელოვანია, რადგან ინფორმაციის დაგვიანებით მიღება ხშირ შემთვევაში მისი არმიღების ტოლფასია. სადღეისოდ არსებობს ინფორმაციის შენახვის ისეთი სისტემები, რომლებიც მომხმარებლებს მონაცემებთან მაქსიმალურად ეფექტური მიმართვის და მათი საიმედო შენახვის საშუალებებს სთავაზობენ.

განვიხილოთ რამდენიმე ყველაზე გავრცელებული სისტემა, კერძოდ, **DAS, NAS** და **SAN**-სისტემები.

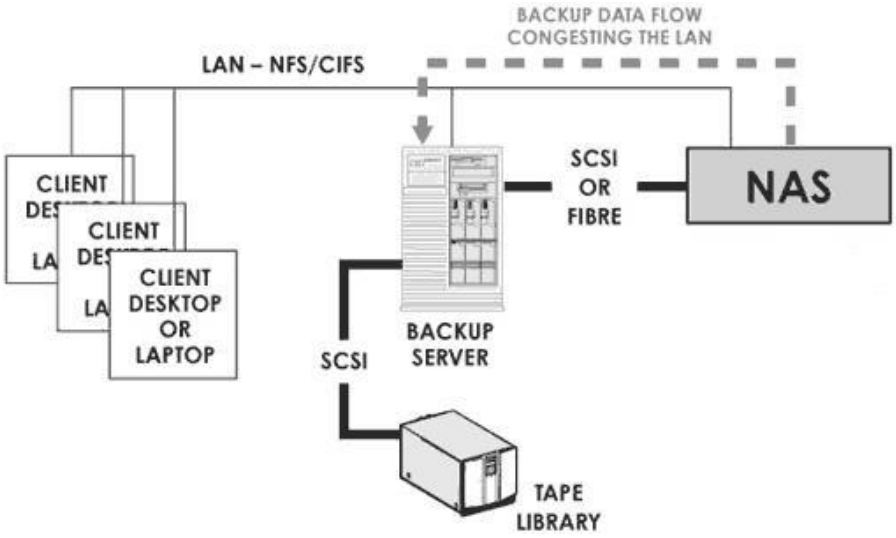
DAS (Direct Attached Storage) - მოწყობილება შიდა მეხსიერებით, პირდაპირ უერთდება ძირითად კომპიუტერს და ძირითადად ლოკალური სარეზერვო კოპირების ამოცანებს ემსახურება. მარტივად რომ ვთქვათ, **DAS** არის ჩვეულებრივი ხისტი დისკი, რომელიც ჰოსტთან დასაკავშირებლად ფართოდ გავრცელებულ **SCSI**-ტექნოლოგიას **(Small Computer System Interface)** იყენებს.



DAS-სისტემის სქემა

DAS-სისტემა ვერ უზრუნველყოფს მონაცემთა სარეზერვო კოპირებას რამდენიმე ჰოსტიდან, მითუმეტეს მონაცემთა განაწილებას. ამგვარი მოწყობილობის დაყენება

სარეზერვო კოპირების იაფფასიანი ვარიანტია, თუმცა გამოუსადეგარი მეტნაკლებად დიდი ორგანიზაციის კომპიუტერულ ქსელში.



NAS-სისტემის სქემა

NAS (Network Attached Storage) - "მონაცემთა ქსელური საცავი". წარმოადგენს კომპიუტერული ქსელის სრულუფლებიან წევრს შესაბამისი საიდენტიფიკაციო მონაცემებით (**MAC** და **IP**-მისამართები). **NAS**-სერვერის ძირითად ფიზიკურ კომპონენტს, როგორც წესი, 1 ან მეტი მეხსიერების ხისტი დისკი წარმოადგენს, თუმცა ხანდახან მის კონფიგურაციაში ოპტიკული ან ლენტური მოწყობილობებიცაა გათვალისწინებული. **NAS**-მოწყობილობა **(NAS Appliance)** მარტივად ირთვება ქსელში და წარმოადგენს ფაილ-სერვერს საკუთარი მცირე ოპერაციული სისტემითა და მართვის ვებ-ბაზირებული ინტერფეისით. **NAS**-სერვერები გარეგნულად **DAS**-მოწყობილობებს ჰგავს, მაგრამ პრინციპული განსხვავება მისგან ფაილებთან ქსელური წვდომის ეფექტური საშუალებებით.

SAN (Storage Area Network) - "მონაცემთა საცავების ქსელი" მაღალი საიმედოობისა და სისწრაფის გამო სადღეისოდ მონაცემთა საიმედო შენახვის ყველაზე გავცელებულ ტექნოლოგიას წარმოადგენს და მასობრივად ინერგება კორპორაციულ ქსელებში.

ტექნოლოგია ეფუძნება გამოყენებულია ძალიან სწრაფ ოპტიკურ-ბოჭკოვანი კავშირის **Fibre Channel**-ტექნოლოგიას, რომელიც ინფორმაციის გადაცემის სიჩქარეა 1-2 გბ/წმ სიჩქარეს უზრუნველყოფს. ამასთან, მონაცემთა საცავის ქსელი ფიზიკურად გამოცალკევებულია ძირითადი კორპორაციული ქსელიდან, რაც ძლიერ ზრდის სარეზერვო ასლების შექმნისა და არქივაციის პროცედურების ეფექტურობას და ინფორმაციის შენახვის საიმედობას. ამასთან, მნიშვნელოვანია ძირითადი ქსელური არხების განტვირთვის ფაქტორიც, რადგან სწორედ აღნიშნული პროცედურები (სარეზერვო კოპირება, არქივაცია) მოითხოვენ

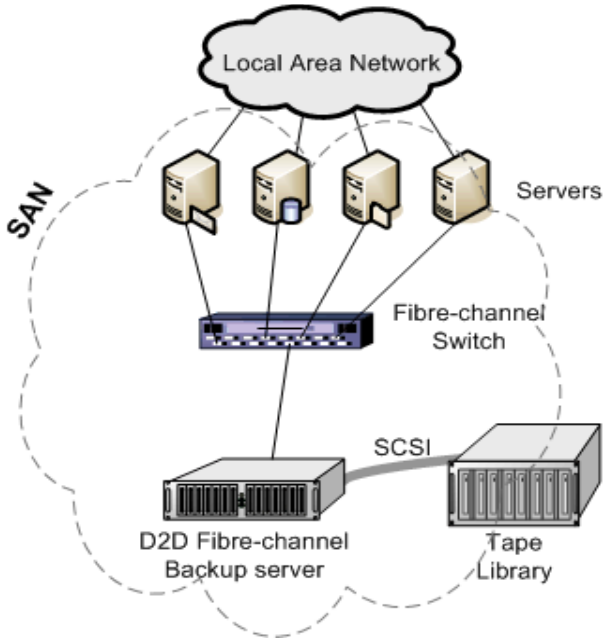
ყველაზე დიდი ოდენობით ქსელურ რესურსებს და ინფორმაციული არხების მაღალ გამტარუნარიანობას.

სადღისოდ სერვერული სისტემების ბაზარზე **SAN**-საცავების საკმაოდ ბევრი ვარიანტი არსებობს, რაც დამკვეთი კომპანიების ერთმანეთისგან რადიკალური მოთხოვნების დაკმაყოფილებას უზრუნველყოფს.

მაგალითად, **Fibre Channel** ტექნოლოგიის გამოყენება შეიძლება 100 კილომეტრის რადიუსში (შედარებისთვის: ჩვეულებრივი **SCSI**-ინტერფეისების მოქმედების რადიუსი მხოლოდ 25 მეტრს შეადგენს).

SAN-ქსელის ცენტრალურ კომპონენტს ოპტიკური არხის ადაპტერი (**Fibre Channel host bus adapter — FC HBA**), რომელიც სერვერებსა და მონაცემთა საცავებს შორის კავშირს უზრუნველყოფს. კერძოდ, იგულისხმება შემდეგი ფუნქციონალი:

- ინტერფეისი სერვერებსა და მონაცემთა საცავებს შორის ნებისმიერი ქსელური ტოპოლოგიის ფარგლებში
- მონაცემთა საცავების ცენტრალიზებული მართვა (კონფიგურება, მონიტორინგი და ქსელის კომპონენტების ანალიზი.
- დისკურ მასივებთან წვდომის უფლებების მართვა.



SAN-სისტემის სქემა

მონაცემთა დამუშავების ცენტრი

მონაცემთა საცავების ყველაზე მასშტაბურ მოდიფიკაციას **მონაცემთა დამუშავების ცენტრი** (**Data Center**) წარმოადგენს, რომელიც დიდი მოცულობის და მრავალფეროვანი ინფორმაციის (ტექსტური, მონაცემთა ბაზები, მულტიმედია) ეფექტურ და საიმედო შენახვას უზრუნველყოფს. მონაცემთა დამუშავების ცენტრი

შედარებით ნაკლებადაა გავრცელებული მისი მაღალი ღირებულების გამო. საკუთარი მონაცემთა ცენტრები გააჩნიათ მეტწილად დიდ კორპორაციებს და ინტერნეტ-სერვის-პროვაიდერებს, რომლებიც მომხმარებლებს კარგად განვითარებულ ჰოსტინგის სერვისს სთავაზობენ.

სარეზერვო კოპირება და არქივაცია

კორპორაციული ქსელის სერვერული სისტემა წარმოუდგენელია კარგად გამართული სარეზერვო კოპირებისა და არქივაციის სისტემის გარეშე. ინფორმაციის სარეზერვო საცავები გვაძლევენ გარანტიას, რომ კორპორაციული ინფორმაცია არ დაიკარგება უკიდურეს შემთხვევაშიც კი, ხანძრის ან სტიქიური უბედურების შედეგად.

სარეზერვო კოპირების მრავალფეროვანი სისტემები არსებობს, რომელთაგან თითოეულს საკუთარი გამოყენების სფერო გააჩნია კომპიუტერული ქსელის მასშტაბებისა და შესასრულებელ ამოცანათა მოცულობის მიხედვით.

კლასტერული არქიტექტურა

კლასტერული არქიტექტურა სერვერულ სისტემებში (განსაკუთრებით მონაცემთა ბაზის სერვერებზე) ერთერთ ყველაზე აპრობირებულ ტექნოლოგიას წარმოადგენს.

კლასტერი - ეს არის კომპიუტერების ჯგუფი რომელიც შედგება ორი ან მეტი კომპიუტერებისგან, რომლებიც მუშაობენ ერთად იმისთვის, რომ უზრუნველყონ პროგრამების საერთო ნაკრების ან სერვისების მუშაობა რომლებსაც მომხმარებელი აღიქვამს როგორც ერთ მთლიანს. კომპიუტერები ფიზიკურად ერთიანდებიან აპარატურული საშუალებებით ქსელის სახით ან საერთო შესანახი მოწყობილობებით. კლასტერების პროგრამული უზრუნველყობა უზრუნველყოფს საერთო ინტერფეისს, ამასთან ერთად მართავს რესურსებს და კლასტერის შიგნით მყოფი კომპიუტერების დატვირთვას. კლასტერი შემდეგი ძირითადი ელემენტებისგან შედგება

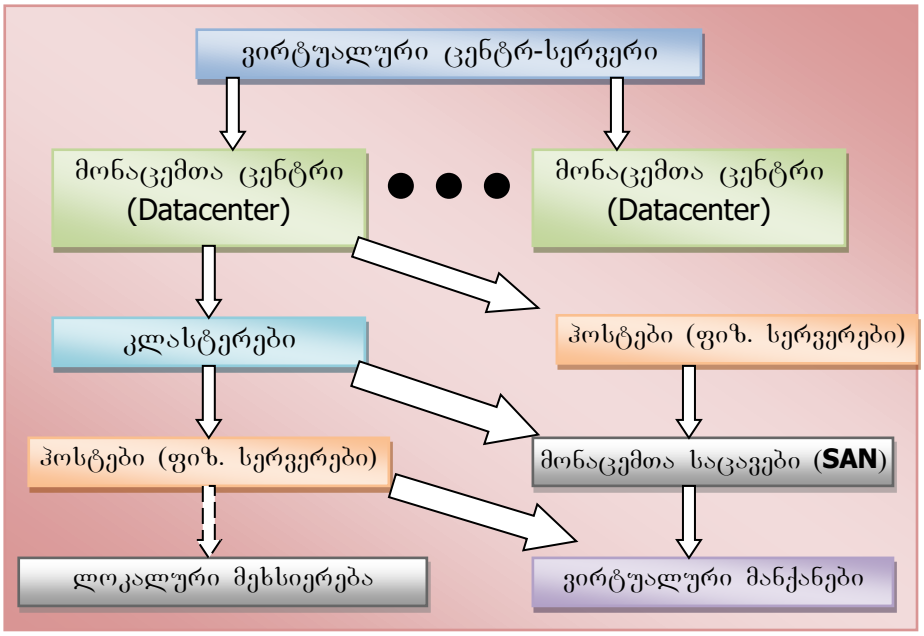
- კვანძი (როგორც წესი, ფიზიკური ან ვირტუალური სერვერი)
- რესურსთა ჯგუფი
- ქვორუმ-რესურსი (ხისტი დისკი კლასტერის კონფიგურაციის მონაცემთა ბაზით)
- რესურსები (ფიზიკური დისკი ლოკალური ან გარე მეხსიერების მასივიდან, IP-მისამართი, კომპიუტერის ქსელური სახელი (ვირტუალური სერვერი), სისტემური სერვისი, განაწილებული ფოლდერი, განაწილებული პროგრამა, ვირტუალური მანქანა

კლასტერის ელემენტებს შორის დამოკიდებულებებს შემდეგი სახე აქვს: **რესურსი -> რესურსი** (მაგ. **განაწილებული ფოლდერი -> ხისტი დისკი**). მოქმედებს იერარქიულობის პრინციპი

კლასტერის მუშაობის პრინციპი: კლასტერის რომელიმე კვანძის მწყობრიდან გამოსვლისას მასზე განთავსებული რესურსები ავტომატურად გადამისამართდება აქტიურ კვანძზე (**Failover**). სისტემა აგრძელებს მუშაობას.

სერვერული სისტემის არქიტექტურა

ზემოთ აღწერილი ტექნოლოგიების კომბინირებული გამოყენება რთული სერვერული სისტემების დაპროექტებისა და აგების საშუალებას იძლევა. სერვერული სისტემის ზოგადი სტრუქტურა ნახ-ზეა მოცემული.



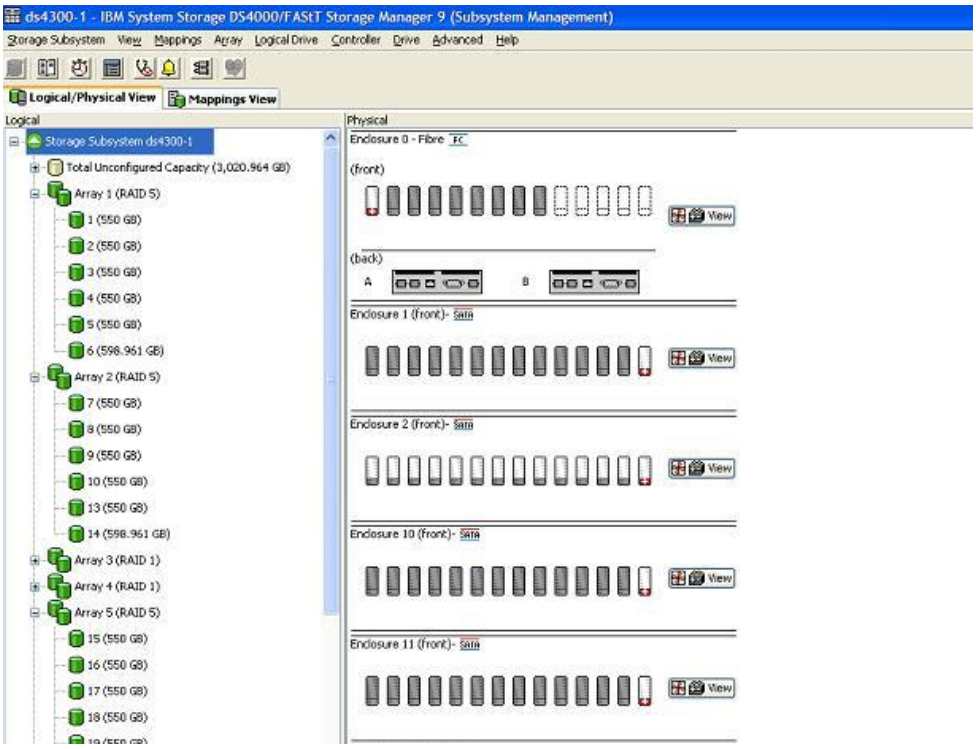
ვირტუალური სერვერული სისტემის არქიტექტურა

როგორც ნახაზი უჩვენებს, ინტეგრირებული სერვერული არქიტექტურა შეიძლება გასცდეს კიდეც კორპორაციული ქსელის ფარგლებს და მონაცემთა ცენტრის სახით რამდენიმე ქსელის ინფორმაციული სივრცე მოიცვას, თუმცა უნდა აღინიშნოს, რომ პრაქტიკაში ამგვარი შემთხვევები შედარებით ნაკლებია.

მონაცემთა საცავების მართვა

მონაცემთა საცავების მართვა განცალკევებულ პროცესს წარმოადგენს და მონაცემთა საცავების საკუთარი შიდა სტრუქტურის აგებას გულისხმობს, რომელიც შემდგომ სხვადასხვა სერვისების მიერ სხვადასხვა მოცულობით და მონაცემთა საცავების სხვადასხვა ქსელების ფარგლებში **(Fibre Channel, iSCSI)** შეიძლება იქნეს გამოყენებული. შიდა სტრუქტურა უნდა აკმაყოფილებდეს

საიმედობის და და მონაცემებთან მაქსიმალურად სწრაფად მიმართვის პირობებს. საამისოდ, მონაცემთა საცავების მართვის პროგრამებს ინსტრუმენტების ფართო ნაკრები გააჩნიათ.



IBM Fibre Storage Manager - ინტერფეისის ფრაგმენტი

საიმედობის მართვა MS SQL Server-ის გარემოში

მონაცემთა ბაზები ნებისმიერი ინფორმაციული სისტემის საკვანძო კომპონენტია. სწორედ ბაზებში შენახული ინფორმაციის საფუძველზე ხორციელდება ნებისმიერი კერძო თუ სახელმწიფო ორგანიზაციის საქმიანობა. ბაზის დაკარგვა ბიზნესის განადგურების ტოლფასია, ამიტომ ნებისმიერ დაწესებულებაში მომუშავე IT-სპეციალისტის ერთერთ უმთავრეს საზრუნავს ისეთი სქემის დამუშავება წარმოადგენს, რომელშიც, ჯერ ერთი, მონაცემთა ბაზების დაკარგვის ალბათობა მინიმალური იქნება და ამასთან, ინფორმაციასთან წვდომის განხორციელება შეუფერხებლად იქნება შესაძლებელი.

მონაცემთა ბაზების მართვის სისტემა MS SQL Server აღნიშნული მიმართულებით ერთერთ მოწინავე პროგრამულ უზრუნველყოფას წარმოადგენს. იგი შეიცავს მძლავრ ინსტრუმენტულ ბაზას როგორც „ცოცხალი“ ბაზების საიმედო მუშაობის (მონაცემთა ბაზის სერვერთა კლასტერი, „სარკე“, რეპლიკაცია), ასევე მათი სარეზერვო ასლების (ბექაფი, ლოგ-შიფი) ეფექტური მართვისთვის.

წინამდებარე ნაშრომში სწორედ მონაცემთა ბაზების საიმედობის უზრუნველყოფის საფუძვლები და MS SQL Server-გარემოში მისი რეალიზაციის

საშუალებებია მოცემულია. თემის დიდი მოცულობის გამო, პრაქტიკულ ნაწილში სისტემის მხოლოდ სამი ფუნქციაა განხილული - სარეზერვო კოპირება, მონაცემთა ბაზების „სარკული“ ასახვა და რეპლიკაცია.

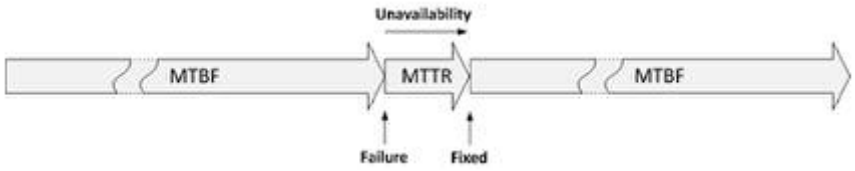
წვდომის უწყვეტობის უზრუნველყოფა ინფორმაციულ სისტემებში

სარგებლიანობის და საიმედობის განსაზღვრა

ნებისმიერი ინფორმაციული სისტემის და მათ შორის მონაცემთა ბაზების უსაფრთხოებაზე ზრუნვა **კიბერმდგრადობის** (Cyber Resilience) უზრუნველყოფით იწყება. უსაფრთხოების ყველა სხვა ზომაზე ფიქრი ძნელია მანამ, სანამ ბაზასთან უწყვეტი წვდომა არ იქნება უზრუნველყოფილი მისი მომხმარებლებისთვის.

ნებისმიერი ინფორმაციული სისტემის გამართულ მუშაობას **ფუნქციონალურ ატრიბუტებთან** (გამოყენებული პროცესორული, ოპერატიული და გარე მეხსიერების რესურსები, მწარმოებლურობა) ერთად **არაფუნქციონალურ ატრიბუტების** ოპტიმალური მნიშვნელობები განაპირობებს. ორ ყველაზე განხილვად და გამოყენებად არაფუნქციონალურ ატრიბუტებს **სარგებლიანობა** (Availability) და **საიმედობა** (Reliability) წარმოადგენს, რომლებიც ერთნაირი წარმატებით გამოიყენება ინფორმაციული ტექნოლოგიების სხვადასხვა ქვესისტემებში (სისტემური და ქსელური აპარატული უზრუნველყოფა, მონაცემთა ბაზები, ვებ-სერვისები), ასევე მთლიანი IT-ინფრასტრუქტურის მუშაობის აღსაწერად.

სარგებლიანობაც და საიმედობაც IT-ინფრასტრუქტურის რესურსებთან **წვდომის უწყვეტობის** უზრუნველყოფას ემსახურება. მათი განსაზღვრისთვის შემდეგი ძირითადი დროითი პარამეტრები გამოიყენება (სურათი 1)[2].



MTBF და MTTR

სადაც:

- MTBF (Mean Time Between Failures) - არის საშუალო დრო IT-ინფრასტრუქტურის კომპონენტის გათიშვებს შორის;
- MTTR (Mean Time to Restore) - არის გათიშვიდან აღდგენის საშუალო დრო.

[2] http://www.eventhelix.com/realtimemantra/faulthandling/reliability_availability_basics.htm#.V1_sZvl96Ul

სარგებლიანობა წარმოადგენს IT-ინფრასტრუქტურის ცალკეული კომპონენტების ან მათი ჯგუფების უწყვეტი მუშაობის თანაფარდობას სისტემის მთლიან საექსპლოატაციო დროსთან და გამოითვლება ფორმულით:

$$A = \frac{MTBF}{MTBF + MTTR}$$

საიმედობა განისაზღვრება IT-ინფრასტრუქტურის კომპონენტების ან კომპონენტთა ჯგუფის უწყვეტი მუშაობისა და უქმად ყოფნის დროის საშუალო მაჩვენებლებით. სისტემა საიმედოა უწყვეტი მუშაობის დროის მაქსიმიზაციისა და გათიშვის დროის მინიმიზაციის შემთხვევაში.

IT-კომპონენტი შეიძლება იყოს **სარგებლიანი,** მაგრამ **არასაიმედო** და პირიქით. მაგალითად, თუ ვებ-გვერდის გაჩერების მაქსიმალურად დასაშვები დრო წელიწადში 4 საათია და ამასთან, სისტემა დროის 99,9%-ის მანძილზე უნდა მუშაობდეს, მაშინ გვექნება სარგებლიანობის და საიმედობის შემდეგი ვარიანტები:

- თუ სისტემა წელიწადში ორჯერ 2-2 საათით გაითიშება, იგი იქნება **სარგებლიანი** და **საიმედო;**
- თუ სისტემა წელიწადში მხოლოდ ერთხელ 5 საათით გაითიშება, იგი იქნება **სარგებლიანი** (არ ირღვევა სისტემის სარგებლიანობის 99,9%-იანი მაჩვენებელი) და **არასაიმედო** (ბიზნეს-პროცესების უწყვეტობის გეგმით გათვალისწინებული გათიშვის პარამეტრის დარღვევა ზიანს აყენებს ბიზნესს);
- თუ სისტემა წელიწადში 10-ჯერ თითო საათით გაითიშება, იგი იქნება **უსარგებლო** (ირღვევა სისტემის სარგებლიანობის 99,9%-იანი მაჩვენებელი), მაგრამ **საიმედო** (ბიზნეს-პროცესების უწყვეტობის გეგმით გათვალისწინებული გათიშვის ზღვრული დროის მნიშვნელობა არ დარღვეულა).

ამრიგად, სარგებლიანობა და საიმედობა ერთმანეთზე მხოლოდ ნაწილობრივ დამოკიდებული სიდიდეებია, მიუხედავად იმისა, რომ მათი გამოთვლისთვის იდენტური მონაცემები გამოიყენება.

თანამედროვე ინფორმაციული ტექნოლოგიების ყველა მიმართულებით საიმედობისა და სარგებლიანობის გაზრდის მრავალრიცხოვანი, დახვეწილი მეთოდებია შემუშავებული. მოვიყვანთ რამდენიმე მაგალითს:

- **ინფორმაციის დუბლირება**, მათ შორის გეოგრაფიულად დაშორებულ პუნქტებში - არქივაცია, სარეზერვო კოპირება, მონაცემთა "სარკე",
- **აპარატული უზრუნველყოფის დუბლირება** - სერვერთა ფერმა, კლასტერი, ქსელური მოწყობილობების სტეკირება, RAID-ტექნოლოგია გარე ხისტი დისკების "ცხელი" ჩანაცვლებით, ოპერატიული მეხსიერება შეცდომათა გასწორების ECC-მექანიზმით;

- **სერვერთა და მონაცემთა საცავების მაქსიმალური განცალკევება** - ტექნოლოგია SAN (Storage Area Network), რომელიც კომპიუტერების, მეხსიერების საცავებისა და მათ შორის კავშირების ერთობლიობას წარმოადგენს
- შესაძლო ავარიულ სიტუაციათა განხილვა (სერვერის, მონაცემთა საცავის, ქსელური მოწყობილობის ან პროგრამული უზრუნველყოფის ავარიული გაჩერება, ელექტროლკვების გათიშვა, სტიქიური უბედურება, მიწისძვრა, ტერაქტი) და მათი თავიდან აცილების საშუალებების დამუშავება **(Disaster Recovery Plan)**

საილუსტრაციოდ ავიღოთ მონაცემთა ცენტრის ტიპიური ბლოკი: სერვერი, SAN-კომუტატორი, მონაცემთა საცავი. მოცემულ ბლოკში, თუ იგი წესების დაცვით არის აწყობილი, მონაცემთა საიმედო შენახვა და სარგებლიანობა რამდენიმე დონეზეა უზრუნველყოფილი:

- **სერვერის ადაპტერის დონე** - FC HBA-ადაპტერები ყოველ ჰოსტზე, როგორც წესი, ორი ცალი ყენდება, ამასთან პირველი გაფორმებულია, როგორც პირველადი და მეორე - როგორც ალტერნატიული ადაპტერი. პირველის მწყობრიდან გამოსვლისას, ინფორმაციის მომსახურების ამოცანებს ავტომატურად მეორე ადაპტერი გადაიბარებს.
- **სერვერის (ჰოსტის) დონე:** კლასტერული ტექნოლოგიის წყალობით ორი ან მეტი ფიზიკური ან/და ვირტუალური ჰოსტი ერთ სერვერად აღიქმება, ანუ კვანძის დაზიანებისას, მის ამოცანებს და რესურსებს ავტომატურად მეორე კვანძი გადაიბარებს. კლასტერის ქსელური სახელები (რომლებსაც სერვისები იყენებენ) კვანძებისგან დამოუკიდებელია და მნიშვნელობა არა აქვს, სერვისი რომელ კვანძზე სრულდება.
- **მონაცემთა საცავების დონე:** ხისტი დისკების საცავის მმართველი სერვერები გეოგრაფიულად დაშორებულ ადგილებშია განთავსებული, ისევე, როგორც ხისტი დისკების სარკისებური მასივები. ერთ ადგილას თუნდაც დენის გათიშვისა ან სტიქიური უბედურებისას საცავები მეორეგან იქნება ხელმისაწვდომი.

ჩვენი ნაშრომი ჩამოთვლილთაგან ერთ კონკრეტულ მიმართულებას, **მონაცემთა ბაზებს** და მათი მუშაობისთვის საიმედო გარემოს შექმნას ეხება, რაზეც მომდევნო ქვეთავში ვისაუბრებთ.

მონაცემთა ბაზების მართვის სისტემების მიმოხილვა

მონაცემთა ბაზების თეორია და მათი მართვის სისტემების შექმნა ინფორმაციული ტექნოლოგიების ერთერთ უმნიშვნელოვანეს სფეროს წარმოადგენს. უდავოა, რომ სადღეისოდ ცხოვრების პრაქტიულად ყველა სფეროში ინფორმაციული

სისტემების დაპროექტებისა და აგებისას ყველაზე დიდი ყურადღება ამ სისტემების **„უკანა მხარეს“** (Back-End), ანუ **მონაცემთა ბაზებს** ერგება. არასწორად შედგენილ მონაცემთა ბაზის მოდელს და მის პრაქტიკულ რეალიზაციას, აგრეთვე არასწორად შერჩეულ და გამართულ მონაცემთა ბაზების მართვის სისტემას ბიზნესის ან სხვა ტიპის საქმიანობისთვის აუნაზღაურებელი ზარალის მიყენება შეუძლია.

სანამ ინფორმაციული სისტემა მონაცემთა ბაზებთან სატესტო თუ საწარმოო რეჟიმში მუშაობას დაიწყებდეს, სისტემის ან/და მონაცემთა ბაზების ადმინისტრატორებს მართებთ საიმედო გარემოს შექმნა, რომელშიც ინფორმაციის დაზიანების ან დაკარგვის ალბათობა მინიმალური იქნება.

მონაცემთა ბაზების აპარატულ საცავს ფიზიკური ან ვირტუალური **ჰოსტი** წარმოადგენს, რომელიც შეიძლება ერთი ან მეტი **მონაცემთა ბაზების სერვერ(ებ)ისგან** (**ეგზემპლარი, ინსტანსი**) შედგებოდეს. მონაცემთა ბაზის სერვერი SQL Server წარმოადგენს დამოუკიდებელ პროგრამას (ოპერაციული სისტემის პროცესები sqlservr.exe, sqlWb.exe), რომელიც შემდეგი ძირითადი კომპონენტებისგან შედგება:

- **მონაცემთა ბაზების მართვის ინსტრუმენტი** (Database Engine)
- **მეხსიერების მართვის ინსტრუმენტი** (Storage engine)
- **უსაფრთხოების ქვესისტემა** (Security Subsystem)
- **პროგრამული ინტერფეისი** (Programming Interfaces)
- **სერვისების ბროკერი** (Service Broker)
- **სერვერის აგენტი** (SQL Server Agent)
- **რეპლიკაციის მოდული** (Replication)
- **მაღალსარგებლიანობის უზრუნველყოფის ინსტრუმენტი** (High Availability)
- **რელაციურ ოპერაციათა მართვის ინსტრუმენტი** (Relational engine)

მონაცემთა ბაზა, თავის მხრივ, შეიცავს რელაციური მოდელის მიხედვით დაპროექტებულ **ცხრილებს, სქემებს (Views), ტრიგერებს, შენახული პროცედურებს** და ინფორმაციის დასამუშავებლად აუცილებელ სხვა ელემენტებს.

მონაცემთა ბაზების უსაფრთხოება. მათი სარგებლიანობის და საიმედობის ამაღლების მეთოდები

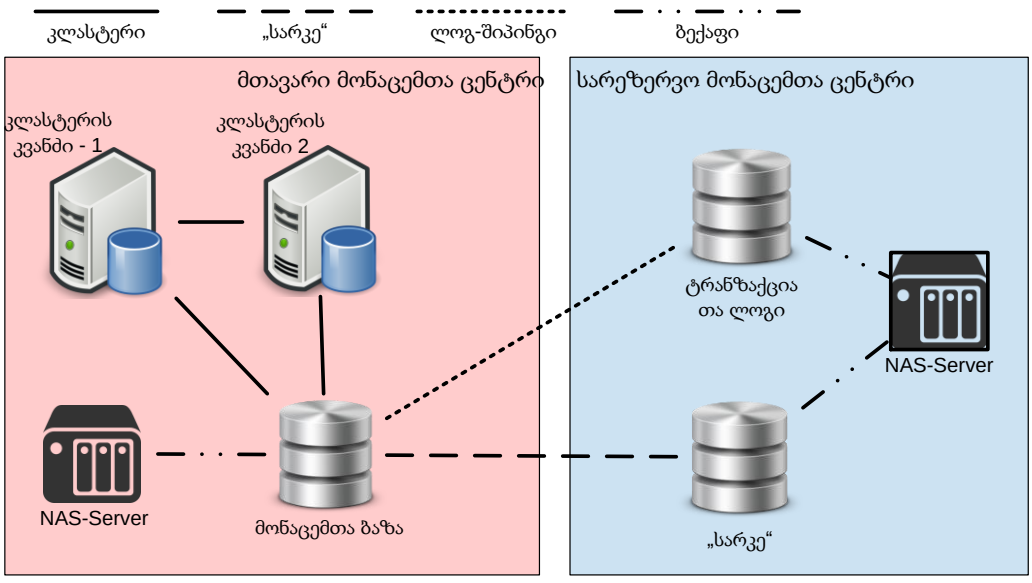
მონაცემთა ბაზებში ინფორმაციის შენახვის **სარგებლიანობის მაღალი დონე** გულისხმობს მონაცემთა გამრავლების (კოპირების) ისეთი მექანიზმის შემუშავებას, რომლებიც:

- მაქსიმალურად შეამცირებს ინფორმაციის დაკარგვის ალბათობას მინიმალური შესაძლო რესურსების გამოყენებით;
- უზრუნველყოფს დაკარგული ინფორმაციის სწრაფ აღდგენას მინიმალური ინფორმაციული დანაკარგებით.

მოცემული მიზნების მისაღწევად მონაცემთა ბაზების სერვერებსა და მონაცემთა ბაზებზე სრულდება შემდეგი პროცედურები:

- მონაცემთა ბაზების სერვერთა **კლასტერის** შექმნა;
- მონაცემთა ბაზების სარკული ასახვა **(მირორინგი);**
- მონაცემთა ბაზების **რეპლიკაცია;**
- ტრანზაქციათა ჟურნალის გატანა **(ლოგ-შიპინგი);**
- მონაცემთა ბაზების სარეზერვო კოპირება **(ბექაფი)**.

ჩამოთვლილი თვისებებით აღჭურვილი მონაცემთა ბაზების მაღალსარგებლიანი ინფრასტრუქტურის ნიმუში მოცემულია სურათზე.



მაღალსარგებლიანი მონაცემთა ბაზების ინფრასტრუქტურის მაგალითი

მონაცემთა ბაზის სერვერთა კლასტერი (Database Server Cluster) ბაზის სერვერების ორი ან მეტი ეგზემპლარისთვის (ინსტანსებისთვის) აიგება. ძირითადი SQL-სერვერის ავარიული გათიშვის შემთხვევაში მონაცემთა ბაზების მართვის ფუნქციებს ავტომატურად, Failover-ფუნქციის გამოყენებით, კლასტერის სხვა სერვერი გადაიბარებს. ამრიგად, კლასტერული არქიტექტურა ერთადერთია, რომელიც არა **მონაცემთა ბაზების,** არამედ **მონაცემთა ბაზის სერვერების** დონეზე მუშაობს.

რეპლიკაცია (Database Replication) შეიძლება განვავრცოთ მთლიან მონაცემთა ბაზაზე ან მის ნაწილზე (ცხრილები, სქემები და სხვა). მის დანიშნულებას მონაცემთა ბაზებს შორის ინფორმაციის საიმედო გაცვლის უზრუნველყოფა წარმოადგენს: **მონაცემთა გამცემი** (Database Publication) მუდამ უახლეს ინფორმაციას აწვდის **მონაცემთა მიმღებს** (Database Subscription). იხილეთ სურათი მომდევნო გვერდზე.

ლოგ-შიპინგი (Log shipping) მონაცემთა სარეზერვო კოპირების ყველაზე იაფ და იოლად განხორციელებად საშუალებას წარმოადგენს. მისი საშუალებით სრულდება **მონაცემთა ბაზის ტრანზაქციათა ლოგის** (ანუ ბაზაში შესრულებული მოქმედებების სრული ჟურნალის) კოპირება მონაცემთა ბაზის სხვა სერვერზე, ხოლო ძირითადი ბაზის დაკარგვის შემთხვევაში არის შესაძლებლობა ლოგიდან ბაზის აღდგენისა. ლოგ-შიპინგის მინუსი ისაა, რომ საწყისი ბაზის აღდგენას ხშირად საკმაოდ დიდი დრო სჭირდება.

მირორი („სარკე“) (Database Mirror) მონაცემთა ბაზისთვის სხვა SQL Server-ის ეგზემპლარზე იდენტური მონაცემთა ბაზის შექმნას გულისხმობს. ნებისმიერი ცვლილება **საწყის ბაზაში** (Primary Database) ავტომატურად ფიქსირდება **„სარკე“-ბაზაშიც** (Secondary Database). საწყისი მონაცემთა ბაზის მწყობრიდან გამოსვლის შემთხვევაში ადმინისტრატორი შეასრულებს გადართვას ბაზის სათადარიგო ეგზემპლარზე. გადართვა შეიძლება ავტომატურ რეჟიმშიც განხორციელდეს, მესამე, ე.წ. **„მოწმე“-სერვერის** (Witness Server) გამოყენებით. სარკული ასახვა 1:1-ტიპის სტრუქტურაა, მონაცემთა ბაზას მხოლოდ ერთი „სარკული“ ასლი შეიძლება გააჩნდეს.

და ბოლოს, მონაცემთა ბაზების **სარეზერვო ასლების** (Backup) შექმნა-ტრანსპორტირება გულისხმობს ბაზის ასლის შექმნას კონკრეტული დროის მდგომარეობით. სარეზერვო ასლების ფორმირების თემა დეტალურად მომდევნო ქვეთავში იქნება აღწერილი.

სარგებლიანობის და საიმედობის უზრუნველყოფა SQL Server-ის გარემოში

მონაცემთა ბაზების სარეზერვო კოპირება

სარეზერვო კოპირებას დროის კონკრეტულ მომენტში მონაცემთა ბაზის მდგომარეობის დასაფიქსირებლად და შესანახად იყენებენ. სარეზერვო ასლის **შექმნის** შემდეგ (Database Backup), საჭიროების შემთხვევაში, შესაძლებელია მონაცემთა ბაზის **აღდგენა** (Restore) იმ მდგომარეობაში, რომელშიც იგი სარეზერვო ასლის შექმნისას იმყოფებოდა.

სარეზერვო ასლები ორ ძირითად ფორმატში ინახება: .bak-ფაილში **სრული** ან **დიფერენციალური** ასლები იქმნება, ხოლო .trn-ფაილები **ტრანზაქციების ჟურნალს** (ანუ ლოგებს) ინახავს. მარტივი სარეზერვო ასლის შესაქმნელად ადმინისტრატორმა SQL Server Management Console-ში უნდა გამოიძახოს ბრძანება:

მონაცემთა ბაზაზე მაუსის მარჯვენა ღილაკი -> Tasks -> Backup

ხოლო აღსადგენად:

მონაცემთა ბაზაზე მაუსის მარჯვენა ღილაკი -> Tasks -> Restore -> Database

ორივე შემთხვევაში გამოდის საკმაოდ მარტივი ინტერფეისი, რომელშიც სისტემის ან/და მონაცემთა ბაზის ადმინისტრატორი ადვილად გაერკვევა. განვიხილოთ შედარებით კომპლექსური ამოცანა, რომელიც ორგანიზაციის ინფორმაციული სისტემების მონაცემთა ბაზების, **გეგმიურ, ავტომატიზებულ სარეზერვო კოპირებასა** და სარეზერვო ასლების **დაშორებულ საცავში** (NAS-სერვერზე) გადატანას გულისხმობს.

სანიმუშოდ ავაგოთ ორგანიზაციის ორი (კადრების და ბუღალტერიის) მონაცემთა ბაზების სარეზერვო კოპირების გრაფიკი.

მბ სერვერი	მონაცემთა ბაზა	ბექაფის ტიპი	თარიღი და დრო
HR	HRMain	ინდექსების გადაშენება	ყოველდღე 12:00AM
	HRMain	სრული	ყოველ კვირადღეს 1:00AM
	HRMain	დიფერენციალური	ყოველდღე გარდა კვირისა 1:00AM
	HRFiles	სრული	ყოველ კვირადღეს 12:30AM
	HRFiles	დიფერენციალური	ყოველდღე 12:30AM

	HRMain, HRFiles	NAS-ზე კოპირება	ყოველ კვირადღეს 2:30AM
Accounting	AccountingDB	სრული	ყოველ კვირადღეს 1:00AM
	AccountingDB	დიფერენციალური	ყოველდღე გარდა კვირისა 1:00AM
	AccountingDB	სრული	ყოველი თვის პირველ რიცხვში 2:00AM
	AccountingDB	NAS-ზე კოპირება	ყოველდღე 1:30AM

მოცემული გრაფიკის რეალიზაციას რამდენიმე პროგრამული მოდულის გამოყენება სჭირდება:

- SQL Server Management Studio
  - Management -> Maintenance Plans
  - SQL Server Agent;
- NAS-სერვერის (Network Area Storage) მართვის პროგრამა.

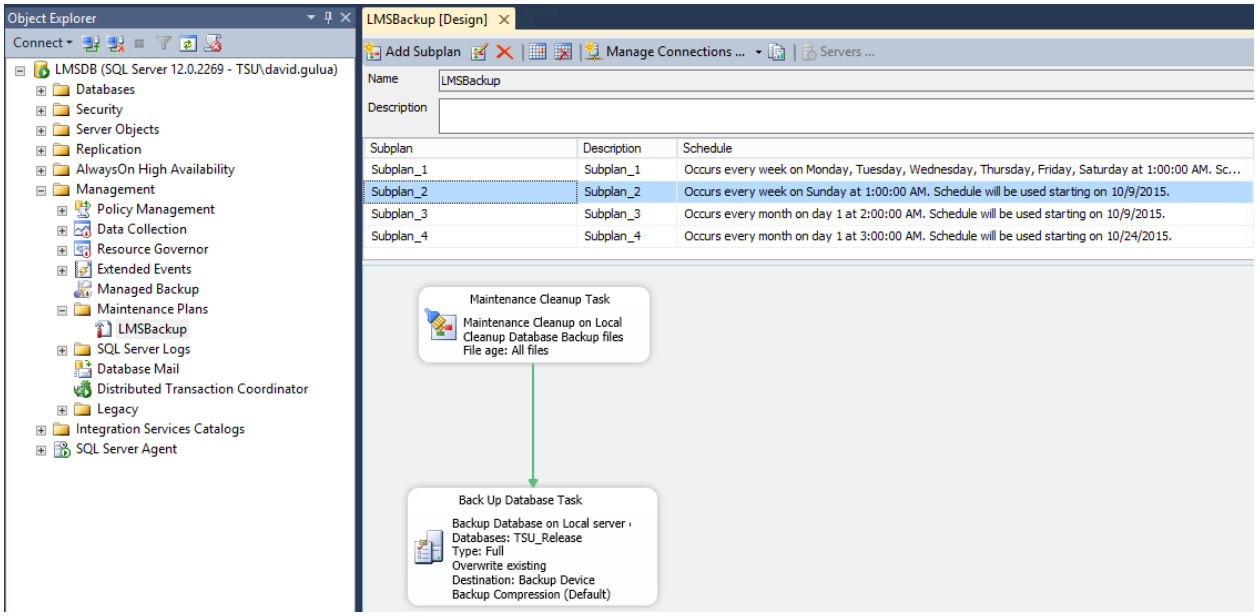
მონაცემთა ბაზების მოვლის მოდული (Management -> Maintenance Plans) არამარტო სარეზერვო კოპირების, არამედ მონაცემთა ბაზების ოპტიმალურ მდგომარეობაში შენახვის მრავალფეროვან ამოცანებს ემსახურება. ჩამოვთვალოთ რამდენიმე:

- სარეზერვო ასლების შექმნა და წაშლა;
- მონაცემთა ცხრილები რეინდექსაცია/ინდექსების რეორგანიზაცია მონაცემთა ბაზასთან მიმართვის დასაჩქარებლად; MS SQL Server-ში რეინდექსაცია (ქართულ აიტი-სლენგზე **ინდექსების გადაშენება)** ორგვარია:
  - Rebuild all – ინდექსების სტრუქტურა თავიდან ყალიბდება. შეფერხების შემთხვევაში გააჩნია როლბექ-ფუნქცია. სრულდება როგორც ონლაინ, ასევე ოფლაინ-რეჟიმში.
  - Reorganize all - უფრო „მსუბუქი“ ოპერაციაა, სრულდება მხოლოდ ონლაინ რეჟიმში.
- მონაცემთა ბაზების შეკუმშვა (Shrinking) გარე მეხსიერების ეკონომიისთვის;
- MS SQL Server-ის გარემოში T-SQL-სკრიპტების გაშვება;

მონაცემთა ბაზის მოვლის გეგმა ყალიბდება **ქვეამოცანების** (Subplans) მიმდევრობის სახით. საჭიროების შემთხვევაში დგება განრიგი ანუ თითოეულ მოქმედებას (ბიჯს) განესაზღვრება შესრულების თარიღი და დრო. მაგალითად, მონაცემთა ბაზების, HRMain და HRFiles-ისთვის ზემოთ მოცემული სარეზერვო კოპირების გეგმის შესასრულებლად საჭირო ბიჯები შემდეგი სახით შეიძლება წარმოვადგინოთ:

- ყოველ კვირა დღეს, ღამის 12 საათსა და 30 წუთზე იქმნება **სრული** სარეზერვო ასლი მონაცემთა ბაზისთვის HRFiles. იმავე სახელის მქონე არსებული სარეზერვო ასლი იშლება;
- ყოველდღე, გარდა კვირისა, ღამის 12 საათსა და 30 წუთზე მონაცემთა ბაზის არსებულ სარეზერვო ასლს ზემოდან „დააშენდება“ **დიფერენციალური** სარეზერვო ასლი (დიფერენციალური სარეზერვო ასლი მხოლოდ იმ ცვლილებებს ინახავს, რომლებიც მონაცემთა ბაზაში ბოლო სარეზერვო ასლის აღების შემდეგ იქნა განხორციელებული);
- ყოველ კვირა დღეს, ღამის 1 საათზე იქმნება სრული სარეზერვო ასლი მონაცემთა ბაზისთვის HRMain. იმავე სახელის მქონე არსებული სარეზერვო ასლი იშლება;
- ყოველდღე, გარდა კვირისა, ღამის 1 საათზე მონაცემთა ბაზის არსებულ სარეზერვო ასლს ზემოდან „დააშენდება“ **დიფერენციალური** სარეზერვო ასლი;
- ყოველ კვირადღეს, ღამის 2 საათსა და 30 წუთზე სრულდება HRFiles და HRMain-ბაზების სარეზერვო ასლების კოპირება მონაცემთა ქსელურ საცავში (NAS-სერვერი).

აღწერილი ამოცანის შესრულების ინტერფეისი მოცემულია სურათზე.

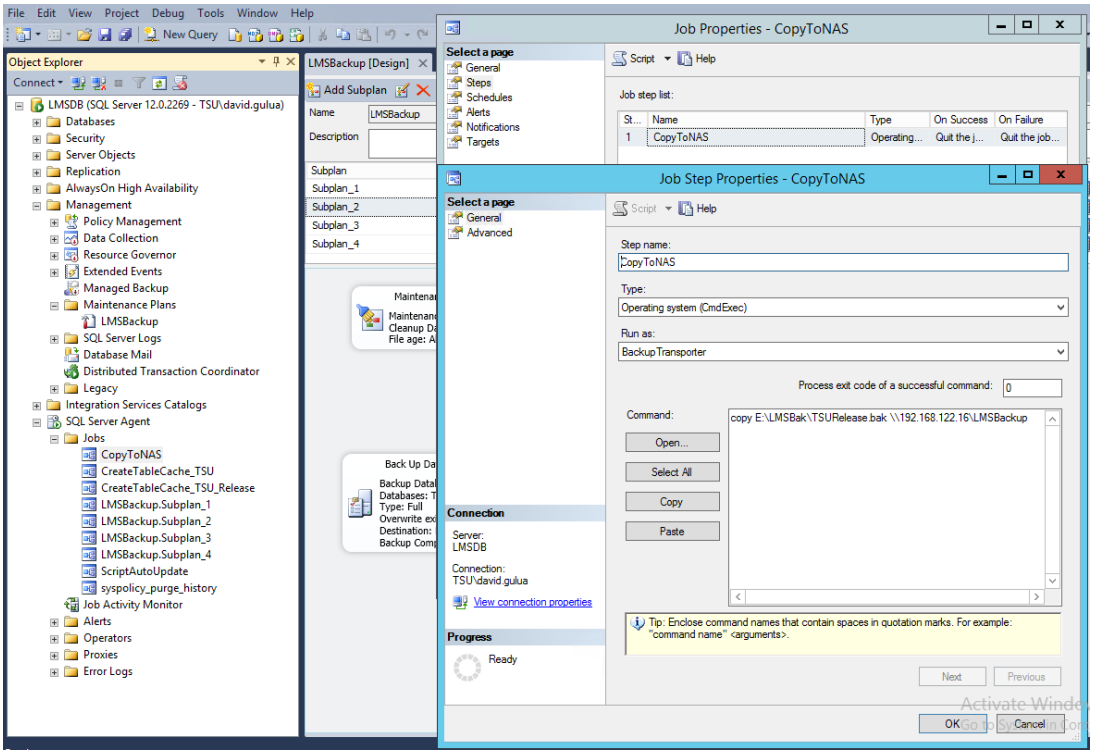


ყოველი ბიჯი თავის შესრულების გეგმით მიეწოდება Microsoft Windows-ის სერვისს SQL Server Agent (SQL Server Agent -> Jobs), რომელიც მათ შესრულებას უზრუნველყოფს. ინფორმაცია შესრულებული სამუშაოს შესახებ ინახება იმავე პროგრამული მოდულის SQL Server Log-განყოფილებაში (სურათი). სურათზე საყურადღებოა ის გარემოება, რომ SQL Server Agent-ის გარემოში შესაძლებელია არამარტო SQL-ის, არამედ ოპერაციული სისტემის ბრძანებათა ინტეგრირებაც,

მაგალითად სარეზერვო ასლების ერთი საცავიდან (მაგ. SQL-ჰოსტი) მეორეზე (მაგ. NAS-სერვერი) კოპირებისთვის. მოვიყვანოთ ორი CMD-ბრძანებისგან შემდგარი სკრიპტი კოპირების ამოცანისთვის, სადაც ბრძანებების გამყოფად „&&“-სიმბოლოების წყვილი გამოიყენება:

copy E:\Bak\HRMain.bak \\192.168.122.16\Backup &&

copy E:\Bak\HRFiles.bak \\192.168.122.16\Backup



სარეზერვო კოპირების ამოცანების შესრულება, ბუნებრივია, შეიძლება გრაფიკული ინტერფეისის გარეშეც, T-SQL-ენაზე შესრულებული სკრიპტის ფორმით. ნახსენები ენა მონაცემთა ბაზებში დაპროგრამების საკმაოდ მძლავრი ინსტრუმენტია, რომელიც მრავალფეროვანი ამოცანების გადაწყვეტის საშუალებას იძლევა. T-SQL-ზე დაწერილი **ტრიგერები** (Triggers) და **შენახული პროცედურები** (Stored Procedures) მონაცემთა ბაზის სერვერზე მიმართული მოთხოვნების უმრავლესობას წარმატებით უმკლავდება.

განვიხილოთ მცირე T-SQL-სკრიპტი, რომლებიც ამ ენაზე წარმოდგენას შეგვიქმნის. პირველ რიგში დავაფიქსიროთ, რომ მონაცემთა ბაზის სერვერი MS SQL Server მართავს მონაცემთა ბაზებს, რომლებიც ოპერაციული სისტემა Windows Server-ის ფაილურ სისტემაში .mdf (მონაცემთა ბაზის ფაილი), .mdl (მონაცემთა ბაზის ინდექსური ფაილი) და .ldf (ტრანზაქციების ლოგ-ფაილი) გაფართოებათა მქონე ფაილების სახითაა წარმოდგენილი. როგორც წესი, ერთ მონაცემთა ბაზას

თითო .mdf და .ldf-ფაილში ინახავენ, თუმცა მათი ოდენობა შეიძლება მეტიც იყოს. MS SQL Server 2012-სთვის მონაცემთა ბაზების სტანდარტულ ადგილსამყოფელს წარმოადგენს ფოლდერი:

%Program FIles%\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA

ჩვენს მიერ ქვემოთ მოყვანილი T-SQL-სკრიპტი მონაცემთა ბაზას სხვა სხვა ადგილას (მაგალითად, არასისტემურ ლოგიკურ დისკზე) გადაიტანს:

ჩვენს მიერ ქვემოთ მოყვანილი T-SQL-სკრიპტი მონაცემთა ბაზას სხვა სხვა ადგილას (მაგალითად, არასისტემურ ლოგიკურ დისკზე) გადაიტანს:

```
-- ბაზის გადაყვანა ოფლაინ-რეჟიმში

ALTER DATABASE TestDB SET single_user  WITH ROLLBACK IMMEDIATE // {SINGLE_USER, RESTRICTED_USER, MULTI_USER}

GO

--ბაზის სახელის შეცვლა

ALTER DATABASE TestDB MODIFY NAME = TestDB1

GO

--ბაზის და ინდექსის ფაილების გადატანა სხვა ადგილას

ALTER DATABASE TestDB1 MODIFY FILE

(NAME = SM_DATA, FILENAME = 'E:\Test_Databases\ TestDB.mdf')

ALTER DATABASE TestDB1 MODIFY FILE

(NAME = SM_LOG, FILENAME = 'E:\Test_Databases\TestDB.LDF')

--ბაზის დაბრუნება ონლაინ-რეჟიმში

ALTER DATABASE TestDB1 SET multi_user

--ALTER DATABASE TestDB SET ONLINE

GO
```

აქვე მოვიყვანოთ T-SQL-ბრძანებები მონაცემთა ბაზის სარეზერვო ასლების შესაქმელად და სარეზერვო ასლიდან ბაზის აღსადგენად:

```
-- სარეზერვო ასლის შექმნა

BACKUP DATABASE master TO DISK = 'c:\master.bak'

GO

--აღდგენა სარეზერვო ასლიდან
```

RESTORE DATABASE master FROM DISK = 'c:\master.bak'

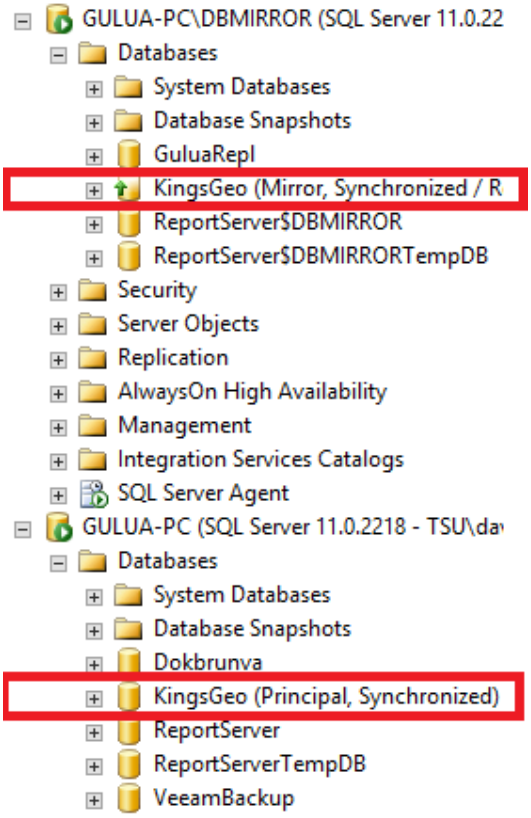
GO

მონაცემთა „სარკული ასახვა“ და რეპლიკაცია SQL-Server-ში

სარკული ასახვის გასამართად მონაცემთა ბაზის ადმინისტრატორის განკარგულებაში უნდა იყოს SQL-Server-ის სხვადასხვა ფიზიკურ ან ვირტუალ ჰოსტებზე განთავსებული მინიმუმ ორი ეგზემპლარი (Instance). მესამე სერვერის საჭიროება წარმოიქმნება მაშინ, როცა ე.წ. „მოწმე-სერვერის“ გამართვაა საჭირო.

საწყის სერვერზე სატესტო მონაცემთა ბაზის შექმნის შემდეგ შეგვიძლია მისი „სარკის“ აგებას შევუდგეთ, რისთვისაც შემდეგი პროცედურების შესრულება იქნება საჭირო:

- 5022-ე და 5023-ე პორტების გახსნა ორივე სერვერის ფაიერვოლში;



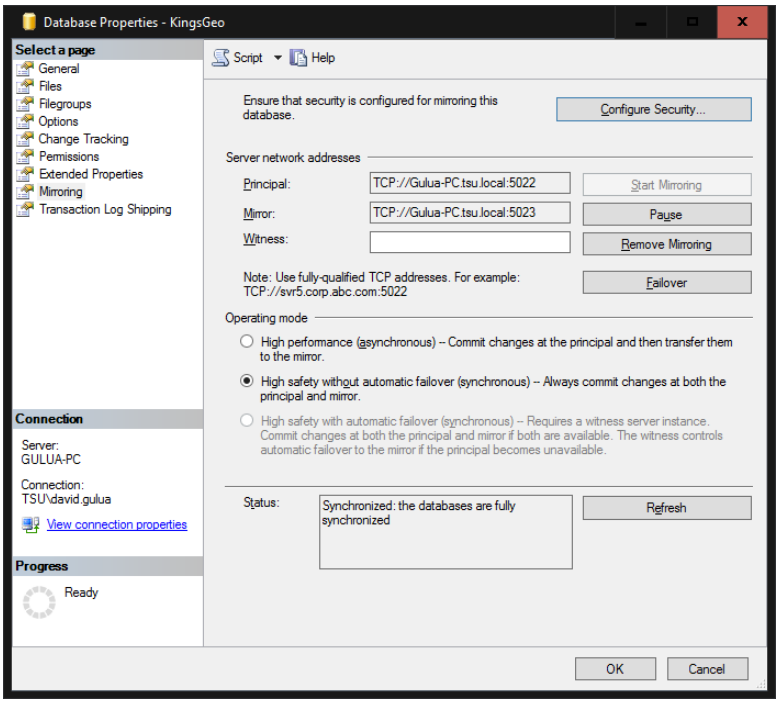
- პირველადი სერვერიდან სასურველი მონაცემთა ბაზის სარეზერვო ასლის შექმნა ბრძანებით: **მაუსის მარჯვენა ღილაკი -> Tasks -> Back Up…;**
- შექმნილი სარეზერვო ასლის აღდგენა სარკე-სერვერზე no recovery ოფციით და მისი მუდმივად restore-რეჟიმში დატოვება ბრძანებით: **მაუსის მარჯვენა ღილაკი -> Tasks -> Restore;**
- Tasks -> Mirror…-დიალოგში ორი ან სამივე სერვერის პარამეტრების მითითება (მათ შორის საკომუნიკავიო 5022-ე პორტისა) და „სარკის“ ამუშავება;

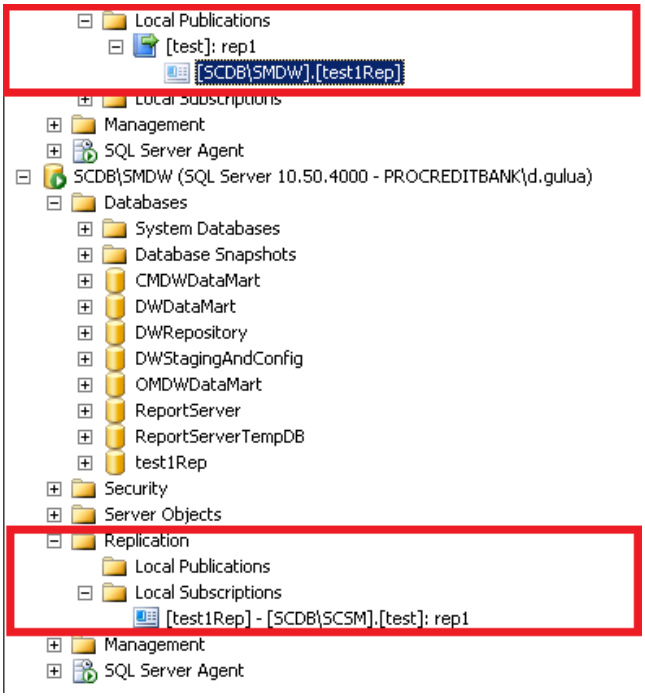
აღნიშნული პროცედურების შესრულების შედეგად „სარკე“ ამუშავდება, რაც ნიშნავს, რომ საწყის მონაცემთა ბაზაში ნებისმიერი ცვლილება ავტომატურად აისახება „სარკე“-ბაზაშიც. ამ უკანასკნელის შიგთავსის დათვალიერება/მოდიფიცირება, ბუნებრივია, არ დაიშვება.

საწყისი და „სარკული“ ბაზების ნიმუში მოცემულია სურათზე.

საწყისი მონაცემთა ბაზა (ქვემოთ) და მისი "სარკე"

ბრძანება Failover („ჩავარდნის აღმოფხვრა“) საჭიროების შემთხვევაში (მთავარი სერვერის დაზიანებისას ან მასზე გეგმიური სამუშაოების შესრულებისას) მართვას „სარკე-სერვერს“ და მონაცემთა ბაზასთან მიმართვა გაგრძელდება შეუფერხებლად.





რეპლიკაციის ნიმუში MS SQL Server-ში

განხილულ იქნა თანამედროვე ინფორმაციულ ტექნოლოგიებში ერთერთი ყველაზე „მტკივნეული“ საკითხი: ინფორმაციის საიმედო შენახვა. ელექტრონულ მატარებლებზე ინფორმაციის გადატანის მზარდი ტენდენცია, ერთი მხრივ, მკვეთრად აჩქარებს მასთან მიმართვას, თუმც მეორე მხრივ, ზრდის მისი დაკარგვის რისკებს. თანამედროვე ინფორმაციულ ტექნოლოგიებს ამგვარ რისკებთან გამკლავების მრავალფეროვანი საშუალებები გააჩნიათ, ამიტომ სწორად დაგეგმილი პროცესების განხორციელებისას თვით სტიქიური უბედურებებიც ვერ იქცევა ინფორმაციული სისტემების გაჩერებისა და მონაცემთა დაკარგვის მიზეზად.

MS SQL Server წარმოადგენს სისტემას, სადაც მონაცემთა საიმედო დაცვა უაღრესად მაღალ დონეზეა აყვანილი. სისტემის ყოველი ახალი ვერსია საიმედობის დაცვის უფრო განვითარებულ საშუალებებს სთავაზობს მომხმარებლებს და ალბათ ეს გარემოებაც მნიშვნელოვნად განაპირობებს იმას, რომ გავრცელების მასშტაბებით SQL Server მონაცემთა ბაზების მართვის სისტემების რეტინგთა მოწინავე ხუთეულში მუდამ სტაბილურადაა წარმოდგენილი, ხოლო საქართველოში ყველაზე პოპულარულ მბმს-ს წარმოადგენს.

ანდრო გოცირიძე - კიბერუსაფრთხოების საგანმანათლებლო კვლევითი ცენტრის CYSEC დამფუძნებელი

კიბერსივრცე - დაპირისპირების მეხუთე დომეინი

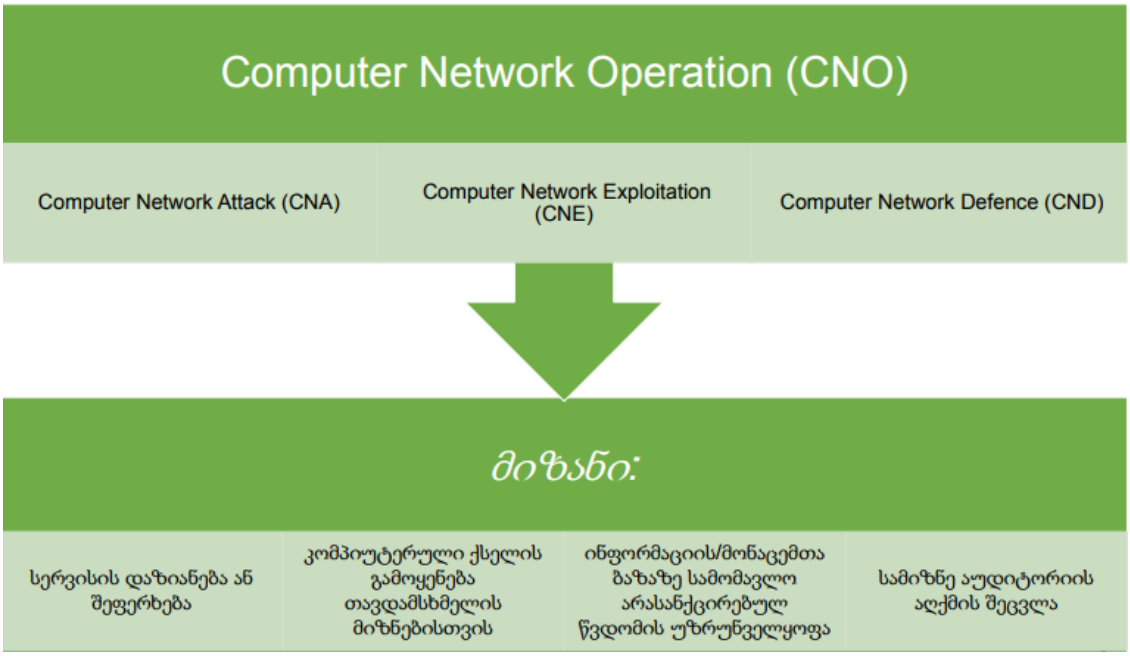
საქართველოს კიბერსივრცეში არსებული საფრთხეები: ქმედებები, აქტორები, შეფასება; კიბერელემენტების გამოყენება თანამედროვე კონფლიქტებში: კიბერკონფლიქტის ტრანსფორმაცია ესტონეთიდან აშშ არჩევნებამდე; კიბერსივრცის გამოყენება საინფორმაციო-ფსიქოლოგური ზემოქმედებისათვის: „ინფორმაციული კონფრონტაცია“, ძირითადი მიმართულებები და მიზნები, საშუალებები, გავრცელება კიბერარხებით, ქეისები;

კიბერჰიგიენა: კომპიუტერული უსაფრთხოების მინიმალური წესები საჯარო სექტორის მომხმარებლისთვის

- მავნე პროგრამული უზრუნველყოფა და მისი სახეები;

- სამუშაო კომპიუტერის უსაფრთხოება;
- ელექტრონული ფოსტის უსაფრთხოება;
- ფიშინგი;
- პასვორდის უსაფრთხოება;
- უსაფრთხო ინტერნეტი მოგზაურობისას;
- უკაბელო ინტერნეტის უსაფრთხოება;
- მობილური მოწყობილობების უსაფრთხოება;
- უსაფრთხო ონლაინ - ბანკინგი და შოპინგი;
- სოციალური ქსელების უსაფრთხოება;
- ID მოპარვა და ინტერნეტ-თაღლითობა;

ბუნებრივი, შემთხვევითი, მიზანმიმართული ინციდენტები და ინფორმაციული ტექნოლოგიების გამოყენება დესტრუქციული მიზნებისათვის სხვადასხვა წყაროს მიერ. კრიტიკული ინფორმაციული სისტემების გამართული ფუნქციონირების შეფერხება მიზანმიმართული კიბერშეტევის მიერ კოლოსალური თანხების გამოყოფა კიბერშესაძლებლობების გასაუმჯობესებლად და კვალიფიციური პერსონალის აღსაზრდელად.



საკანონმდებლო ბაზა და საქართველოს კიბერარქიტექტურა კიბერდანაშაულთან ბრძოლის ევროპული კონვენცია (CETS 185) – 01/07/ 2004.

2001 წლის 23 ნოემბერს ბუდაპეშტში ხელი მოეწერა კიბერდანაშაულთან ბრძოლის ევროპულ კონვენციას (CETS 185)133 , რომელიც ძალაში შევიდა 2004 წლის 1 ივლისს. კონვენცია მომზადდა ევროპის საბჭოს ფარგლებში კანადის, შეერთებული შტატების, იაპონიისა და სამხრეთ აფრიკის რესპუბლიკის მონაწილეობით. დღესდღეისობით ეს კონვენცია არის მოცემულ სფეროში ერთადერთი აღიარებული იურიდიული დოკუმენტი, რომელიც მიღებულია საერთაშორისო დონეზე და ის არის ღია ყველა დაინტერესებული ქვეყნისთვის. ასევე საინტერესოა კონვენციაზე დამატებით მიღებული პროტოკოლი (CETS 189)134 კომპიუტერულ ქსელებში ქსენოფობიისა და რასიზმის ნიადაგზე ჩადენილი დანაშაულების შესახებ, რომელსაც ხელი მოეწერა 2003 წლის იანვარში და ძალაში შევიდა 2006 წლის მარტის თვეში. კონვენცია ხელმომწერ ქვეყნებს ავალდებულებს შექმნან სამართლებრივ - ნორმატიული ბაზა აუცილებელი კიბერდანაშაულის პრობლემის ეფექტური გადაწყვეტისთვის. ასევე ყველა ხელმომწერი ქვეყანა თავის თავზე იღებს ერთმანეთისთვის დახმარების აღმოჩენას კიბერდამნაშავეთა სამართლებრივი დევნისა და ინციდენტების გამოძიების საკითხში. ევროპული კონვენცია არის ერთერთი პირველი საერთაშორისო დოკუმენტი, სადაც განსაზღვრულია და კლასიფიცირებულია კიბერდანაშაული. ხუთ ქვეყანას მიეცა რეკომენდაცია და გაუკეთდა შეთავაზება მიუერთდეს კონვენციას. ისეთმა დიდმა ქვეყნებმა, როგორებიცაა ჩინეთი და რუსეთი უარი თქვეს ხელი მოეწერათ კონვენციაზე და მიერთებოდნენ მას ევროპული კონვენცია გამოიყენება როგორც სახელმძღვანელო და ცნობარი მსოფლიოს ასზე მეტი ქვეყნის სტანდარტული ან

ტიპიური საკანონმდებლო ბაზისათვის. გარდა ამისა, კონვენცია მხარს უჭერს ყველა სხვა ორგანიზაციას, რომლებიც იყენებენ მას თავიანთი გადაწყვეტილების მიღებაში. ეს ორგანიზაციებია ევროპის კავშირი, ამერიკის სახელმწიფოთა ორგანიზაცია (OAS)138 , ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაცია (OECD)139 , აზია - წყნარი ოკეანის ეკონომიკური თანამშრომლობის ორგანიზაცია (APEC)140 , ინტერპოლი, ასევე კერძო სექტორის წარმომადგენლები. მიუხედავად იმისა, რომ მოცემულ კონვენციას აქვს ფართო საერთაშორისო აღიარება, ზოგიერთი ქვეყანა მაინც ამტკიცებს, რომ კონვენცია ითვალისწინებს კიბერდანაშაულის აღსაკვეთად საჭირო არასაკმარის ზომებს, და რამაც შეიძლება დიდი ზიანი მიაყენოს ეროვნულ უსაფრთხოებას. პირველ რიგში, კონვენცია კომპიუტერულ ქსელზე განხორციელებულ შეტევას განიხილავს როგორც კერძო და სახელმწიფო საკუთრების წინააღმდეგ ჩადენილ დანაშაულს, და არა როგორც ეროვნული უსაფრთხოების საფრთხეს. მეორე, კონვენცია ერთმანეთისგან არ ანსხვავებს შეტევებს ჩვეულებრივი კომპიუტერული ქსელებსა და კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტებს შორის, ისევე როგორც ფართომასშტაბიან და ლოკალურ შეტევებს შორის. თუმცა კონვენცია წარმოადგენს სტანდარტულ დოკუმენტს, რომელიც წარმოადგენს საერთაშორისო კანონმდებლობის ძალზედ მნიშვნელოვან შემადგენელ ნაწილს. მასში მოცემულია იურიდიული და ტექნიკური ნორმების ოპტიმალური კომპლექსი, რომელიც შეიძლება გამოყენებულ იქნას ამ სფეროში საერთაშორისო თანამშრომლობის გაფართოებაზე დამატებითი შეთანხმებების დამუშავების მიზნით. გამომდინარე, რომ კიბერდანაშაულს, კიბერტერორიზმსა და კიბერომს გააჩნიათ ბევრი საერთო ნიშანი და მახასიათებელი, კონვენცია ნებისმიერ კიბერშეტევაზე, მიუხედავად მათი მოტივაციისა, ითვალისწინებს, რომ მასზე ხელმომწერმა ქვეყნებმა პასუხისმგებელი უწყებების მოთხოვნაზე უნდა დააკავონ და გადასცენ ყველა კიბერდამნაშავე სამართალდამცავ ორგანოებს, მიუხედავად იმისა, განიხილებიან თუ არა ისინი საკუთარ ქვეყნებში როგორც დამნაშავეები, ტერორისტები ან კიდევ პატრიოტები.

კანონი „ინფორმაციული უსაფრთხოების შესახებ“

ინფორმაციული უსაფრთხოების წესები 1. კრიტიკული ინფრასტრუქტურის სუბიექტი ვალდებულია მიიღოს შიდასამსახურებრივი გამოყენების წესები, რომელიც ემსახურება ამ კანონის დებულებათა აღსრულებას და განსაზღვრავს ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკას. 2. ინფორმაციული უსაფრთხოების პოლიტიკა უნდა აკმაყოფილებდეს ინფორმაციული უსაფრთხოების მინიმალურ მოთხოვნებს სუბიექტის კრიტიკულობის კლასიფიცირების გათვალისწინებით, რომელსაც განსაზღვრავს საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი საჯარო სამართლის

იურიდიული პირი – მონაცემთა გაცვლის სააგენტო (შემდგომში: მონაცემთა გაცვლის სააგენტო) სტანდარტიზაციის საერთაშორისო ორგანიზაციისა (ISO) და ინფორმაციული სისტემების აუდიტისა და კონტროლის ასოციაციის (ISACA) მიერ დადგენილ სტანდარტებსა და მოთხოვნებთან შესაბამისობაში. 3. კრიტიკული ინფრასტრუქტურის სუბიექტი ვალდებულია წარუდგინოს მონაცემთა გაცვლის სააგენტოს მიღებული ინფორმაციული უსაფრთხოების პოლიტიკა, ისევე როგორც მასში განხორციელებული ნებისმიერი ცვლილება.

კიბერ უსაფრთხოების უზრუნველყოფა. კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფი:

1. ამ კანონის დებულებათა აღსრულებას, კერძოდ, ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვას საქართველოს კიბერ–სივრცეში, ასევე ინფორმაციული უსაფრთხოების კოორდინაციაზე მიმართულ სხვა, დაკავშირებულ საქმიანობას, რომელიც ინფორმაციული უსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრას ემსახურება, ახორციელებს მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფი – cert.gov.ge (შემდგომში – სწრაფი რეაგირების ჯგუფი).
2. კიბერ უსაფრთხოების პრიორიტეტულ საფრთხეებს მიეკუთვნება: ა. კიბერ–შეტევა, რომელიც საფრთხის ქვეშ აყენებს ადამიანთა სიცოცხლეს და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას; ბ. კიბერ–შეტევა კრიტიკული ინფრასტრუქტურის ინფორმაციული სისტემის წინააღმდეგ; გ. კიბერ–შეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურებს ან/და საკუთრების უფლებას; დ. სხვა ნებისმიერი ქმედება, რომელიც, მისი ხასიათიდან, მიზნიდან,

წყაროდან, მოცულობიდან, რაოდენობიდან ან მისი აღკვეთისათვის საჭირო რესურსების ოდენობიდან გამომდინარე, საკმარისი საფრთხის შემცველია კრიტიკული ინფრასტრუქტურის ნორმალური ფუნქციონირებისათვის.

3. სწრაფი რეაგირების ჯგუფის მოვალებებში შედის: ა. კრიტიკული ინფრასტრუქტურის ინფორმაციული უსაფრთხოების დაცვის თაობაზე რეკომენდაციების გაცემა; ბ. კომპიუტერული ინციდენტების დროული გამოვლენა; გ. კომპიუტერულ ინციდენტებზე რეაგირება და მათზე რეაგირების კოორდინაცია; დ. კომპიუტერული ინციდენტების აღრიცხვა და მათზე რეაგირების პრიორიტეტების დადგენა/კატეგორიზაცია; ე. კომპიუტერული ინციდენტების ანალიზი; ვ. დახმარების გაწევა კომპიუტერული ინციდენტის შედეგების გამოსწორებისა და ზიანის მინიმიზაციის პროცესში; ზ. კომპიუტერული ინციდენტების პრევენციაზე მიმართული ზომების კოორდინაცია და დახმარების გაწევა ამგვარი ზომების დანერგვაში; თ. ცნობიერიების ამაღლება ინფორმაციული უსაფრთხოების საკითხებში, მათ შორის ინფორმაციის მიწოდება კრიტიკული ინფრასტრუქტურის ინფორმაციულ სისტემებში არსებული საფრთხეებისა და სუსტი წერტილების შესახებ, თუ ინფორმაციის ამგვარი ხელმისაწვდომობა ზიანს არ აყენებს ინფორმაციულ უსაფრთხოებას; ი. მომხმარებელთა ფართო წრისათვის გაფრთხილებისა და ინფორმაციის მიწოდება შესაძლო საფრთხეების შესახებ; კ. საგანმანათლებლო და ინფორმაციული უზრუნველყოფა ინფორმაციული უსაფრთხოების საკითხებში; ლ. ინფორმაციული უსაფრთხოების საკითხების წარმომადგენლობა და კოორდინაცია საერთაშორისო დონეზე; მ. სხვა ფუნქციები, რომელიც დაკავშირებულია ინფორმაციული უსაფრთხოების მიზნებთან და განისაზღვრება კანონით ან სხვა ნორმატიული აქტით.
4. სწრაფი რეაგირების ჯგუფს უფლება აქვს, მოითხოვოს წვდომა კრიტიკული ინფრასტრუქტურის სუბიექტის ინფორმაციულ აქტივზე, ინფორმაციულ სისტემაზე ან/და ინფორმაციულ ინფრასტრუქტურაში შემავალ საგანზე, თუ ამგვარი წვდომა აუცილებელია მიმდინარე ან მომხდარი კომპიუტერული ინციდენტზე სათანადო რეაგირებისათვის. კრიტიკული ინფრასტრუქტურის სუბიექტის ინფორმაციული უსაფრთხოების ოფიცერი, მოთხოვნის გონივრულ ვადაში განხილვის შედეგად, სწრაფი რეაგირების ჯგუფს დაუყოვნებლივ აცნობებს შესაბამისი წვდომის შესაძლებლობის თუ შეუძლებლობის შესახებ.
5. სწრაფი რეაგირების ჯგუფის კომპეტენცია, მუშაობის პროცედურები, რეაგირების მექანიზმები და საქმიანობის სხვა წესები განისაზღვრება მონაცემთა გაცვლის სააგენტოს ნორმატიული აქტით.

საქართველოს კიბერუსაფრთხოების სტრატეგია გამოქვეყნდა 2013 წლის 20 მაისს, საქართველოს პრეზიდენტის 2013 წლის 17 მაისის №321 ბრძანებულების მიღების თანახმად. მოცემული დოკუმენტი შემუშავდა საქართველოს ეროვნული უშიშროების საბჭოსთან არსებული ეროვნული უსაფრთხოების სტრატეგიული დოკუმენტების შემუშავების მაკოორდინირებელი მუდმივმოქმედი საუწყებათაშორისო კომისიის მიერ და ის წარმოადგენს არამარტო სტრატეგიას, არამედ მასში მოცემულია ასევე ამ სტრატეგიის განხორციელების 2013 – 2015 წ.წ. სამოქმედო გეგმაც.

„საქართველოს კიბერუსაფრთხოების სტრატეგია არის კიბერუსაფრთხოების სფეროში სახელმწიფო პოლიტიკის განმსაზღვრელი ძირითადი დოკუმენტი, რომელიც ასახავს სტრატეგიულ მიზნებს, ძირითად პრინციპებს, აყალიბებს სამოქმედო გეგმებს და ამოცანებს. სტრატეგიაზე დაყრდნობით, საქართველოს ხელისუფლება გაატარებს ღონისძიებებს, რომლებიც ხელს შეუწყობს სახელმწიფო ორგანოების, კერძო სექტორისა და სამოქალაქო საზოგადოების კიბერსივრცეში დაცულად ფუნქციონირებას, ელექტრონული ოპერაციების უსაფრთხო განხორციელებას და ქვეყანაში ეკონომიკისა და ბიზნესის შეუფერხებლად მოქმედებას“. სანამ სტრატეგიის განხილვაზე გადავიდოდეთ, ვნახოთ კანონში „ინფორმაციული უსაფრთხოების შესახებ“ თუ როგორი განსაზღვრება აქვს იმ ძირითად საკითხებს, რაც უშუალო კავშირშია კუბერუსაფრთხოების უზრუნველყოფასთან. კერძოდ: „კრიტიკული ინფორმაციული სისტემა - ინფორმაციული სისტემა, რომლის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოების ნორმალური ფუნქციონირებისათვის“ და „კრიტიკული ინფორმაციული სისტემის სუბიექტი - სახელმწიფო ორგანო ან იურიდიული პირი, რომლის ინფორმაციული სისტემის უწყვეტი ფუნქციონირება მნიშვნელოვანია ქვეყნის თავდაცვისათვის ან/და ეკონომიკური უსაფრთხოებისათვის, სახელმწიფო ხელისუფლების ან/და საზოგადოებრივი

ცხოვრების შენარჩუნებისათვის“. საქართველოს ეროვნული უსაფრთხოების კონცეფცია კიბერსივრცის დაცვის უზრუნველყოფასა და ზოგადად კიბერუსაფრთხოებას განიხილავს, როგორც ქვეყნის უსაფრთხოების ერთ - ერთ ძირითად შემადგენელ ნაწილსა და მის მნიშვნელოვან მიმართულებას. კიბერსივრცის დაცვასა და კიბერუსაფრთხოების უზრუნველყოფაზე ბევრად არის დამოკიდებული ქვეყნის შემდგომი ეკონომიკური სტაბილურობა და სოციალური განვითარება. მოცემული მიზნის მისაღწევად, სტრატეგია განიხილავს შემდეგი თანამშრომლობის მნიშვნელოვან პრინციპებს:

- საქართველოს მთავრობის ერთიანი მიდგომა;
- თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის;
- აქტიური საერთაშორისო თანამშრომლობა;
- ინდივიდუალური პასუხისმგებლობა;
- ადეკვატური ზომები.

სტრატეგიის მთავარი მიზანია კიბერშეტევის ან სხვა ქმედებების საზიანო შედეგები და რისკები მაქსიმალურად იქნას შემცირებული და უმოკლეს დროში მოხდეს დაზიანებული ინფორმაციული ინფრასტრუქტურის სრული აღდგენა. ყოველივე ამას ემატება კრიტიკული ინფორმაციული სისტემების მდგრადობისა და დაცულობის ამაღლება, ასევე დროული პრევენცია. გლობალური ინტერნეტ სივრცის მუდმივი განვითარება და მასთან დაკავშირებული არსებული საფრთხეები, საქართველოს კიბერსივრცესა და შესაბამისად კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემის გამართულ ფუნქციონირებას მუდმივად ახალი გამოწვევების წინაშე აყენებს. სტრატეგიის თანახმად, ინფორმაციული სისტემის კრიტიკულობა და კიბერუსაფრთხოების მდგრადობა განისაზღვრება ისეთი კრიტერიუმებით, როგორიცაა მოსალოდნელი მატერიალური ზარალის სიმძიმე და მასშტაბები, ინფორმაციული სისტემის აუცილებლობა სახელმწიფოსა და საზოგადოების ნორმალური ფუნქციონირება, სისტემის მომხმარებელთა რაოდენობა და კიბერუსაფრთხოების სათანადო დონის უზრუნველყოფა საჭირო რესურსებით.

საერთაშორისო სისტემაში არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით, საქართველოს უსაფრთხოების პოლიტიკის დაგეგმვა და განხორციელება განიხილავს კიბერუსაფრთხოების სფეროში შემდეგ საფრთხეებსა და გამოწვევებს:

- კიბერომი ან/და კიბერშეტევა, რომელიც მიმართულია პოტენციური მოწინააღმდეგის მხრიდან საქართველოს მთლიანი კიბერსივრცის დაზიანებისა და მწყობრიდან გამოყვანისკენ. ამასთან, ქვეყანა კვლავ დგას მასიური კიბერშეტევის საფრთხის წინაშე;

- კიბერტერორიზმი, რომელმაც კრიტიკულ ინფორმაციულ ინფრასტრუქტურაზე კიბერშეტევით შეიძლება მნიშვნელოვანი ზიანი მიაყენოს ქვეყნის ეროვნულ უსაფრთხოებას;
- კიბერსივრცის გამოყენებით ჩადენილი სხვა ქმედებები, რომელმაც შეიძლება ზიანი მიაყენოს კრიტიკული ინფორმაციული ინფრასტრუქტურის ცალკეულ სუბიექტებს, რაც გამოიწვევს ეკონომიური, სოციალური თუ სხვა სფეროს ფუნქციონირების უარყოფით შედეგებს.

სტრატეგიაში განხილულია ასევე საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიმართულებები:

- კვლევა და ანალიზი;
- ახალი საკანონმდებლო - ნორმატიული ბაზა;
- კიბერუსაფრთხოების უზრუნველყოფის ინსტიტუციური კოორდინაცია;
- საზოგადოებრივი ცნობიერების ამაღლება და საგანამანმათლებლო ბაზის ჩამოყალიბება;
- საერთაშორისო თანამშრომლობა.

ძალზედ მნიშვნელოვანია, რომ კიბერუსაფრთხოების და მასთან დაკავშირებული ქმედებები, იქნება ეს სამართლებრივი და ნორმატიული აქტები, სხვადასხვა ინიციატივები, რეკომენდაციები, ინსტრუქციები, ასევე კიბერსივრცეში მიმდინარე

პროცესები, ემყარებოდეს კვლევებსა და ანალიზს, რომელიც უზრუნველყოფს არამარტო კიბერუსაფრთხოების პოლიტიკის ეფექტიანობასა და კრიტიკული ინფორმაციული ინფრასტრუქტურის სისტემის ნორმალურ ფუნქციონირებას, არამედ ასევე დადებითად აისახება მთლიანად ეროვნული უსაფრთხოების პოლიტიკაზე. სტრატეგიის მიხედვით, კვლევა და ანალიზი აუცილებელია განხორციელდეს შემდეგი მიმართულებებით:

- სხვა ქვეყნების საუკეთესო პრაქტიკის შესწავლა და გამოცდილების გაზიარება;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის ობიექტების იდენტიფიცირების კრიტერიუმებისა და სტანდარტების კვლევა;
- კრიტიკული ინფორმაციული ინფრასტრუქტურის მდგრადობის ანალიზი;
- კიბერუსაფრთხოების სფეროში რეგიონში არსებული პრობლემატიკის შესწავლა;
- კიბერუსაფრთხოების განმსაზღვრელი სტანდარტების შემუშავება მათი შემდგომი დანერგვის მიზნით;
- საქართველოს კიბერსივრცის წინაშე მდგარი საფრთხეების და რისკების გამოვლენაზე წინადადებების პერიოდული მომზადება.

მიუხედავად მსოფლიოში არსებული ახალი გამოწვევებისა, საფრთხეებისა და პოტენციური მოწინააღმდეგების არსებობისა, დღევანდელი მდგომარეობით საქართველოს კიბერუსაფრთხოების სფეროში არ გააჩნია ეროვნული კანონმდებლობა. აუცილებელი და მნიშვნელოვანია საკანონმდებლო ბაზის შექმნა, რომელიც შესაბამისობაში იქნება მოსული საერთაშორისო სტანდარტებთან და ხელს შეუწყობს მოცემული სფეროს განვითარებას. სტარტეგიის მიხედვით, სამართლებრივი ბაზის შექმნისა და მისი სრულყოფისათვის აუცილებელია გატარდეს შემდეგი ღონისძიებები:

- კიბერუსაფრთხოების საკითხებზე საერთაშორისო ურთიერთობების განმტკიცება ამ სფეროში მომუშავე საერთაშორისო ორგანიზაციებთან (OECD, EU, OSCE, CoE, UN, ITU)41 და სახელმწიფო ორგანოებთან;
- კიბერუსაფრთხოების სფეროში საერთაშორისო ინიციატივებში აქტიური მონაწილეობის მიღება და ამ ინიციატივების რეგიონის მასშტაბით მხარდაჭერა;
- სხვა ქვეყნების CERT - ებთან კიბერუსაფრთხოების სფეროში ორმხრივ და მრავალმხრივ ფორმატებში თანამშრომლობის ინიცირება.

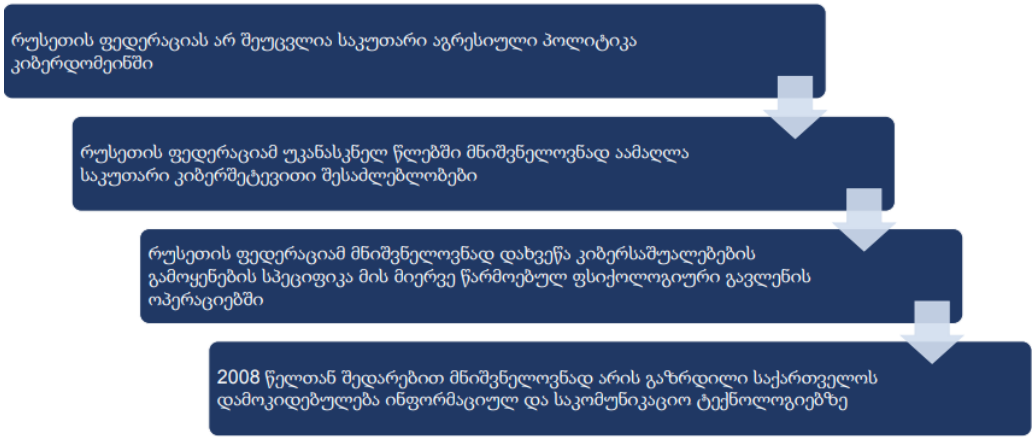
საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიზნები და პრინციპები:

- კიბერუსაფრთხოება როგორც ეროვნული უსაფრთხოების განუყოფელი ნაწილი
- ადამიანის უფლებათა და ძირითად თავისუფლებათა განუხრელი დაცვა და პატივისცემა
- საქართველოს მთავრობის ერთიანი მიდგომა თანამშრომლობა სახელმწიფო და კერძო სექტორებს შორის
- აქტიური საერთაშორისო თანამშრომლობა ინდივიდუალური პასუხისმგებლობა ადეკვატური ზომები

კიბერსაფრთხეები

„კიბერსივრცის“ ტერმინის განსაზღვრების ბევრი ვარიანტი არსებობს. თითოეული მათგანი იძლევა თავისებურ განმარტებას. თუმცა ყველა განმარტებაში განსაზღვრულია, რომ „კიბერსივრცე“ ეს არის ინფორმაციული და ტექნოლოგიური ინფრასტრუქტურის ურთიერთკავშირში არსებული კომპლექსი, სადაც შედის გლობალური ინტერნეტისა და ტელეკომუნიკაციის ქსელები, კომპიუტერული სისტემები, ასევე ჩართული პროცესორები, სერვერები და მაკონტროლირებელი მოწყობილობები, რომლებიც გამოიყენება მრეწველობის სხვადასხვა დარგში.

ახალი ტექნოლოგიების განვითარებასთან ერთად იზრდება საფრთხეები, რომლებიც დიდ ზიანს აყენებს კიბერსივრცეს და მის მომხმარებელს. სახელმწიფოს და სახელისუფლებო ორგაონოებს პირველ რიგში ადარდებთ ეროვნული უსაფრთხოების უზრუნველყოფა, კრიტიკული ინფორმაციისა და ინფორმაციული ინფრასტრუქტურის დაცვა როგორც უცხო სახელმწიფოს, ისე არასამთავრობო სუბიექტებისა და დაჯგუფებების მხრიდან ხელყოფისგან, რათა თავიდან იქნას აცილებული ინფორმაციის მოპარვა ან/და გადაცემა, ქსელის დაზიანება ან/და საერთოდ განადგურება. სახელმწიფოს უსაფრთხოების რეალურ საფრთხეს წარმოადგენს კიბერშეტევები, რომლებიც მიმართულია ისეთი სასიცოცხლო მნიშვნელობის მქონე ინფრასტრუქტურის განადგურებისკენ, როგორებიცაა სატელეკომუნიკაციო ქსელების, ენერგოგენერირებისა და ნავთობგადამამუშავებელი სიმძლავრეების სისტემები, ასევე ელექტრომომარაგების, საფინანსო, ჯანდაცვისა და სატრანსპორტო სისტემები.



საფრთხისშემცველი ქმედებები

საერთაშორისო სისტემაში არსებული საფრთხეებისა და გამოწვევების გათვალისწინებით, საქართველოს უსაფრთხოების პოლიტიკის დაგეგმვა და განხორციელება განიხილავს კიბერუსაფრთხოების სფეროში შემდეგ საფრთხეებსა და გამოწვევებს:

- კიბეროში ან/და კიბერშეტევა, რომელიც მიმართულია პოტენციური მოწინააღმდეგის მხრიდან საქართველოს მთლიანი კიბერსივრცის დაზიანებისა და მწყობრიდან გამოყვანისკენ. ამასთან, ქვეყანა კვლავ დგას მასიური კიბერშეტევის საფრთხის წინაშე;
- კიბერტერორიზმი, რომელმაც კრიტიკულ ინფორმაციულ ინფრასტრუქტურაზე კიბერშეტევით შეიძლება მნიშვნელოვანი ზიანი მიაყენოს ქვეყნის ეროვნულ უსაფრთხოებას;

- კიბერსივრცის გამოყენებით ჩადენილი სხვა ქმედებები, რომელმაც შეიძლება ზიანი მიაყენოს კრიტიკული ინფორმაციული ინფრასტრუქტურის ცალკეულ სუბიექტებს, რაც გამოიწვევს ეკონომიური, სოციალური თუ სხვა სფეროს ფუნქციონირების უარყოფით შედეგებს.

საქართველოს კიბერუსაფრთხოების პოლიტიკის ძირითადი მიმართულებები

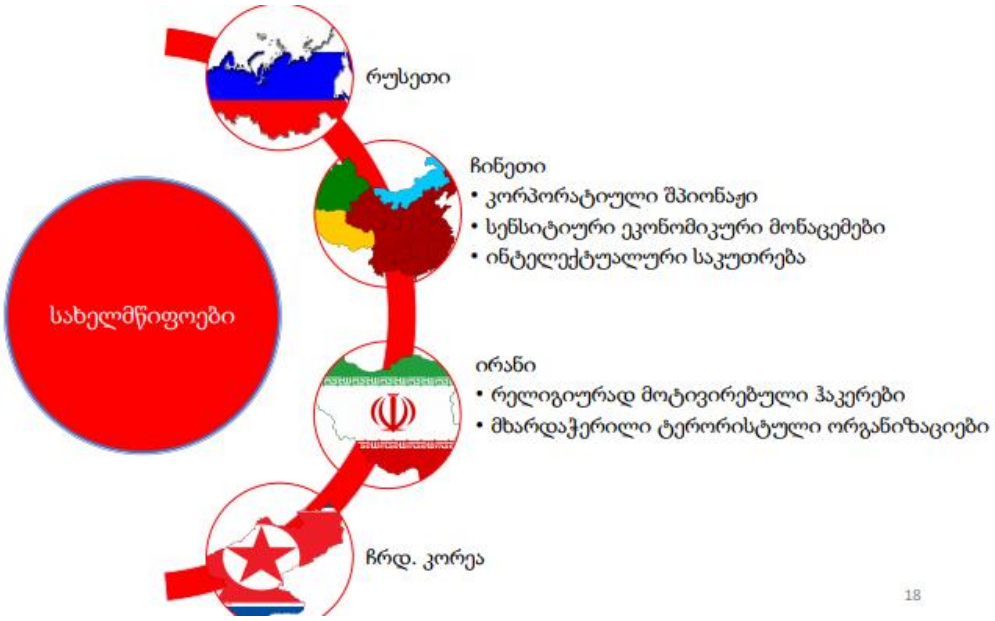
- კვლევა და ანალიზი;
- ახალი საკანონმდებლო - ნორმატიული ბაზა;
- კიბერუსაფრთხოების უზრუნველყოფის ინსტიტუციური კოორდინაცია;
- საზოგადოებრივი ცნობიერების ამაღლება და საგანამანმათლებლო ბაზის
- ჩამოყალიბება;
- საერთაშორისო თანამშრომლობა.

აქტორები

კიბერსაფრთხეების წარმოშობის წყაროებს წარმოადგენენ როგორც სახელმწიფო და კერძო სექტორის წარმომადგენლები, ისე სხვადასხვა სახისა და ნიშნით შექმნილი ორგანიზაციები და ფიზიკური პირები. შეერთებული შტატების კონტროლის პალატის მასალების მიხედვით, კიბერსაფრთხეების წარმოშობის წყაროები შეიძლება დავაკვალიფიციროთ შემდეგნაირად, კერძოდ:

სახელმწიფო - უცხოეთის ქვეყნების სადაზვერვო სამსახურები კომპიუტერულ ტექნოლოგიებს იყენებენ ინფორმაციის შეგროვებისა და ჯაშუშობისთვის. მსგავსი ქმედებები სადაზვერვო სამსახურების მხრიდან შეიძლება მიმართული იყოს როგორც მეგობარი, ისე მოწინააღმდეგე ქვეყნების მიმართ, ან არასახელმწიფო

სუბიექტების წინააღმდეგ. სახელმწიფო თავისი სადაზვერვო სამსახურების გამოყენებით, ახორციელებს კიბერშეტევებს პოტენციური მოწინააღმდეგე სახელმწიფოების მიმართ დეზინფორმაციის, დესტაბილიზაციის, დაშინების ან ფართომასშტაბიანი კიბერომის წარმოების მიზნით. ასევე საყურადღებოა ის გარემოება, რომ ხშირად ხდება პიროვნების უსაფრთხოებისა და უფლებების დარღვევა. კერძოდ, სახელმწიფოს სპეციალურმა სამსახურებმა შეიძლება მიმართონ ისეთ ქმედებებს, რომელთა გამოყენებითაც ხდება მოქალაქეთა პერსონალური მონაცემების გადაჭერა, მოპარვა და გამოყენება. მსგავსი ქმედებები ხშირ შემთხვევაში ხდება სასამართლოს შესაბამისი ორგანოების სანქციისა და სწორი დემოკრატიული კონტროლის გარეშე;



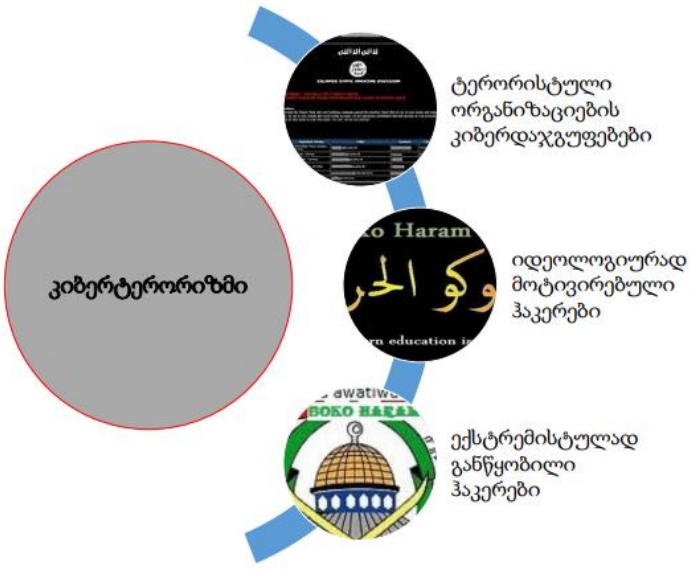
კომპანიები - დაკავებულნი არიან სამრეწველო/კორპორაციული ჯაშუშობითა და/ან დივერსიული საქმიანობით, რაშიც ისინი ხშირად იყენებენ ჰაკერებსა და ორგანიზებულ დამნაშავეთა ჯგუფებს. კომპანიების, კორპორაციებისა და კერძო სექტორის სხვა წარმომადგენლებს ასევე შეუძლიათ დაარღვიონ ადამიანის უფლებები პიროვნების პერსონალური მონაცემების შეგროვებისა და ანალიზის გზით, ან ზოგ შემთხვევაში მოცემული მონაცემების სახელმწიფო ორგანოებთან ან სხვა დაინტერესებულ პირებთან გაცვლით;

ჰაკერები - იყო დრო როცა ჰაკერების მხრიდან ქსელებში არასანქცირებული შეღწევა ან პროგრამების გატეხვა დაკავშირებული იყო ჰაკერთა საზოგადოებაში ავტორიტეტის მოპოვებასთან ან წვრილმან ჰულიგნობასთან. დღესდღეისობით სურათი კარდინალურად არის შეცვლილი, კერძოდ ჰაკერთა უმრავლესობის ქმედება ატარებს კრიმინალურ ხასიათს. ადრე თუ ჰაკერებისთვის ქსელის

გატეხვისათვის საჭირო იყო კომპიუტერული ტექნოლოგიების სფეროში სპეციალური უნარ - ჩვევების ცოდნა, როცა ამჟამად საკმარისია ინტერნეტიდან შესაბამისი ინსტრუქციებისა და პროტოკოლების გადმოქაჩვა და მათი გამოყენება შერჩეულ საიტზე კიბერშეტევის ორგანიზებისთვის. ამის გამო, კიბერშეტევის განხორციელება მომხმარებლისთვის გახდა უფრო ადვილად ხელმისაწვდომი. ჰაკერთა მომსახურეობით სარგებლობენ არამარტო კორპორაციები და კომპანიები, არამედ სადაზვერვო ან სხვა სახის სპეციალური სამსახურებიც;

ჰაკტივისტები - ტერმინი „ჰაკტივიზმი“ (hacktivism) წარმოიშვა ორი სიტყვის „Hack“ და “Activism” შეერთებით და ის აღნიშნავს სოციალური პროტესტის გამოხატვის ახალ მოვლენას, რომელიც წარმოადგენს თავისებურ სინთეზს რაღაცის მიმართ გამოხატული პროტესტის სოციალური აქტიურობისა და ჰაკერობის, რომელიც მიმართულია გარკვეული ვებ - გვერდების ან საფოსტო სერვისების წინააღმდეგ. თავიანთი პოლიტიკური მიზნების მისაღწევად, ჰაკტივისტები მიისწრაფვიან დააზიანონ ან საერთოდ მწყობრიდან გამოიყვანონ ზოგიერთი ვებ - გვერდი;

კიბერ დივერსანტები ქსელის უკმაყოფილო მომხმარებელთა რიცხვიდან - ზოგადად, უკმაყოფილო მომხმარებლები წარმოადგენენ სერიოზულ საფრთხეს, ვინაიდან ისინი კარგად იცნობენ სისტემის მუშაობის პრინციპებს და შეუძლიათ თავიანთი ეს ცოდნა გამოიყენონ დესტრუქციული მიზნებისთვის. მაგალითად, სისტემის დასაზიანებლად ან კონფიდენციალური ინფორმაციის მოსაპარად. შეერთებული შტატების ფედერალური საგამოძიებო ბიუროს (FBI) მონაცემებით, სისტემის მომხმარებლებისა და გარე წყაროების მხრიდან კიბერშეტევის ორგანიზების შესაძლებლობის ერთმანეთთან შეფარდება შეადგენს 2:1;



ტერორისტები - ცდილობენ ინფრასტრუქტურის მნიშვნელოვანი ობიექტები გამოიყვანონ მწყობრიდან, საერთოდ გაანადგურონ ან გაომიყენონ თავიანთი მიზნებისთვის. მათი ქმედება სერიოზული საფრთხის ქვეშ აყენებს ქვეყნების ეროვნულ უსაფრთხოებას, იწვევს ადამიანთა მასიურ მსხვერპლს, ასუსტებს ეკონომიკას, ასევე ზიანს აყენებს საზოგადოების მორალურ მდგომარეობასა და ამცირებს მათ სანდოობას ხელისუფლების მიმართ. ყველა ტერორისტული ორგანიზაცია და დაჯგუფება არ ფლობს საკმარის ცოდნასა და ტექნიკურ საშუალებებს ეფექტური კიბერშეტევის განხორციელებისთვის, თუმცა არსებობს თეორიული დაშვება, რომ მათ მიიღონ მსგავსი ცოდნა და შესაძლებლობა, ან დახმარებისთვის მიმართონ ორგანიზებული დანაშაულის წარმომადგენლების მომსახურებას;

ბოტნეტი - ინტერნეტ პროგრამას, რომელიც ფარულად არის დაყენებული მსხვერპლის/ობიექტის კომპიუტერულ მოწყობილობაში, რაც დამნაშავეს/ბოროტმოქმედს საშუალებას აძლევს დავირუსებული კომპიუტერის რესურსების გამოყენებით, შეასრულოს გარკვეული ქმედებები. ჰაკერების ეს სახეობა თავისი პროგრამებით ავირუსებენ კომპიუტერების დიდ რაოდენობას, რომელთა რესურსებსაც შემდეგ იყენებენ კიბერშეტევის კოორდინირებისთვის, ასევე „სპამის“ გასაგზავნად, ფიშინგისთვის და სხვა მავნე ქმედებისთვის. მსგავსი სახის ქსელები წარმოადგენენ არალეგალური ვაჭრობის ობიექტს; **ფიშერები** - ეს არის ფიზიკური პირები ან პატარა დაჯგუფებები, რომლებიც იყენებენ ფიშინგის ტექნოლოგიებს45 პერსონალური რეკვიზიტების მოპარვისა და ფასიანი ინფორმაციების გადაყიდვის მიზნით. თავიანთი მიზნების მისაღწევად ფიშერები ხშირად იყენებენ „სპამებს“ და ჯაშუშურ პროგრამებს; **სპამერები** - ფიზიკური ან იურიდიული პირები, რომლებიც მასიურად აგზავნიან არამოთხოვნილ ელექტრონულ ფოსტას დაფარული ან მცდარი ინფორმაციით, რომლის მიზანია ფიშინგითა და ჯაშუშური პროგრამების გამოყენებით კონკრეტულ ორგანიზაციებზე კიბერშეტევის განხორციელება;

ჯიჰადისტური ვიდეო ქართული ჯარის წინააღმდეგ 2013 წლის ივნისში Youtube-ის მეშვეობით გავრცელდა, მუქარის შემცველი ორი ვიდეორგოლი. ვიდეო ინტერნეტსივრცეში ოკუპირებული აფხაზეთიდან მალაიზიაში წინასწარ მომზადებული სერვერის გამოყენებით, დაშიფრული ხაზით ატვირთა ყირგიზეთის მოქალაქე სამარ ჩოკუტაევმა. გამოყენებულ იქნა ქართული მობილური ოპერატორების ინტერნეტმოდემები, თავად ანძები კი, რომლებითაც ბრალდებულმა ისარგებლა, საქართველოს ხელისუფლების მიერ კონტროლირებულ ტერიტორიაზეა განლაგებული ავტორი "თალიბანის" სახელით საუბრობს, ქართველ სამხედროებს ჯვაროსნებად მოიხსენიებს და ავღანეთის

მისიაში მათი მონაწილეობის გამო შურისძიებით იმუქრება. მუქარა მიმართულია როგორც ქართველი ჯარისკაცების, ასევე საქართველოს ხელისუფლებისა და ქვეყნის მოსახლეობის მიმართ.

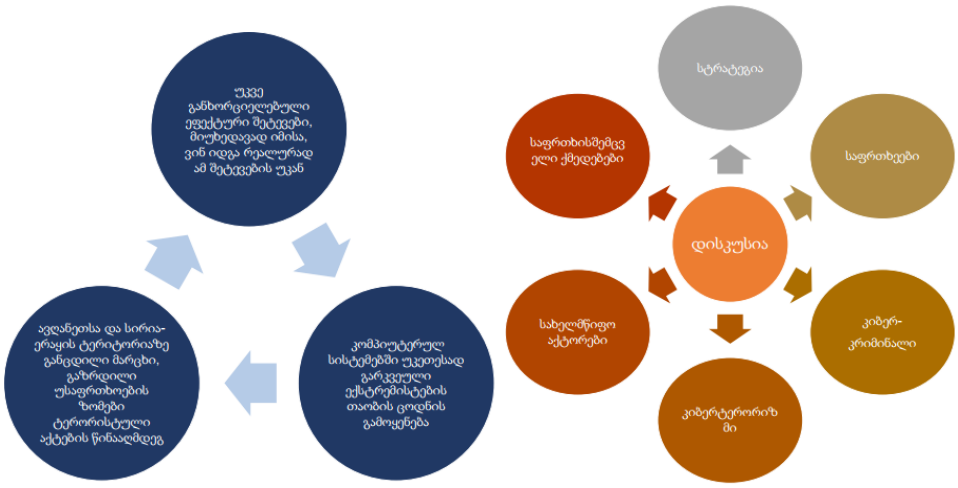
კიბერშეტევის ხელწერა და მავნე კოდებში აღმოჩენილი კირილიცის ელემენტები ჰაკერული დაჯგუფება APT28-ის ხელწერის იდენტურია • შეტევის დრო ემთხვევა ფრანგულ-რუსული ურთიერთობების გაუარესებას • „მისტრალის“ რუსეთისთვის მიყიდვის ბლოკირება • საფრანგეთის პრეზიდენტის უარი მოსკოვში 9 მაისის ღონისძიებებში მონაწილეობაზე • APT 28 რუსეთის სპეცსამსახურებთან აფილირებული ორგანიზაციაა, რომელიც პასუხისმგებელია საქართველოს, უკრაინის, ევროკავშირის ქვეყნებსა თუ აშშ-ის კიბერსივრცეზე მრავალჯერად კიბერთავდასხმებსა და კიბერშპიონაჟის ფაქტებზე. • ფრანგულ მაუწყებელზე კარგად ორგანიზებულმა შეტევამ რუსულ სპეცსამსახურებს შესაძლებლობა მისცა მოეპოვებინათ კონტროლი ათამდე საინფორმაციო არხსა და მათ სოციალურ მედიაზე, გაევრცელებინათ ჯიჰადისტური პროპაგანდა და გამოექვეყნებინათ სირიაში დისლოცირებული ფრანგი სამხედროების პირადი მონაცემები.

ფრანგულ მაუწყებელზე კარგად ორგანიზებულმა შეტევამ რუსულ სპეცსამსახურებს შესაძლებლობა მისცა მოეპოვებინათ კონტროლი ათამდე საინფორმაციო არხსა და მათ სოციალურ მედიაზე, გაევრცელებინათ ჯიჰადისტური პროპაგანდა და გამოექვეყნებინათ სირიაში დისლოცირებული ფრანგი სამხედროების პირადი მონაცემები. რუსეთის სახელმწიფოს მიერ ფინანსირებული „ტროლების არმიის“ მიერ შეიქმნა და სოციალურ ქსელებში ხდებოდა ყალბი ვიდეოს გაზიარება, რომელშიც ამერიკელი ჯარისკაცი თითქოსდა იარაღს ესვრის ყურანს. იგივე ორგანიზაცია, ტროლების მეშვეობით გამუდმებით ცდილობს ისლამისტური საფრთხის გაზვიადებას. ასევე „კიბერხალიფატის“ სახელით, სოციალურ ქსელებში აიტვირთა ამერიკელი სამხედროების პირადი მონაცემები, ხოლო სამხედროების ოჯახის წევრებმა კი მიიღეს მუქარის შემცველი წერილები. მოგვიანებით დადგინდა, რომ სინამდვილეში ეს აქცია ჯიჰადისტების საფარქვეშ განახორციელა რუსულ სამთავრობო სტრუქტურებთან დაკავშირებულმა ჰაკერულმა იმავე დაჯგუფებამ - APT28/Fancy Bear, რომელიც ასევე პასუხისმგებელია აშშ -ის საპრეზიდენტო არჩევნების დროს განხორციელებულ კიბერშეტევებზე.

კიბერტერორიზმი - მზარდი საფრთხე

რთულად პროგნოზირებადია მოგებაზე ორიენტირებულ კიბერდამნაშავეთაგან მომდინარე საფრთხეები საზოგადოებრივი ცნობიერების ამაღლება მუდმივი კონტაქტი კერძო სექტორში განთავსებულ კრიტიკულ ინფრასტრუქტურის სუბიექტებთან ადგილობრივი კანონმდებლობის საერთაშორისო სამართლის

ნორმებთან ჰარმონიზაცია კიბერკრიმინალთან ბრძოლის სართაშორისო თანამშრომლობის მექანიზმების აქტიური გამოყენება. კრიტიკული სერვისების პროვაიდერებში არსებული მონაცემთა ბაზები პერსონალური ინფორმაცია (სამედიცინო, სადაზღვევო, რეგისტრაცია, საბანკო) ინფორმაცია ქვეყნის თავდაცვისუნარიანობის შესახებ (შესყიდვები, კვება).



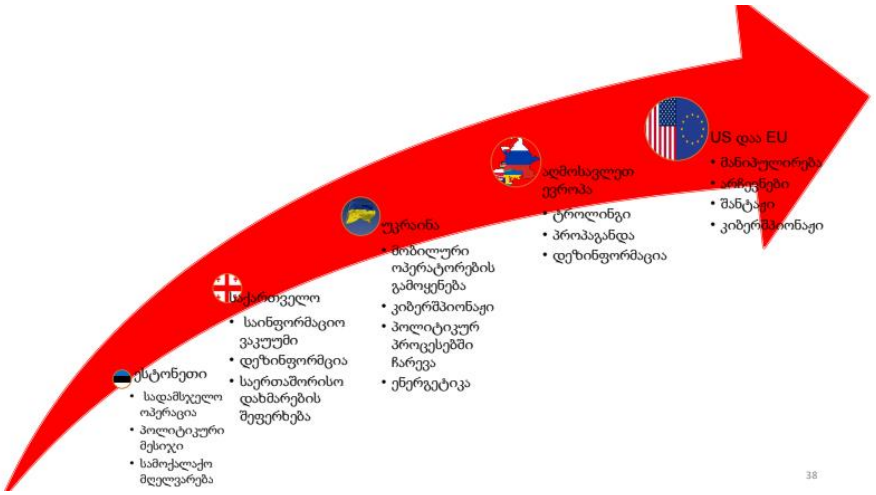
საკანონმდებლო ბაზა და საქართველოს კიბერარქიტექტურა

ბოლო პერიოდში, კიბერუსაფრთხოების კუთხით, საქართველომ ბევრი მნიშვნელოვანი ნაბიჯი გადადგა. ამის საუკეთესო დასტური გაერთიანებული ერების საერთაშორისო სატელეკომუნიკაციო ორგანიზაციის, ITU-ს კიბერუსაფრთხოების ინდექსია, რომლის მიხედვითაც საქართველო, მსოფლიო მასშტაბით, "კიბერუსაფრთხო" ქვეყნების პირველ ათეულში იკავებს ადგილს.

იმისათვის, რომ კიბერსივრცეში სანდო პარტნიორი და საიმედო მოთამაშე ვიყოთ, საჭიროა, სახელმწიფო უზრუნველყოფდეს საკუთარ კიბერუსაფრთხოებას. ამ თვალსაზრისით, მნიშვნელოვანია მთავრობის ერთიანი მიდგომა და, ასევე, კერძო სექტორის ჩართულობა. დემოკრატიულ სახელმწიფოში კრიტიკული ინფრასტრუქტურის სუბიექტების აბსოლუტური უმრავლესობა ბიზნესის ხელშია. სწორედ ამიტომ, მოწინავე სახელმწიფოებისთვის კიბერუსაფრთხოება საერთო პასუხისმგებლობაა და სისტემის მდგრადობას ვერც მხოლოდ ბიზნესი და ვერც მხოლოდ სახელმწიფო ვერ უზრუნველყოფს.

მეორე მნიშვნელოვანი ფაქტორი გახლავთ ინფორმაციის გაზიარების აუცილებლობა კიბერაქტორებს შორის ქვეყნის შიგნით და პარტნიორებთან-საზღვარგარეთ. გახშირებული კიბერშეტევების ფონზე განსაკუთრებულ

მნიშვნელობას იძენს მომხმარებლის ცნობიერების ამაღლებისკენ მიმართული ღონისძიებები: ტრენინგები, სასწავლო კურსების ჩამოყალიბება, კვლევის წარმოება და სხვა.



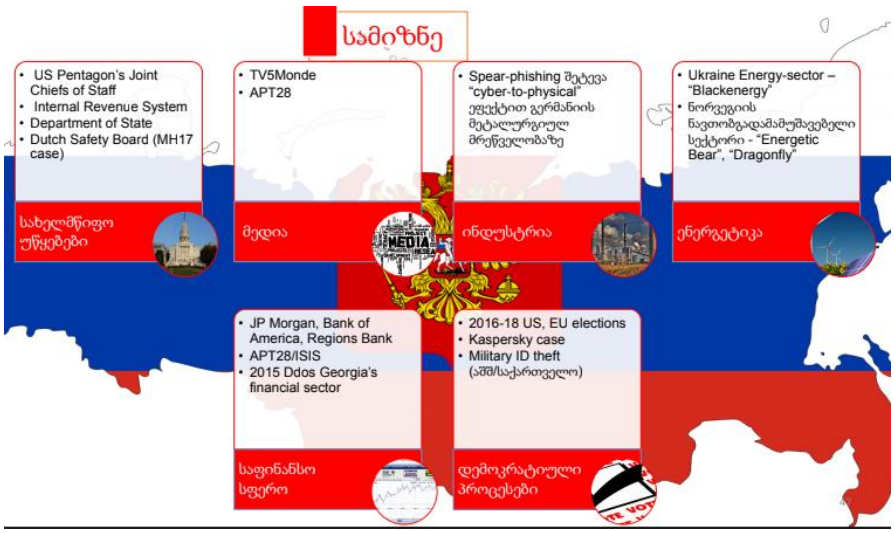
რას ემუქრება კიბერომი

კიბერელემენტების გამოყენება პოლიტიკური, ეკონომიკური თუ სამხედრო მიზნების მისაღწევად, გეოპლიტიკური უპირატესობის მოსაპოვებლად, თანამედროვე მსოფლიოს რეალობაა. დასავლელი ექსპერტები სულ უფრო ხშირად მსჯელობენ იმ ტენდენციაზე, რომელიც კიბერომის ქსელურ ომად გარდაქმნას ახლავს თან. კიბერომი ინფორმაციული და საკომუნიკაციო სისტემების განადგურებისაკენ მიმართული ქმედებაა, მაშინ, როდესაც ქსელური ომი არის განზრახ ქმედება, რომელიც გულისხმობს ერთი ან რამდენიმე აქტორის მცდელობას, ღია ან ფარული არხების მეშვეობით იმგვარად შეცვალოს სამიზნე აქტორის აღქმა, რომ ამ ცვლილებამ შემდგომში შემტევისათვის სასურველი შედეგი მოიტანოს.

კიბერომი ემუქრება შემდეგ სფეროებს:

- სახელმწიფო
- სახელმწიფო უწყებები
- მრეწველობა
- ენერგეტიკა
- საფინანსო სფერო
- პოლიტიკური და
- საზოგადოებრივი პროცესი

კიბერომის სამიზნე შეიძლება იყოს:



საქართველოს კიბერსივრცეში არსებული საფრთხეები

საქართველოს წინაშე მდგარი კიბერსაფრთხეების მასშტაბი მზარდია, როგორც სირთულის, ისე მრავალფეროვნების თვალსაზრისით. საჭიროა განსაკუთრებული ყურადღება დაეთმოს კიბერაქტორების განზრახვების, შესაძლებლობებისა თუ ღონისძიებების შესახებ ინფორმაციის მოპოვებისა და ანალიზის მექანიზმის ჩამოყალიბებას და ამ მხრივ აქტიური მუშაობის წარმართვას. ყველაზე რეალური საფრთხის შემცველი საქართველოს კიბერსივრიცისათვის არის რუსეთის კიბერაქტივობები, რომელიც მიმართულია როგორც კრიტიკული ინფრასტრუქტურის მოშლის, ასევე საკუთარი მიზნებისათვის გამოყენებისაკენ. ხაზგასმით უნდა აღინიშნოს, რომ ისეთი დაბალტექნოლოგიური თავდასხმებიც კი, როგორიცაა DDoS და Defacement შეტევა, სუსტად დაცული ინფრასტრუქტურის პირობებში შესაძლოა არაპროპორციული ზარალის მიზეზი გახდეს. ცალსახად უნდა აღინისნოს, რომ რუსეთის მიერ განხორციელებულმა ან მხარდაჭერილმა კიბერშეტევამ საქართველოში შესაძლოა გამოიწვიოს მნისვნელოვანი ზარალი და მსხვერპლიც კი. რაც შეეხება ირანისა და ჩინეთის მხრიდან მომდინარე კიბერსაფრთხეებს, აქ, უპირველეს ყოვლისა, არ უნდა გამოგვრჩეს საქართველოში განთავსებული იმ სახელმწიფოების ინფრასტრუქტურა და მონაცემთა ბაზები, რომელთაც ეს ქვეყნები საკუთარ მოწინააღმდეგედ განიხილავენ. ასეთებს განეკუთვნება საქართველოს სტრატეგიული პარტნიორი აშშ, ჩრდილოატლანტიკური ალიანსისა და ევროკავშირის წევრი ქვეყნები და თავად ამ საერთაშორისო ორგანიზაციების სისტემები. ჩინეთის კიბერშეტევები ძირ ტერორისტული ორგანიზაციების მხრიდან დიდია ალბათობა ისეთი კიბერშეტევის განხორციელებისა, რომელიც გამოიწვევს ელექტრონული სერვისების და ვებ-გვერდების დროებით, ლოკალურ დაზიანებას. მასობრივი

ზიანის ან მსხვერპლის გამომწვევი კიბერშეტევის ორგანიზება და განხორციელება ამ ეტაპზე ნაკლებად სავარაუდოა. რთულად პროგნოზირებადია მოგებაზე ორიენტირებულ კიბერდამნაშავეთაგან მომდინარე საფრთხეების ალბათობა. ამ მხრივ მეტად მნისვნელოვანია საზოგადოებრივი ცნობიერების ამაღლება, მუდმივი კონტაქტი კერძო სექტორში განთავსებულ კრიტიკულ ინფრასტრუქტურასთან, ადგილობრივი კანონმდებლობის საერთაშორისოსთან ჰარმონიზაცია და კიბერკრიმინალთან ბრძოლის სართაშორისო თანამშრომლობის მექანიზმების აქტიური გამოყენება.

კიბერჰიგიენის ზოგადი წესები

თქვენი კომპიუტერული მოწყობილობები ინახავენ თქვენს მონაცემებს და წარმოადგენენ თქვენს ონლაინ პორტალებს. ქვემოთ ჩამოთვლილია რამდენიმე რჩევა, რომლებიც დაგეხმარებიან თქვენი კომპიუტერული მოწყობილობების ჰაკერებისგან დასაცავად:

· **გქონდეთ ფაიერვოლი ჩართული** – მიუხედავად იმისა, თქვენ გაქვთ პროგრამული თუ აპარატურული ფაიერვოლი როუტერზე, იგი გამუდმებით ჩართული და განახლებული უნდა გქონდეთ, რათა თავიდან აიცილოთ ჰაკერების მიერ თქვენს პირად ან კომპანიის მონაცემებთან წვდომა. დააკლიკეთ Windows 7, Window 8, ან Windows 10 ბმულებზე, რათა გააქტიუროთ ფაიერვოლი ვინდოუსის შესაბამის ვერსიაზე. დააკლიკეთ აქ, რათა გააქტიუროთ ფაიერვოლი Mac OS X მოწყობილობებზე.

გამოიყენეთ ანტივირუსი და Antispyware – მავნე პროგრამები, როგორიცაა ვირუსები, ტროიანები, ჭიები, ransomware და spyware,თქვენს კომპიუტერში ინსტალირდებიან თქვენი ნებართვის გარეშე იმისათვის, რომ მოიპოვონ თქვენს კომპიუტერსა და მონაცემებზე წვდომა. ვირუსები ანადგურებენ თქვენ მონაცემებს, ანელებენ თქვენი კომპიუტერის სიჩქარეს ან იღებენ მასზე კონტროლს. ვირუსის მიერ თქვენი კომპიუტერის კონტროლის გამოყენების ერთ-ერთი გზაა, მოცემული კომპიუტერით სპამების გავრცელება თქვენი ანგარიშიდან. Spyware-ს შეუძლია თქვენი ონლაინ მოქმედებების მონიტორინგი, თქვენი პირადი ინფორმაციის შეგროვება ან თქვენს ვებ-ბრაუზერში არასასურველი პოპ-აპ რეკლამების განთავსება. Spyware-ის თავიდან აცილების კარგი გზა არის, პროგრამული უზრუნველყოფის ჩამოტვირთვისას, მხოლოდ სანდო ვებ-საიტების გამოყენება. ანტივირუსული პროგრამა შექმნილია თქვენი კომპიუტერისა და შემომავალი ელ-ფოსტების სკანირებისთვის ვირუსებზე და მათ წასაშლელად. ზოგჯერ, ანტივირუსული პროგრამა შეიცავს antispyware-საც. უახლესი მავნე

პროგრამებისგან თქვენი კომპიუტერის დასაცავად, ყოველთვის იქონიეთ განახლებული პროგრამული უზრუნველყოფა.

მართეთ თქვენი ოპერაციული სისტემა და ბრაუზერი – ჰაკერები ყოველთვის ცდილობენ თავის სასარგებლოდ გამოიყენონ თქვენი ოპერაციული სისტემისა და ვებ ბრაუზერის ხარვეზები. თქვენი კომპიუტერისა და მონაცემების დასაცავად, დაცვის პარამეტრები დააყენეთ საშუალოზე ან ძლიერზე. რაგულარულად განაახლეთ თქვენი ოპერაციული სისტემა და ვებ-ბრაუზერები და რეგულარულად გადმოტვირთეთ პაჩებისა და უსაფრთხოების პროგრამული უზრუნველყოფის უახლესი განახლებები, შესაბამისი მომწოდებლებისგან.

დაიცავით თქვენი ყველა მოწყობილობა – არაავტორიზებული წვდომისაგან თავდასაცავად, თქვენს კომპიუტერულ მოწყობილობებზე, როგორებიცაა PC-ები, ლეპტოპები, პლანშეტები ან სმარტფონები, გამოიყენეთ პაროლით დაცვა. შენახული ინფორმაცია უნდა იყოს დაშიფრული, განსაკუთრებით მგრძნობიარე ან კონფიდენციალური მონაცემები. მობილურ მოწყობილობებში შეინახეთ მხოლოდ აუცილებელი ინფორმაცია, იმ შემთხვევებისთვის, თუ მოხდება მათი მოპარვა ან დაკარგვა, როდესაც არ იმყოფებით სახლში. თუ თქვენი რომელიმე მოწყობილობა არის კომპრომეტირებული, კრიმინალებს შესაძლებელია გააჩნდეთ წვდომა თქვენს ყველა მონაცემზე, ღრუბლების გამოყენებით, როგორიცაა iCloud ან Google drive.

IoT მოწყობილობები გაცილებით დიდი რისკის წყაროა, ვიდრე თქვენი სხვა კომპიუტერული მოწყობილობები. როდესაც დესკტოპის, ლეპტოპისა და მობილურის პლატფორმები ხშირად ღებულობენ პროგრამულ განახლებებს, IoT-ის მოწყობილობები ჯერ კიდევ საწყის ჩაშენებულ პროგრამას იყენებენ. თუკი მოცემულ ჩაშნეებულ პროგრამებში ხდება ხარვეზების აღმოჩენა, მოცემული IoT მოწყობილობა, დიდი ალბათობით, დარჩება დაუცველი. პრობლემას აუარესებს ის ფაქტი, რომ IoT მოწყობილობები ხშირად ისეა დაპროექტებული, რომ უკავშირდებიან სახლს და ითხოვენ ინტერნეტთან წვდომას. ინტრნეტთან წვდომისთვის, უმეტესობა მათგანი იყენებს მომხმარებლის ლოკალურ ქსელს. შედეგად, დიდია ალბათობა, რომ მოხდეს IoT მოწყობილობათა კომპრომეტირება და როდესაც ეს ხდება, ისინი საშუალებას აძლევენ თავდამსხმელებს მოიპოვონ წვდომა მოცემული მომხმარებლის ლოკალურ ქსელსა და მონაცემებზე. საუკეთესო გზა მოცემული შემთხვევის თავიდან ასაცილებლად არის, IoT მოწყობილობებს მისცეთ მხოლოდ იზოლირებულ ქსელთან წვდომა, რომელსაც იგი გაიზიარებს დანარჩენ IoTმოწყობილობებთან.

ჩვენ ვიყენებთ უამრავ ანგარიშს, რომლებასც სჭირდებათ პაროლები; რაც რთული დასამახსოვრებელია. ერთ-ერთი გამოსავალი მოცემული სიტუაციიდან, არის პაროლების მენეჯერის გამოყენება. იგი ინახავს და შიფრავს ყველა თქვენს განსხვავებულ და კომპლექსურ პაროლს. იგი, შესაძლოა, დაგეხმაროთ თქვენს

ონლაინ ანგარიშებზე ავტომატურად ავტორიზაციაში. ამ შემთხვევაში დაგჭირდებათ მხოლოდ ერთი მთავარი პაროლის დამახსოვრება, რათა წვდომა გქონდეთ პაროლების მენეჯერთან და შეძლოთ სხვა ანგარიშებისა და პაროლების მართვა.

რჩევები კარგი პაროლის შესარჩევად:

- არ გამოყენოთ არცერთი ენის ლექსიკონის სიტყვები ან სახელები
- არ გამოიყენოთ ლექსიკონის სიტყვების ცნობილი სახესხვაობები
- არ გამოიყენოთ კომპიუტერის ან ანგარიშის სახელები
- თუ შესაძლებელია, გამოიყენეთ სპეციალური სიმბოლოები, როგორებიცაა: ! @ # $ % ^ & * ( )
- გამოიყენეთ ათი ან მეტი სიმბოლოს შემცველი პაროლები

ფიშინგი არის ბოროტმოქმედი მხარის მიერ თაღლითური ელ-ფოსტის გაგზავნა, კანონიერი და სანდო მხარის ნიღბით. მოცემული შეტყობინების მიზანია ელ-ფოსტის მიმღების შეცდომაში შეიყვანა, რათა მან დააინსტალიროს მავნე პროგრამა საკუთარ მოწყობილობაზე ან გაუზიაროს თავდამსხმელს პერსონალური ან ფინანსური ინფორმაცია. ფიშინგის მაგალითს წარმოადგენს ელ-ფოსტა, გამოგზავნილი ყალბი საცალო მაღაზიის მიერ, რომელიც მომხმარებელს სთხოვს დააკლიკოს მასში მითითებულ ბმულზე პრიზის მისაღებად. ბმულს შეიძლება მომხმარებელი გადაჰყავდეს ყალბ საიტზე, რომელიც ითხოვს პერსონალურ ინფორმაციას, ან აინსტალირებდეს ვირუსს.

Spear phishing წარმოადგენს უაღრესად მიზანმიმართულ ფიშინგის შეტევას. მაშინ, როცა ფიშინგიც და Spear phishing-იც, მსხვერპლთან დასაკავშირებლად იყენებენ ელ-ფოსტას, Spear phishing იმით განსხვავდება უბრალო ფიშინგისგან, რომ ელ-ფოსტის შეტყობინებები გამიზნულია კონკრეტული პირისთვის. მაგალითად, თავდამსხმელი შეისწავლის, რომ სამიზნე პირი დაინტერესებულია მანქანებით და ეძებს კონკრეტული მოდელის ავტომობილს შესაძენად. მოცემული თავდამსხმელი უერთდება ავტომობილების განხილვის იმ ფორუმს, რომლის წევრიც არის მისი სამიზნე, აყალბებს ავტომობილის გაყიდვის შეთავაზებას და ელ-ფოსტით უგზავნის სამიზნეს. მოცემული ელ-ფოსტა შეიცავს ბმულს სასურველი მანქანის სურათებით. როდესაც სამიზნე პირი დააკლიკებს მოცემულ ბმულზე, მის კომპიუტერში დაყენდება მავნე პროგრამა.

ელ-ფოსტისა და ვებ-ბრაუზერის კონფიდენციალურობა

ყოველდღე, მილიონობით ელ-ფოსტის შეტყობინებები გამოიყენება მეგობრებსა და ბიზნეს პარტნიორებთან კომუნიკაციისთვის. ელ-ფოსტა მოსახერხებელ გზას წარმოადგენს ერთმანეთთან კომუნიკაციისთვის. როდესაც აგზავნით ელ-ფოსტას,

ეს იგივეა, რაც გააგზავნოთ საფოსტო ბარათი. საფოსტო ბარათის შეტყობინება გადაიცემა ტექსტური ფორმით ისე, რომ ყველას შეუძლია ხილვა, თუ გააჩნია შესაბამისი წვდომა და ელ-ფოსტის შეტყობინებაც გადაიცემა ტექსტური ფორმით და ყველას შეუძლია მისი წაკითხვა, ვისაც გააჩნია წვდომა. მოცემული კომუნიკაციები, აგრეთვე, იგზავნება მრავალი სერვერის გავლით მანამ, სანამ მიაღწევს დანიშნულების ადგილს. მაშინაც, კი თუ თქვენ წაშლით თქვენს ელ-ფოსტის შეტყობინებებს, ისისნი გარკვეული დროით კვლავ ინახებიან ელ-ფოსტის სერვერებზე.

ყველას, ვისაც გააჩნია ფიზიკური წვდომა თქვენს კომპიუტერთან ან როუტერთან, შეუძლია ნახოს, რომელ ვებ-საიტებს ეწვიეთ, ვებ-ბრაუზერის ისტორიის, ქეშის ან შესაძლოა log ფაილების გამოყენებით. ეს პრობლემა შეიძლება თავიდან აიცილოთ, ბრაუზერზე კონფიდენციალური რეჟიმის გააქტიურებით. ყველაზე პოპულარულ ბრაუზერებს გააჩნიათ საკუთარი სახელი კონფიდენციალური რეჟიმისთვის:

- Microsoft Internet Explorer: InPrivate
- Google Chrome: Incognito
- Mozilla Firefox: Private tab / private window
- Safari: Private: Private browsing

კონფიდენციალური რეჟიმის გააქტიურებით, დაბლოკილია ქუქების და დროებითი ინტერნეტ ფაილების დაგროვების პროცესი და ბრაუზერის ისტორია იშლება, ბრაუზერის ფანჯრის ან პროგრამის დახურვის შემდეგ.

თქვენი ინტერნეტ ბრაუზერის კონფიდენციალურ რეჟიმში გამოყენებით, შესაძლებელია უცხო პირების მიერ თქვენი ონლაინ აქტივობების შესახებ ინფორმაციის შეგროვებისა და ამ ინფორმაციის გამოყენებით სხვადასხვა არასასურველი რეკლამების გამოგზავნის პრევენცია. მიუხედავად კონფიდენციალური რეჟიმის გააქტიურებისა და ქუქების დაბლოკვისა, კომპანიები ავითარებენ სხვადასხვა გზებს, მომხმარებლის სათვალთავალოდ, ინფორმაციის შესაგროვებლად და მისი ქცევის გასაკონტროლებლად. მაგალითად, შუალედური მოწყობილობები, როგორებიცაა როუტერები, შეიძლება შეიცავდნენ ინფორმაციას თქვენი ინტერნეტ აქტივობების შესახებ.

საბოლოო ჯამში, თქვენი მონაცემების, იდენტობის და კომპიუტერული მოწყობილობების დაცვაზე თავად ხართ პასუხისმგებელი. როდესაც აგზავნით ელ-ფოსტას, დასაშვებია თუ არა, რომ იგი შეიცავდეს თქვენს სამედიცინო ჩანაწერებს? ახალ ჯერზე ინტერნეტში შესვლისას, არის თუ არა თქვენი კავშირი ინტერნეტთან უსაფრთხო? მხოლოდ რამდენიმე მარტივი სიფრთხილის წესის დაცვით, შესაძლოა, სამომავლოდ მრავალი პრობლემა აიცილოთ თავიდან.

თქვენი მონაცემებისა და კონფიდენციალურობის დაცვა

მოცემული თავი კონცენტრირებული იყო თქვენს პერსონალურ მოწყობილობებსა და მონაცემებზე. იგი მოიცავდა თქვენი მოწყობილობების დასაცავად, ძლიერი პაროლების შესაქმნელად და უკაბელო ქსელის უსაფრთხოდ გამოყენების შესახებ რჩევებს. მასში დაფარულია მონაცმეების სარეზერვო ასლების შექმნა და მონაცემდა სამუდამო წაშლა.

განხილული იყო ავთენტიფიკაციის მეთოდები თქვენი მონაცემების უსაფრთხო მართვაში დასახმარებლად. იგი მოკლედ ხსნის, რამდენად მარტივია მეტისმეტად ბევრი ინფორმაციის გავრცელება სოციალურ მედიაში და მოცემული უსაფრთხოების რისკების თავიდან აცილების მეთოდებს.

უსაფრთხოება სოციალურ ქსელში

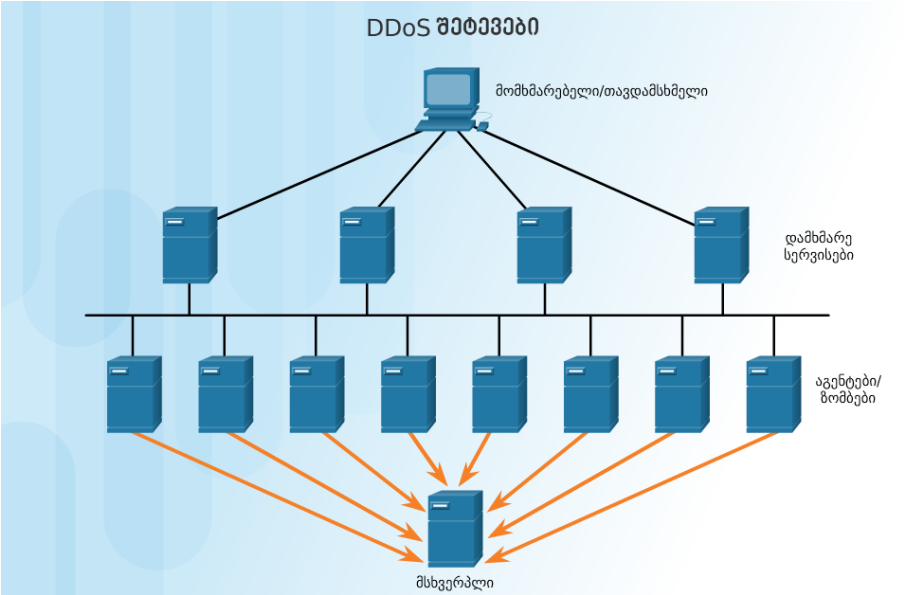
ორგანიზაციის უსაფრთხოება

მოცემულ თავში დაფარულია ზოგიერთი ტექნიკა და პროცესი, რომლებსაც იყენებენ კიბერ-უსაფრთხოების პროფესიონალები, როდესაც იცავენ ორგანზაციის ქსელს, აღჭურვილობასა და მონაცემებს. თავდაპირველად, მოკლედ არის ახსნილი ფაიერვოლების მრავალი ტიპი, დაცვის ტექნიკები და პროგარმული უზრუნველყოფა, რომლებიც ამჟამად გამოიყენება, საუკთესო გამოცდილების გათვალისწინებით.

შემდეგ, მოცემულ თავში, წარმოადგენილია ბოტნეტები, მკვლელობათა ჯაჭვი , ქცევაზე დაფუძნებული უსაფრთხოება და NetFlow-ს გამოყენებით ქსელის მონიტორინგი.

მესამე ნაწილში, საუბარია, Cisco-ს მიდგომაზე კბერ უსაფრთხოებაში, CSIRT ჯგუფის და უსაფრთხოების მოქმედებების გეგემის ჩათვლით. მოკლედ არის დაფარული საშუალებები, რომლებსაც კიბერ უსაფრთხოების სპეციალისტები იყენებენ ქსელზე შეტევების აღმოსაჩენად და პრევენციისთვის

შეტევების დეტექტირება რეალურ დროში



თავდამსხმელები შეტევებისთვის იყენებენ ბევრ ჰოსტებს, რომლებსაც "ზომბები" ეწოდებათ

პორგამული უზრუნველყოფა არ არის უნაკლო. როდესაც ჰაკერი იყენებს პროგრამულ უზრუნველყოფაში არსებულ ხარვეზს, პროგრამის შემქმნელის მიერ მოცემული ხარვეზის გამოასწორებამდე, მოცემულ შეტევას ეწოდება ნულოვანი დღის შეტევა. დღევანდელ დღეს, ნულოვანი დღის შეტევათა სიზუსტისა და სიმძლავრის გათვალისწინებით, უფრო და უფრო ხშირად სრულდება ქსელზე შეტევები წარმატებულად. მაშასადამე, დაცვის ეფექტურობა განისაზღვრება იმით, თუ რამდენად სწრაფად მოხდება მოცემულ შეტევაზე რეაგირება. რეალურ დროში შეტევათა დეტექტრება, ასევე, მათი დაუყოვნებლივი შეჩერება, წარმოადგენს იდეალურ მიზანს. საუბედუროდ, მრავალ კომპანიასა და ორგანიზაციას არ შეუძლია შეტევათა აღმოჩენა, მათი განხორციელებიდან რამდენიმე დღის ან თუნდაც თვის განმავლობაშიც კი.

სრული სკანირება რეალურ დროში - შეტევების დეტექტირება რეალურ დროში, მოითხოვს განუწყვეტელ სკანირებას ფაიერვოლისა და IDS/IPS ქსელურ მოწყობილობათა გამოყენებით. ასევე, გამოყენებული უნდა იყოს, მომავალი თაობის კლიენტის/სერვერის მავნე პროგრამათა აღმომჩენი სისტემები, საერთაშორისო ონლაინ საფრთხეების ცენტრთან თანამშრომლობით. დღესდღეისობით, აქტიური სკანირების მოწყობილობებსა და პორგრამულ უზრუნველყოფებს, უნდა შეეძლოთ ქსელში ანომალიების დეტექტირება, კონტექსტზე დაფუძნებული ანალიზისა და მოქმედებების დეტექტირებით.

განაწილებული შეტევა მომსახურების დაბლოკვის მიზნით (DDoS) და რეაგირება რეალურ დროში - DDoS წარმოადგენს ერთ-ერთ უდიდეს საფრთხეს, რომელზეც რეალურ დროში რეაგირება და დეტექტორება გადამწყვეტი მნიშვნელობისაა. მსგავსი შეტევებისგან თავდაცვა განსაკუთრებით რთულია, რადგან შეტევის პროცესში ჩართულია უამრავი ზომბირებული ჰოსტი და თავდამსხმელები არ

განირჩევიან ჩვეულებრივი მომხმარბელებისგან, როგორც ეს სურათზეა ნაჩვენები. არსებობს მრავალი კომპანია და ორგანიზაცია, რომელთა სერვერებისა და ქსელების დაზიანება მოხდა, მრავალჯერადი DDoS შეტევების გამოყენებით. მაშასადამე, DDoS შეტევათა რეალურ დროში დეტექტირება და რეაგირება, გადამწყვეტი მნიშვნელობისაა.

მავნე პროგრამებისგან თავდაცვა. როგორ უზრუნველყოფთ მუდმივი ნულოვანი დღის შეტევებისგან ან მაღალი დონის შეტევებისგან (APT) თავდაცვას, რომლებიც განკუთვნილია დიდი დროის განმავლობაში, მონაცემების მოსაპარად, თქვენგან შეუმჩნევლად? ერთ-ერთ გადაწყვეტას წარმოადგენს enterprise-დონის მოწინავე ანტივირუსული პრიგრამის გამოყენება, რომელიც გვთავაზობს რეალურ დროში მავნე პროგრამების დეტექტორებას.

ქსელების ადმინისტრატორებმა გამუდმებით უნდა ადევნონ თავალი ქსელში მავნე პროგრამების ნიშნებს ან მოქმედებებს, რომლებიც APT შეტევაზე მიუთითებენ. Cisco-ს გააჩნია მოწინავე მავნე პროგრამებისგან დაცვის (AMP) ქსელი, რომელიც აანალიზებს მილიონობით ფაილს და ადარებს მათ სხვა მილიონობით უკვე შესწავლილ მავნე პროგრამათა ნიმუშებს. მოცემული სქემა უზრუნველყოფს გლობალურ ხედვას მავნე პროგრამების შეტევებზე, კამპანიებსა და მათ გავრცელებაზე. AMP წარმოადგენს კლინტის/სერვერის პროგრამულ უზრუნველყოფას, რომელის განთავსებულია ჰოსტების ბოლოებში, როგორც განცალკევებული სერვერი ან სხვა ქსელის დაცვის მოწყობილობებში. მოცემული სურათზე ნაჩვენებია AMP ქსელის უპირატესობები.

მრავალმა ნაციონალურმა და პროფესიონალურმა ორგანიზაციამ გამოაქვეყნა უსაფრთხოების საუკეთესო გამოცდილებები. ქვემოთ ჩამოთვლილია ზოგიერთი მათგანი:

- **შეაფასეთ რისკი** – თქვენი დასაცავი ობიექტის შეფასება, დაგეხმარებათ უსაფრთხოების ხარჯების განსაზღვრაში.
- **ჩამოაყალიბეთ უსაფრთხოების ნორმები** – ჩამოაყალიბეთ ნორმები, რომელბიც ცალსახად გამოხატავენ კომპანიის წესებს, სამსახურეობრივ მოვალეობებსა და მოლოდინებს.
- **ფიზიკური უსაფრთხოების ზომები** – შეზღუდეთ წვდომა ქსელური აპარატურის ოთახებთან, სერვერების ადგილმდებარეობასთან, ასევე გამოიყენეთ ხანძარსაწინააღმდეგო სიტემა.
- **ადამიანური რესურსების უსაფრთხოების ზომები** – თანამშრომლების არჩევა უნდა მოხდეს დეტალური შესწავლისა და წარსულის გადამოწმების შემდეგ.
- **იქონიეთ და ამოწმეთ სარეზერვო ასლები** – რეგულარულად შეინახეთ სარეზერვო ასლები და შეამოწმეთ მონაცემების აღდგენა მათგან.

- **იქონიეთ უსაფრთხოების პაჩები და განახლებები** – რეგულარულად განაახლეთ სერვერის, კლიენტისა და ქსელის მოწყობილობათა ოპერაციული სისტემები და პროგრამები.
- **აკონტროლეთ წვდომის დონეები** – დააკონფიგურირეთ მომხმარებლის როლისა და პრივილეგიების დონეები, ასევე მოითხოვეთ მომხმარებლის ძლიერი ავთენტიფიკაცია.
- **რეგულარულად ამოწმეთ გაუთვალისწინებელ შემთხვევებზე რეაგირება** – ჩამოაყალიბეთ გაუთვალისწინებელ შემთხვევებზე რეაგირების ჯგუფი და გაითამაშეთ სწრაფი რეაგირების სცენები.
- **გამოიყენეთ ქსელის მონიტორინგის, ანალიზის და მართვის ინსტრუმენტები** - შეარჩიეთ უსაფრთხოების მონიტორინგის საშუალება და მოახდინეთ მისი ინტეგრაცია სხვა ტექნოლოგიებში.
- **გამოიყენეთ ქსელის უსაფრთხოების მოწყობილობები** – გამოიყენეთ მომავალი თაობის როუტერები, ფაიერვოლები და სხვა უსაფრთხოების ხელსაწყოები.
- **გამოიყენეთ მძლავრი უახლესი უსაფრთხოების საშუალებები** – გამოიყენეთ enterprise-დინის ანტივირუსული პროგრამული უზრუნველყოფა.
- **ასწავლე მომხმარებლებს** – გააცანით მომხამრებლებს და თანამშრომლებს უსაფრთხოების პროცედურები.
- **დაშიფრეთ მონაცემები** – დაშიფრეთ კომპანიის ყველა მგრძნობიარე ინფორმაცია, ელ-ფოსტის ჩათვლით.

ზოგიერთი ყველაზე გამოყენებადი გზამკვლევის პოვნა, შესაძლებელია ორგანიზაციულ საცავებში, როგორიცაა სტანდარტებისა და ტექნოლოგიების ნაციონალური ინსტიტუტის (NIST) კომპიუტერული უსაფრთხოების ცენტრი, რაც ნაჩვენებია სურათზე.

მიუხედავად იდენტიფიცირების გაზრდილი შესაძლებლობისა, დღევანდელი საერთაშორისო სამართალი ვერ უზრუნველყოფს კიბერშპიონაჟისა თუ კიბერთავდასხმების ეფექტურ შემაკავებელ გარემოს. არ არსებობს კიბერსივრცეში უნივერსალურად მიღებული და სამართლებრივად სანქციერებული წესები. იმ შემთხვევაშიც, თუკი დგინდება კონკრეტული კიბერშეტევის განმახორციელებელი აქტორი, შეტევასა და თავდამსხმელის იდენტიფიცირებას შორის არსებული ხანგრძლივი პერიოდი დანაშაულის გამოძიებისათვის არახელსაყრელ გარემოს ქმნის. შემტევი ოპერაციების სიმარტივისა და ეფექტურობის გამო, კიბერშპიონაჟისა და კიბერშეტევების განხორციელების მოტივაცია მაღალია, ზოგიერთი სახელმწიფო კი მუდმივად განაგრძობს დაინტერესების ობიექტის

ტექნიკური შესაძლებლობებისა თუ კიბერუსაფრთხოების მდგომარეობის ტესტირებას.

ვლადიმერ ადამია - აკადემიური დოქტორი

საქართველოს ტექნიკური უნივერსიტეტი. ასოცირებული პროფესორი.

ლოკალური ქსელის უსაფრთხოება

გამოთვლითი ტექნიკის და საინფორმაციო ქსელების სწრაფმა განვითარებამ გამოიწვია მათი ფართო გავრცელება როგორც ყოველდღიურ ცხოვრებაში, ასევე ბიზნესში. მძლავრი გამოთვლითი შესაძლებლობები და ინფორმაციის გადაცემის ოპერატიულობა ხელს უწყობს როგორც ტრადიციული ბიზნესის განვითარებას, ასევე ბიზნესის ახალი ფორმების წარმოშობას. განსაკუთრებული მნიშვნელობა საინფორმაციო ტექნოლოგიებმა საბანკო სფეროში შეიძინა.

საინფორმაციო სისტემების ასეთმა ფართო გავრცელებამ სულ უფრო მნიშვნელოვანი გახადა მათი საიმედოობისა და უსაფრთხოების გაზრდა. ინფორმაციის დაგროვების, გადამუშავების და გადაცემის თანამრდროვე მეთოდებმა განაპირობა ინფორმაციის დაკარგვის, მოდიფიცირების და მოპარვის საფრთხის წარმოშობა. გარდა ამისა საფრთხეს წარმოადგენს საინფორმაციო სისტემების მწყობრიდან გამოსვლა. სწორედ ამიტომ გაიზარდა საინფორმაციო სისტემების დაცვის მნიშვნელობა.

მომხმარებლის ინფორმაციის დაცვის ძირითადი ამოცანებია:

- ინფორმაციის კონფიდენციალობის უზრუნველყოფა;
- ინფორმაციის მთლიანობის უზრუნველყოფა;
- ინფორმაციის სარწმუნოების უზრუნველყოფა;
- ინფორმაციასთან ოპერატიული მიმართვის უზრუ- ნველყოფა;
- ელექტრონული სახით წარმოდგენილი ინფორმაციის იურიდიული მნიშვნელობის უზრუნველყოფა;

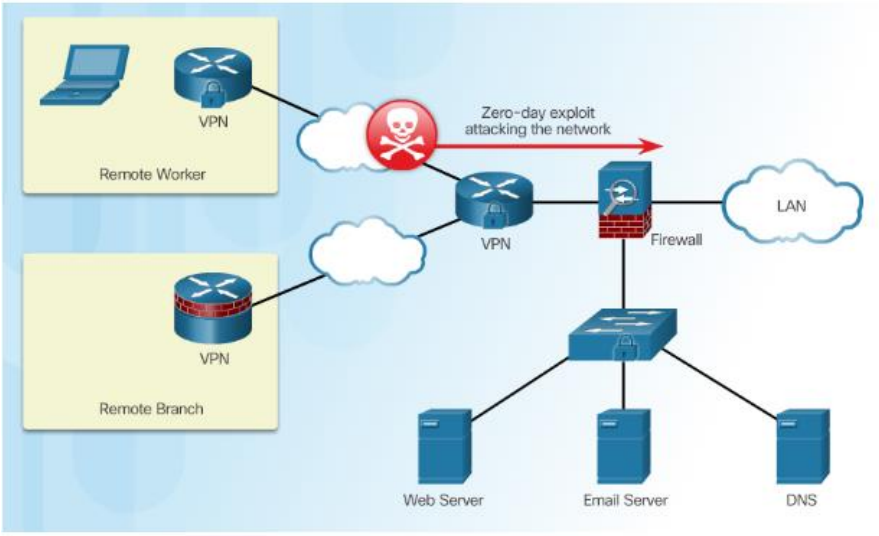
- კლიენტის მოქმედებების კონფიდენციალურობის უზრუნველყოფა.

ინფორმაციის კონფიდენციალობა ნიშნავს, რომ მასთან მიმართვა მხოლოდ მომხმარებელთა გარკვეული ჯგუფს შეუძლია. მთლიანობაში იგულისხმება ინფორმაციის ან პროგრამული უზრუნველყოფის თვისება შეინარჩუნოს თავისი სტრუქტურა და შინაარსი გადაცემის და შენახვის პროცესში.

ინფორმაციის სარწმუნოება მას მკაცრად მიაკუთვნებს ობიექტს, რომელიც მის წყაროს წარმოადგენს, ან იმ ობიექტს, რომლისაგანაც ეს ინფორმაციაა მიღებული. ოპერატიულობა განსაზღვრავს საინფორმაციო რესურსის უნარს იყოს მისაწვდომი საბოლოო მომხმარებლისათვის მისი მოთხოვნილების შესაბამისად.

ინფორმაციის იურიდიული მნიშვნელობა ნიშნავს, რომ დოკუმენტს გააჩნია იურიდიული ძალა. ამ მიზნით სუბიექტები, ვისთვისაც მნიშვნელოვანია გადაცემული გზავნილის იურიდიული მნიშვნელობა, თანხმდებიან ინფორმაციის იმ განსაკუთრებული ატრიბუტების საყოველთაო აღიარებაზე, რომლებიც გამოხატავენ მის იურიდიულ მნიშვნელობას. გზავნილების იურიდიული მნიშვნელობა განსაკუთრებით მნიშვნელოვანია ელექტრონული გადახდის სისტემებში, სადაც ხდება ფულის ელექტრონული გადარიცხვის ოპერაციები. დოკუმენტების იურიდიული მნიშვნელობის განმსაზღვრავი ატრიბუტები ერთმნიშვნელოვნად უნდა ადასტურებდნენ, რომ დოკუმენტი კონკრეტული პირის მიერაა გამოგზავნილი.

ოპერაციების კონფიდენციალურობის უზრუნველყოფა ნიშნავს, რომ მომხმარებელს აქვს საშუალება აწარმოოს ოპერაციები ისე, რომ არავის შეეძლოს მისი თვალთვალი. მსგავსი მოთხოვნის აქტუალურობა ცხადი გახდა ელექტრონული ფულის წარმოშობასთან ერთად. ელექტრონული ანგარიშსწორების სისტემასთან მიმართვისას მომხმარებელი აწვდის მას გარკვეულ საიდენტიფიცირო ინფორმაციას. ამ სისტემების ფართო გავრცელებასთან ერთად შესაძლოა გაჩნდეს ანგარიშსწორების ოპერაციების კონტროლირების და მომხმარებლებზე ტოტალური თვალთვალის საშიშროება სახელმწიფო სტრუქტურების ან სხვა დაინტერესებული პირების მხრიდან.



ამ პრობლემის გადაწყვეტის ერთი გზა საკანონმდებლო აქტებით საშუალებით საინფორმაციო სისტემების მომხმარებლებზე ყოველგვარი ტოტალური თვალთვალის აკრძალვაა. მეორე გზა კი სპეციალური კრიპტოგრაფიული მეთოდების გამოყენებაა.

როგორც უკვე აღვნიშნეთ საინფორმაციო უსაფრთხოება უნდა განვიხილოთ როგორც ინფორმაციის კონფიდენცი- ალურობის დაცვის, ასევე ინფორმაციული სისტემების მიერ მოცემული ფუნქციების შესრულების უნარის მხრივ. საინფორმაციო სისტემების გამართულად მუშაობისათვის საჭიროა უზრუნველვყოთ:

- სისტემაში არასანქცირებული შეღწევისაგან დაცვა;
- დაცვის შიდა და გარე სისტემების დაცვა გატეხვისაგან;
- მომხმარებლების და ქსელის მომსახურე პერსონალის მიერ სისტემაში არასანქცირებული მოქმედებებისაგან დაცვა;
- ავარიული სიტუაციების დროს სისტემის დაცვა მწყობრიდან გამოსვლისაგან.

საინფორმაციო-ტელეკომუნიკაციურ ქსელებში უსაფრთხოების უზრუნველყოფისათვის საჭიროა:

- ინფორმაციის დაცვა შენახვის, გადამუშავების და გადაცემის დროს;
- მონაცემების და მომხმარებლების სარწმუნოების დამოწმება (მხარეების აუტენტიფიკაცია);
- მონაცემების მთლიანობის დარღვევის აღმოჩენა და გაფრთხილება;

- ტექნიკური მოწყობილობების და სათავსოების დაცვა;

- კონფიდენციალური ინფორმაციის დაცვა სათვალთვალო მოწყობილობების საშუალებით მოპოვებისაგან და გაჟონვისაგან;

- პროგრამული პროდუქტების დაცვა ვირუსებისაგან და სხვა პროგრამული ჩანართებისაგან;

- არასანქცირებული შეღწევებისაგან საინფორმაციო სისტემების დაცვა.

საინფორმაციო რესურსების უსაფრთხოების უზრუნველყოფა კონკრეტულ შემთხვევაში შეიძლება გამოიხატოს ორგანიზაციული ან ტექნიკური მეთოდებით ინფორმაციის დაცვაში. ორგანიზაციული მეთოდები გულისხმობს პერსონალის უფლებამოსილებების ზუსტ განსაზღვრას მომხმარებლების მხრიდან. ინფორმირებას შესაძლო საფრთხის შესახებ, სამუშაო პროცესის ისეთ ორგანიზებას, რომ გამოირიცხოს კონფიდენციალური ინფორმაციის გაჟონვის შესაძლებლობა და სხვა. დაცვის ტექნიკური მეთოდები გულისხმობს ინფორმაციული სისტემების მუშაობის და ინფორმაციის შენახვის საიმედოობის გაზრდას (დუბლირება, სარეზერვო კოპირება და სხვა) ინფორმაციის კრიპტოგრაფიული დაცვის მეთოდებს შენახვის და გადაცემის პროცესში, აუტენტიფიკაციის პროგრამულ საშუალებებს, ქსელის დაცვას ქსელური ეკრანებით და შლუზებით და სხვა.

თანამედროვე დაცვის სისტემები საკმაოდ რთულია, მაგრამ რაღაც ზეჩვეულებრივი მაგათში მაინც არ არის, იმიტომ რომ ინფორმაციული ტექნოლოგიების განვითარებას ისინი ყოველთვის ჩამორჩებიან. წარმოუდგენელია ქსელთაშორისი ეკრანის არსებობა სისტემაში (Firewall) სადაც კომპიუტერები ერთმანეთთან არ არის დაკავშირებული, ან რა საჭიროა ანტივირუსი თუ არ არსებობს ვირუსული პროგრამები, მეტ- ნაკელებად სერიოზული დაცვითი ტექნოლოგიები ჩნდება ახალი ტექნოლოგიური სიახლეების შექმნის საპასუხოდ. უფრო მეტიც ზოგჯერ ტექნოლოგიური სიახლე არ ითხოვს აუცილებელ დაცვის სისტემის შექმნას, ის იქმნება მაშინ როდესაც გაჩნდება მაგის ფინანსური მიზანშეწონილობა. მაგალითად დაცვითი მეანიზმების შექმნა მონაცემთა ბაზების მართვის სისტემების კლიენტ-სერვერული მოდელისთვის აუცილებელია, იმიტომ რომ ის უშუალოდ მოქმედებს მომხმარებლებზე, რომლებიც სარგებლობენ აღნიშნული სისტემით. ხოლო დაცვითი ფუნქციების არ არსებობა მობილურ ტელეფონებში დიდად არ აისახება მათ გაყიდვებზე. აგრეთვე დაცვითი ტექნოლოგიების განვითარება გავლენას ახდენს "ჰაკერებზე". ეს გასაგებიცაა, რადგანაც ყველაზე გამოყენებად ტექნოლოგიებშიც კი მანამ არ შეიქმნება დაცვითი სისტემის სექმა, სანამ მათზე არ მოხდება ჰაკერული თავდასხმა. ნათელ მაგალითს წარმოადგენს უკებელო ქსელური ტექნოლოგია, რომელსაც არც თუ ისე დიდი ხნის წინ ქონდა, არც თუ ისე სერიოზული დაცვის სისტემა. მაგრამ ბოროტმოქმედების მოქმედებამ გამოაჩინა არსებულის სიტემის ხარვეზები, ამიტომ დაუყონებლივ

შეიქმნა სპეციალიზირებული დაცვის მექანიზმები და საშუალებები მაგალითად როგორიც არის ხარვეზების აღმომჩენები (სკანერები), შეტევის აღმომჩენი სისტემები და სხვა.

ურთიერთობის მიხედვით გამოიყენება სხვადასხვა დაცვითი ტექნოლოგიები, მაგალითად ინტერნეტთან კავშირისას არასდროს გამოვიყენებთ VPN (Virtual Private Network - ვირტუალური კერძო ქსელი) ტექნოლოგიას, მაგრამ როდესაც კავშირს ვანხორციელებთ დაშორებულ ფილიალებთან აღნიშნული ტექნოლოგია საკმაოდ მნიშვნელოვანია.

ინფორმაციული დაცვის ტექნოლოგიის შერჩევისას, მნიშვნელოვან გავლენას ახდენს კომპიუტერების რაოდენობა რომელიც გაერთიანებულია ქსელში. ქსელის მასშტაბი თავის წესებს კარნახობს- რადგან ფულის უკმარისობის გამო ვერ

ხერხდება საჭირო ინფორმაციული დაცვის სისტემების შეძენა, ისევე როგორც ზოგჯერ უკანასკნელის საჭიროების საერთოდ არ ქონის გამო. ასე რომ ერთი კომპიუტერი, რომელიც ჩართულია ინტერნეტის ქსელში არ სჭირდება კონფიდენციალური ინფორმაციის გაჟონვის საწინააღმდეგო კონტროლის სისტემა, როდესაც აღნიშნული სასიცოცხლოდ აუცილებელია უკვე მცირე კომპიუტერული ქსელის არსებობისას.

ინტერნეტის ხანაში კომპიუტერული ინფორმაციის უსაფრთხოება და ქსელური უსაფრთხოება ერთმანეტს შეერწყა. კომპიუტერული ინფორმაციის სრული დაცვა, რომელიც შეიზლება განისაზღვროს, როგორც დაუშებელი მოქმედებების აღმოფხვრა და გამოვლენა. აღნიშნულის გაკეთება კომპიუტერული სისტემის მომხმარებლების მხრიდან, გაცილებით რთული და ძნელია, ვიდრე მარტივი მათემატიკა კრიპტოგრაფიისა.

არსი მდგომარეობს იმაში რომ მხოლოდ მათემატიკას არ შეუძლია უზრუნველყოს სრული უსაფრთხოება. კრიპტოგრაფიაში დაცვას მატემატიკა აძლევს უდიდეს უპირატესობას ბოროტმოქმედებთან შედარებით. ერთი ბიტის დამატება გასაღებზე ორჯერ ართულებს მის გატეხვას, 10-ის მიახლოებით 1000-ჯერ როდესაც ლაპარაკი მიდის კომპიუტერულ უსაფრთხოებაზე ერთიანად, მხარეები იმყოფებიან თანაბარ მდგომარეობაში: ბოროტმოქმედებმა და დამცველებმა შესაძლებელია მიიღონ ტექნოლოგიისგან ერთდაიგივე მოგება, ეს იმას ნიშნავს, რომ თუ თქვენ გექნებოდათ საკმარისი კრიპტოგრაფია უსაფრთხოების უზრუნველსაყოფად, მაშინ თქვენ გექნებოდათ ყველაფერი წესრიგში, მაგრამ სამწუხაროდ უმრავლეს შემთხვევაში ეს ასე არ არის.

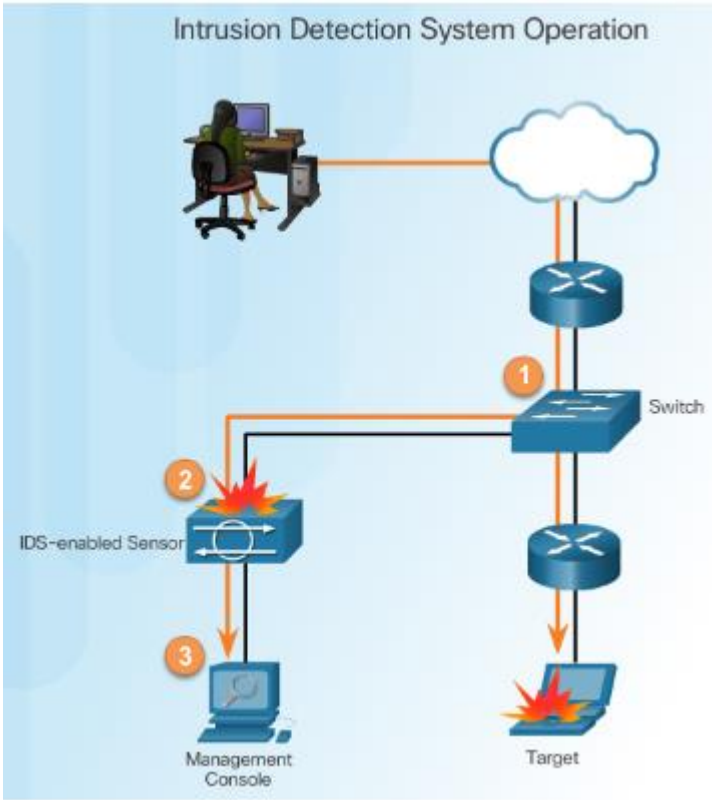
არსებობს უსაფრთხოების ბევრი თეორიული მოდელი, რომელთა უმრავლესობა ფინანსდებოდა ამერიკის თავდაცვის სამინისტროს მიერ და გამოიყენებოდა სამხედრო საიდუმლოების დაცვის მიზნით. ძირითადად ასეთი სისტემები არის

მრავალდონიანი, იმიტომ, რომ ისინი გამოიყენება მრავალი დონის საიდუმლოების მხარდასაჭერად.

თანამედროვე თავდასხმების კლასიფიკაცია და მათთან ბრძოლის მეთოდები

ინტერნეტის პოპულარიბის კოლოსალურ ზრდასთან ერთად, წარმოიქმნა პერსონალური ინფორმაციის, კრიტიკულად მნიშვნელოვანი კორპორაციული რესურსების, სახელმწიფო საიდუმლოების და სხვა ინფორმაციის გაჟონვის უპრეცედენტო საშიშროება. ყოველ დღე ჰაკერები ამ რესურსებს უქმნიან საშიშროებას. და ცდილობენ მიიღონ ეს ინფორმაცია თავდასხმის სხვადასხვა გზების გამოყენებით, რომლებიც ერთი მხრივ ხდებიან უფრო და უფრო დახვეწილები და მეორე მხრივ - მარტივი გამოსაყენებლად. ამას განაპირობებს ორი ფაქტორი.

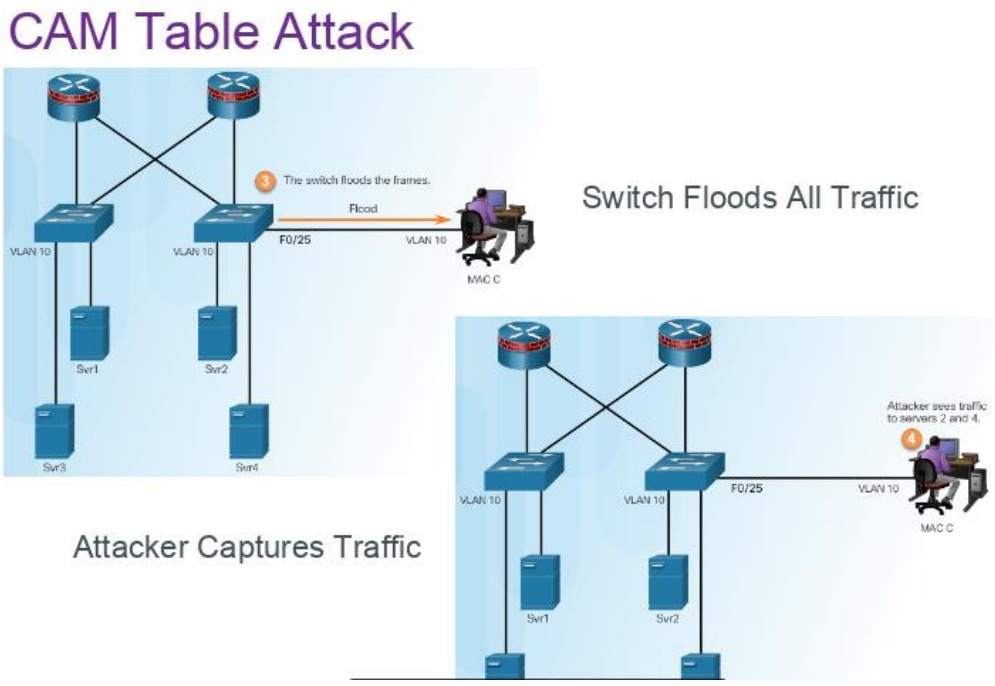
პირველი: ეს არის ინტერნეტში ყოველმხრივი შეღწევადობა. დღესდღეისობით ქსელებში დაკავშირებულია მილიონობით მოწყობილობა და კიდევ მარავალი მილიონი ჩაერთვება უახლოეს მომავალში. ამიტომ ნაკლოვან მოწყობილობებშიც ჰაკერების შეღწევის ალბათობაც იზრდება. აგრეთვე ინტერნეტის ფართოდ გავრცელება ჰაკერებს აძლევს შესაძლებლობას გაცვალონ ინფორმაცია გლობალურ მასშტაბში.



მეორე: ეს არის გამოყენებისთვის მარტივი ოპერაციული სისტემების

და მათი შექმნის საშუალებების გავრცელება. აღნიშნული ფაქტორი ამცირებს ჰაკერის აუცილებელი განათლებას დონეს. მანამდე, რომ შექმნილიყო და გავრცელებულიყო მარტივი გამოყენებითი პროგრამა ჰაკერს უნდა ქონოდა კარგი განათლება პროგრამირებაში. ახლა რომ მივიღოთ წვდომა ჰაკერული საშუალებებზე, საჭიროა მხოლოდ საიტის IP მისამართის ცოდნა და რომ განვახორციელოთ შეტევა უბრალოდ საჭიროა დავაწკაპუნოთ მაუსს.

ქსელური თავდასხმები იმდენად მრავალგვარია, ისევე როგორც სისტემები, რომლის წინააღმდეგაც ისინი არიან მიმართული. ზოგიერთი შეტევა გამოირჩევა დიდი სირთულით. შეტევის ტიპების შეფასებისას აუცილებელია ვიცოდეთ ზოგიერთი შეზღუდვები, თავდაპირველად რომელსაც მივყავართ Tcp/Ip პროტოკოლამდე -მდე. ინტერნეტი შეიქმნა იმისათვის, რომ დაკავშირებულიყო სახელმწიფო ორგანიზაციები და უნივერსიტეტები და გაეწია დახმარება სასწავლო პროცესისთვის და მეცნიერული გამოკვლევებისათვის. ამ ქსელის შემქმნელები არ ელოდებოდნენ მის ასე გავრცელებას. შედეგად ინტერნეტის პროტოკოლის ადრეულ სფეციფიკაში არ იყო უსაფრთხოების მოთხოვნა გათვალისწინებული. რამდენიმე წლის შემდეგ, საბოლოლოდ დაიწყეს უსაფრთხოების ზომების დანერგვა, იმის გათვალისწინებით რომ თავიდანვე არ იყო გათვალისწინებული უსაფრთხოების ზომები, ამიტომ ამის გაკეთება დაიწყეს სხვადსხვა საშუალებებით და პროცედურებით, რომ დაეწიათ რისკი, რომელსაც შეიცავდა ეს პროტოკოლები. შემდგომში დაწვრილებით განვიხილავთ შემთხვევებს დაკავშირებულს IP ქსელების წინააღმდეგ და ჩამოვთვლით მათ საწინააღმდეგო ხერხებს.



```
macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

ფაიერვოლი

ფაიერვოლი ღებულობს გადაწყვეტილებას პაკეტის გატარების ან დაბლოკვის შესახებ წესების ბაზის საფუძველზე. ადმინისტრატორის მოვალეობაა შექმნას ისეთი წესების ბაზა, რომელიც შეესაბამება კონკრეტულ ქსელს და ქსელში არსებულ სერვისებს.

ფაიერვოლი განიხილავს წესებს მათი ნომრების ზრდადობის მიხედვით. თუ პაკეტი შეესაბამება მოცემულ წესს, მაშინ ფაიერვოლი ან ატარებს ამ პაკეტს ან ბლოკავსმას. შემდეგ წესებს ის აღარ განიხილავს. ქსელის დონეზე მომუშავე ფაიერვოლის წესი შედგება შემდეგი ველებისგან:

1. წესის ნომერი

2. მოქმედება

3. პროტოკოლი

4. გამგზავნის ჰოსტის ან ქსელის მისამართი

5. გამგზავნის პორტის ნომერი ანინტერვალი

6. ადრესატის ჰოსტის ან ქსელის მისამართი

7. მიმღების პორტის ნომერი ან ინტერვალი

შესაძლებელია ამ წესებში იყოს ინფორმაცია, რომელიც დამოკიდებულია კონკრეტულ პროტოკოლზე, მაგალითად TCP პროტოკოლისათვის — ინფორმაცია სესიის მდგომარებოაზე, ICMP პროტოკოლისათვის — ინფორმაცია პაკეტის ტიპზე და ა.შ.

ზემოთ ჩამოთვლილი ველებიდან აუცილებელია მხოლოდ პირველი ხუთი. დანარჩენების მითითება აუცილებელი არ არის თუ ამას სიტუაცია არ მოითხოვს. განვიხილოთ რა მნიშვნელობები შეიძლება მიიღოს თითოეულმა ველმა და თუ რა მოთხოვნებს უნდა აკმაყოფილებდნენ ისინი.

1. **წესის ნომერი** – რიცხვი 1-დან 65534-მდე. (ფაიერვოლში შესაძლო წესების რაოდენობა დამოკიდებულია კონკრეტული რეალიზაციაზე. აქ მოყვანილია მნიშვნელობები FreeBSD ოპერაციული სისტემის ქვეშ მომუშავე IPFW

ფაიერვოლისთვის).

2. მოქმედება — შესაძლებელია ორი მოქმედება: გატარება

(permit, allow, pass) ან დაბლოკვა (deny).

3. პროტოკოლი — შეიძლება მიიღოს შემდეგი მნიშვნელობები: IP, TCP, UDP, ICMP და სხვა.

4. გამგზავნის მისამართი — აუცილებელია ჩაიწეროს ქსელის მისამართი შესაბამისი ნიღბით (Network Mask) ან ჰოსტის მისამართის შემთხვევაში წინ მიეწეროს სიტყვა: "host". ნიღაბი შეიძლება ჩაიწეროს ორნაირად — ათობითი ფორმატის მისამართის თითოელ ბაიტში ქსელის ნაწილის მითითებით (მაგალითად: 255.255.255.252), ან უბრალოდ ქსელის ნიღაბში ერთიანების რაოდენობის მითითებით (/30).

პაკეტების სნიფერი

პაკეტების სნიფერი წარმოადგენს გამოყენებით პროგრამას, რომელიც იყენებს ქსელურ ადაპტერს, რომელიც მუშაობს თვალთვალის რეჟიმში (Promiscuous mode - ამ რეჟიმში ადაპტერი ყველა პაკეტს, მიღებული ფიზიკური არხის მიერ, უგზავნის აპლიკაციას დამუშავებისათვის) ამ დროს სნიფერი იჭერს ყველა ქსელურ პაკეტს, რომელიც გადაიცემა განსაზღვრულ დომეინში. ამ დროისთვის სნიფერები ქსელებში სავსებით კანონიერად მუშაობენ ქსელებში. ისინი გამოიყენება დიაგნოსტიკისათვის და ტრაფიკის ანალიზისათვის, მაგრამ თუ მხედველობაში მივიღებთ იმას, რომ ზოგიერთი ამლიკაცია გადასცემს მონაცემებს ტექსტურ ფორმაში (Ftp, Telnet, SMTP, POP3 და სხვა) სნიფერის საშუალებით შესაძლებელია გავიგოთ კონფიდენციალური ინფორმაცია (მაგ. მომხმარებლის სახელი და პაროლი).

სახელებისა და პაროლის დადგენა იძლევა დიდ საშიშროებას, რადგანაც მომხმარებლები ხშირად იყენებენ ერთი და იგივე სახელს და პაროლს მრავალი პროგრამისთვის, მრავალ მომხმარებელს საერთოდ აქვს მხოლოდ ერთი სახელი და პაროლი. თუ პროგრამა მუშაობს როგორც კლიენტ-სერვერი, ხოლო აუტენტიფიცირებული მონაცემები გადაეცემა ქსელის საშუალებით და კითხვადი ტექსტური ფორმატით, მაშინ ეს ინფორმაცია დიდი ალბათობით შეიძლება გამოყენებულ იქნას კორპორატიულ და გარე რესურსებზე წვდომისათვის (შეტევის მეთოდები ხშირად ბაზირდება სოციალური ინჟინერიის საფუძველზე). მათ კარგად აქვთ წარმოდგენილი, რომ ჩვენ ვიყენებთ ერთი და იგივე პაროლს მარვალი რესურსის წვდომისათვის, ჩვენი პაროლის გაგებით, მას შეუძლია ჩვენი რესურსის გამოყენება ყველაზე ცუდ ვარიანტში ის მიიღებს წვდომას სამომხმარებლო დონეზე და მისი სასუალებით შექმნის ახალ მომხმარებელს, რომლის საშუალებით მას შეეძლება ნებისმიერ მომენტში შემოვიდეს ქსელში და მის რესურსებში.

პაკეტების სნიფინგის საშიშროების დასაწევად შესაძლებელია გამოვიყენოთ შემდეგი საშუალებები:

აუტენტიფიკაცია

აუტენტიფიკაციის ძლიერი საშუალებები წარმოადგენენ მნიშვნელოვან ხერხს, პაკეტების სნიფინგის წინაღმდეგ. ”ძლიერი” საშუალებების ქვეშ იგულისხმება ისეთი მეთოდები, რომლისთვის გვერდის ავლა ძნელად შესაძლებელია.

მაგალითად ისეთი აუტენტიფიკაციისა არის ერთჯერადი პაროლები (One Time Passwords, OTP) OTP- ეს არის აუტენტიფიკაციის ორფაქტორიანი ტექნოლოგია, რომლის დროსაც ხდება გათვალისწინება იმისა რაც თქვენ გაქვთდა იმასა რაც თქვენ იცით, ტიპიური მაგალითია ორფაქტორიანი აუტენტიფიკაცისა წარმოადგენს ბანკომატი, რომელიც ამოგიცნობთ თქვენ, ჯერ ერთი თქვენი პლასტიკური ბარათით და მეორე თქვენი პინ კოდით. აუტენტიფიკაციისათვის OTP- სისტემაში აგრეთვე მოითხოვება პინ კოდი და თქვენი პირადი ბარათი. ”ბარათი”(Token) ის ქვეშ იგულისხმება აპარატურულ ან პროგრამული საშუალება, რომელიც აგენირირებს უნიკალურ(შემთხვევითი შერჩევის პრინციპით) ერთმომენტიან, ერთჯერად პაროლს. თუ ჰაკერი გაიგებს მოცემულ პაროლს სნიფერის საშუალებით, მისთვის ეს ინფორმაცია იქნება გამოუსა- დეგარი, რადგანაც ეს პაროლი უკვე იქნება გამოყენებული და უვარგისი შემდგომი გამოყენებისთვის ავღნიშნოთ, რომ ეს ხერხი სნიფინგის საწინააღმდეგოდ საბრძოლველად ეფექტურია მხოლოდ პაროლის დაჭერის შემთხვევაში, სნიფერი, რომელიც დაჭერს სხვა ინფორმაციას (მაგ. ელ ფოსტის ინფორმაციას) არ კარგავს თავის ეფექტურობას.

აუტენტიფიკაციის პროტოკოლი. აუტენტიფიკაცია ამოწმებს კომუნიკაციის დროს პირის უტყუარობას. დაშორებული პროცესის უტყუარობის შემოწმება ითხოვს რთულ პროტოკოლებს, დამყარებულს კრიპტოგრაფიაზე.

აღსანიშნავია, რომ ხშირად ერთმანეთში ურევენ აუტენტიფიკაციას და ავტორიზაციას. აუტენტიფიკაცია დაკავებულია მოსაუბრის უტყუარობის შემოწმებით, ავტორიზაციას კი საქმე აქვს ნებართვებთან. მაგალითად პროგრამა კლიენტი მიმართავს ფაილურ სერვერს და ეუბნება: "მე ვარ პროცესი A და მინდა test.doc ფაილის წაშლა". ფაილურმა სერვერმა უნდა გადაწყვიტოს:

1. არის თუ არა სინამდვილეში ეს პროცესი A? (აუტენტიფიკაცია)
2. აქვს თუ არა A-ს test.doc ფაილის წაშლის უფლება? (ავტორიზაცია)

მხოლოდ იმის შემდეგ, რაც ორივე კითხვაზე იქნება არაორაზროვანი პასუხი

გაცემული, შესაძლებელია განხორციელდეს მოთხოვნილი მოქმედება. მნიშვნელოვანი არის პირველი კითხვა. მას შემდეგ, რაც სერვერმა იცის თუ ვის ელაპარაკება, უფლების შესამოწმებლად საჭიროა მხოლოდ ცხრილების ლოკალურად შემოწმება.

ყველა აუტენტიფიკაციის პროტოკოლის მიერ გამოყენებული საერთო სქემა შემდეგნაირია:

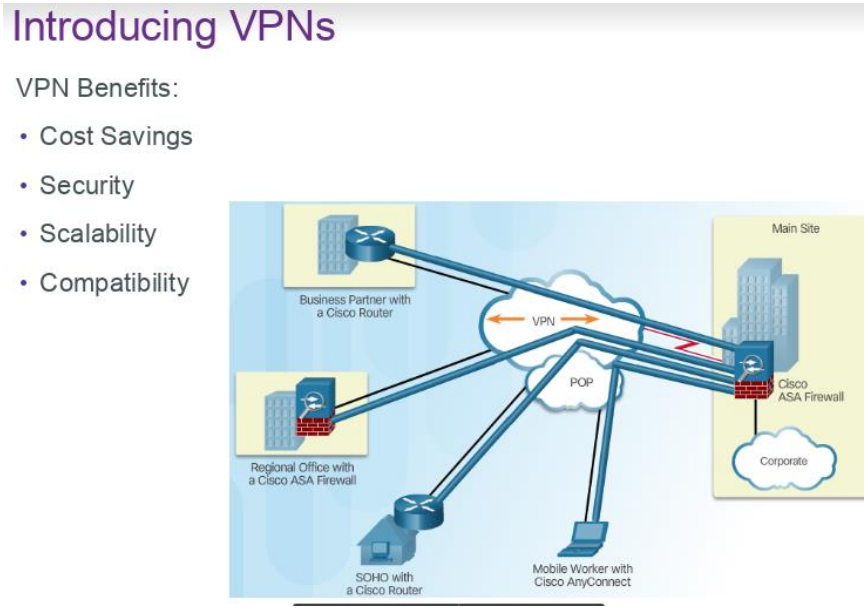
მომხმარებელს (პროცესს) A-ს, სურს დაამყაროს დაცული კავშირი მეორე მომხმარებელთან, B-სთან. B ბანკირია და A-ს უნდა მასთან საქმიანი გარიგება. A იწყებს იმით, რომ უგზავნის B-ს შეტყობინებას, ან ნდობით აღჭურვილ გასაღებების გამავრცელებელ ცენტრს (KDC – key distribution center). შემდეგ მრავალი მიმართულებით აგზავნის კიდევ რამოდენიმე შეტყობინებას. ამის შემდეგ ბოროტმიქმედმა შეიძლება დაიჭიროს, შეცვალოს და ხელახლა შექმნას ეს შეტყობინება იმისათვის, რომ მოატყუოს A და B ან უბრალოდ ჩაშალოს გარიგება.

ასე თუ ისე, როდესაც პროტოკოლი ამთავრებს თავის მუშაობას, A უნდა იყოს დარწმუნებული, რომ ელაპარაკება B-ს, ხოლო B — კი A-ს. ბევრ პროტოკოლში მოსაუბრეები ქმნიან სეანსის საიდუმლო გასაღებს, რომლითაც მომხმარებლები გაცვლიან შემდგომ ინფორმაციას. პრაქტიკაში მონაცემთა ყველა გაცვლა იშიფრება სიმეტრიული ალგორითმის გამოყენებით,

ვირტუალური კერძო ქსელი (VPN ტექნოლოგია)

VPN- ის ძირითადი მიზანი არის თქვენი მონაცემების უსაფრთხო გვირაბის შექმნა, რომელიც გადაეცემა სერვერებს ინტერნეტში გადასვლამდე. თუმცა, ამან გამოიწვია ზოგიერთი სხვა სარგებელი, როგორიცაა ადგილმდებარეობა spoofing.

მიუხედავად იმისა, რომ ეს ჩანდეს უმნიშვნელოა, ბევრჯერ არის ადგილი, როდესაც საიდან spoofing დაეხმარა ხალხს გადალახოს geo- ადგილმდებარეობა ბარიერები. მიიღეთ ჩინეთის დიდი ხანძარიმაგალითად. ჩინეთის მთავრობა სერიოზულად უწოდებს ინტერნეტს და ბევრ რამეს მივუახლოვდებით ინტერნეტში ინტერნეტში დაბლოკილია ჩინეთში. მხოლოდ VPN- ის გამოყენებით შეუძლია ჩინეთში დაფუძნებული მომხმარებლებს წვდომა საიტები, როგორიცაა Google და Facebook.



თანატოლებისთვის (P2P) მომხმარებლებისთვის, საიდენტიფიკაციო რისკის გარდა, თქვენ ასევე აწარმოებთ თქვენი პორტის რუკების რისკებს Torrenting- ის მეშვეობით. VPNs დაეხმარება ნიღაბს ამგვარად, რომ თქვენი ღია პორტები ადვილად ვერ გამოიყენონ.

VPN-ების პირველი და უპირველესი მიზანი დღეს ანონიმურობაა. თქვენი მოწყობილობიდან უსაფრთხო გვირაბის შექმნისა და სერვერების უსაფრთხოდ შექმნით და მონაცემთა გადასატანად, რომელიც გვირაბით გადის, VPN- ები ეფექტურად იყენებენ თქვენს მონაცემებს.

ანონიმურობა

ეს იმას ნიშნავს, რომ ვინმეს ცდილობთ მოძებნოთ ის, რასაც აკეთებ ინტერნეტში, მაგალითად, თქვენს მიერ მონახულებულ საიტებზე და ა.შ. VPNs იმდენად ფოკუსირებულია ანონიმურობით, რომ დღეს ბევრი მათგანი გადაიხდის გადასახადების მიღებას, რაც არ უნდა იყოს traced, როგორიცაა crypto ვალუტა და საჩუქარი სერთიფიკატები.

spoofing

იმის გამო, რომ VPN მომსახურება აქვს სერვერების ბევრ ადგილას მთელს მსოფლიოში, მიერ დამაკავშირებელი იმ სერვერების შეგიძლიათ 'spoof' თქვენი ადგილმდებარეობა, როგორც იგივე, რაც VPN სერვერზე.

უსაფრთხოება

ბევრი VPN მომსახურება დღესაც იწყება უფრო მეტი უსაფრთხოების ზომების განხორციელება მათი მომხმარებლებისთვის. იგი ძირითადად დაიწყო ონლაინ მონაცემთა შეგროვებისა და თვალთვალის დაბლოკვაში, მაგრამ ახლა გაფართოვდა რეკლამის ბლოკირება და ზოგიერთ შემთხვევაში კი ანტივირუსული გადაწყვეტილებებიც კი.

VPN პროტოკოლები

მიუხედავად იმისა, რომ არსებობს მრავალი საკომუნიკაციო ოქმები, არსებობს ზოგადი პირობა, რომლებიც ხშირად მხარს უჭერენ VPN სერვისის ბრენდის მიუხედავად. ზოგი უფრო სწრაფია, ზოგი ნელა, ზოგი უფრო უსაფრთხოა, სხვები ნაკლებად არიან. არჩევანი შეესაბამება თქვენს მოთხოვნებს, ასე რომ, ეს შეიძლება იყოს კარგი სექცია, რომ ყურადღება მიაქციოთ თუ თქვენ აპირებთ VPN- ს გამოყენებას.

OpenVPN: ღია ოქმის ოქმი, რომელიც საშუალო სიჩქარე ჯერ კიდევ გთავაზობთ ძლიერი დაშიფვრის მხარდაჭერა.

L2TP / IPSec: ეს არის საკმაოდ გავრცელებული და გთავაზობთ ღირსეული სიჩქარით, მაგრამ ადვილად დაბლოკილია ზოგიერთი საიტები, რომლებიც არ უჭერენ მხარს VPN მომხმარებლებს.

SSTP: არც ისე საყოველთაოდ ხელმისაწვდომი და გარდა კარგი შიფრირების არ აქვს ბევრი რეკომენდაციას თავად.

IKEV2: ძალიან სწრაფი კავშირი და განსაკუთრებით კარგი მობილური მოწყობილობებისთვის, თუმცა სუსტი დაშიფვრის სტანდარტებს სთავაზობს.

PPTP:

	შიფრაცია	უსაფრთხოების	სიჩქარის
OpenVPN	256-bit	ყველაზე მაღალი კოდირება	სწრაფი მაღალი შეყოვნების კავშირი
L2TP	256-bit	ყველაზე მაღალი კოდირება	ნელი და უაღრესად პროცესორი დამოკიდებული
SSTP	256-bit	ყველაზე მაღალი კოდირება	ნელი
IKEV2	256-bit	ყველაზე მაღალი კოდირება	სწრაფი
PPTP	128-bit	მინიმალური უსაფრთხოება	სწრაფი

მიუხედავად ამისა, OpenVPN გახდა ძალიან მნიშვნელოვანი და რჩება ერთ-ერთი ყველაზე უსაფრთხო ოქმები. იგი მხარს უჭერს ძალიან მაღალი შიფრირების დონის ჩათვლით, რაც ითვლება, როგორც "შეუვალი" 256- ის საკვანძო კოდირებით მოითხოვს 2048-bit RSA ამოცნობის და 160- ის სიმებიანი SHA1 ალგორითმი.

არსებობს უამრავი VPN სერვისის პროვაიდერები out there, ასე რომ, როდესაც სავაჭრო მომსახურების მიმწოდებელი მნიშვნელოვანია გვახსოვდეს ზუსტად რა

თქვენი მოთხოვნები. თუ თქვენ უბრალოდ ცდილობს გარკვეული ცენზურის ფარდების გვერდის ავლით, უფრო იაფი ალტერნატივებია, როგორიცაა HTTP / HTTPS პროქსი.

VPNs არის ყველაზე მაღალი ფორმა ნორმალური მომხმარებელთა კონფიდენციალურობის და ანონიმურობის დაცვა, ისინი განკუთვნილია შენარჩუნება თქვენ უსაფრთხო, უსაფრთხო და უზრუნველყოს, რომ თქვენი ათვალიერებს საქმიანობის ინახება პირადი. თუმცა, თითოეული პროვაიდერი თავად იცის, რომ ისინი განკუთვნილია გარკვეული მიზნებისათვის.

მიიღეთ მაგალითად TorGuard, რომელიც ძირითადად ნიშნავდა იმ ადამიანებს, ვინც მუდმივად იყო Peer-to-Peer (P2P) ფაილის გაზიარების ქსელები. ამასთან, მოდით შევხედოთ კონკრეტულ სფეროებში VPNs თქვენ უნდა გაითვალისწინოს, როდესაც შეფასების ერთი.

ანონიმურობა

მიუხედავად იმისა, რომ მართალია, ინტერნეტ უკვე გარშემო ასაკის, ტექნოლოგია უკვე ვითარდება სწრაფად. დღეს, კომპანიები მთელს მსოფლიოში იწყებენ თვალყური მომხმარებლებს ციფრულად, რათა დაეხმაროს მათ მონაცემთა ანალიზი. ზოგიერთ შემთხვევაში, მთავრობები უკვე ცნობილია ან ეჭვობენ, რომ თვალთვალის მომხმარებელი ციფრულად.

თუ ფიქრობთ, რომ ეს არ მოხდება თქვენთან, რადგან თქვენ ცხოვრობთ X ქვეყანაში, რაც მშვენიერია, კვლავ იფიქრეთ.

არსებობს ცნობილი სამთავრობო მეთვალყურეობა პროექტები ხორციელდება ქვეყნებში, როგორც შემაკავებელი, როგორც ჩინეთი და რუსეთი, ნეიტრალური შვეიცარიის ყველა გზა!

თქვენ შეგიძლიათ გააკონტროლოთ ელ-ფოსტით, ვებ-გვერდებზე დარეგისტრირება და დიახ, ვებსაიტზე ნებისმიერი ადგილის მონახულებაც კი. საშიში, არა?

ეს არის VPN სერვისის ერთ – ერთი ძირითადი ფუნქცია, რომელიც დაგეხმარებათ ინტერნეტში ანონიმურობის შენარჩუნებაში. ამას აკეთებს ის თქვენი IP მისამართის დამალვათქვენი მდებარეობის ნიღაბი, მონაცემების დაშიფვრა, რომელიც გადაეცემა თქვენსა და ინტერნეტს შორის და იმის უზრუნველსაყოფად, რომ თავად პროვაიდერიც კი არ აკონტროლებს თქვენს მიერ გაკეთებულ საქმეს (უმეტეს შემთხვევაში).

მეტი VPN მომსახურების დღესაც იღებენ მიღების ანონიმური გადახდის პარამეტრები, როგორიცაა crypto ვალუტა და ფულადი, ან საჩუქარი სერთიფიკატები.

პირადად, ერთი ნივთის შენარჩუნება მე არ მაქვს არწივის თვალი, ის არის ქვეყანა, სადაც VPN რეგისტრირებულია მის საქმიანობასთან. ბევრი VPN- ის მტკიცებით, ისინი არ იმოქმედებს მომხმარებლის აქტივობაზე, მაგრამ ზოგიერთ ქვეყანაში

სავალდებულოა მონაცემთა შეკავების კანონები. მირჩევნია აირჩიოს VPN პროვაიდერი, რომელიც რეგისტრირებულია ქვეყანაში, სადაც კანონი VPN მხარეს, როგორიცაა პანამა ან ბრიტანეთის ვირჯინიის კუნძულები მაგალითად.

რეკომენდებული VPN საუკეთესო ანონიმურობისთვის:

- NordVPN - პანამაში დაფუძნებული კომპანია ქვეყნის იურისდიქციას ექვემდებარება და პანამა არ აქვს მონაცემთა შენახვის კანონებს.
- ზედაპირზე - Surfshark იღებს ყველა მნიშვნელოვან საკრედიტო ბარათის გადახდას (VISA, Master, AMEX, Discover) და სხვადასხვა ანონიმური გადახდის ვარიანტები, მათ შორის Bitcoin, GooglePay და AliPay.

უსაფრთხოება

Encryption პროტოკოლები საწყისი აშენებული უსაფრთხოების მახასიათებლები VPN კლიენტის პროგრამული უზრუნველყოფა, VPNs დღეს გთავაზობთ უსაფრთხოების ბევრ დონეზე. რა თქმა უნდა, ყველაზე კრიტიკული არის უსაფრთხოებისა და მთლიანობის კავშირი, რომელიც ინარჩუნებს შენს და ინტერნეტს შორის.

კიდევ ერთი ფუნქცია, რომელიც ბევრ VPN მომსახურების გთავაზობთ გთავაზობთ მკვლელობის შეცვლას. ეს ნიშნავს, რომ ნებისმიერ დროს თქვენი აპარატისა და VPN სერვერს შორის კავშირის დაშლა ან დაკარგა რაიმე მიზეზით, VPN კლიენტი შეაჩერებს ყველა მონაცემს, რომელიც გამოდის ან თქვენს მოწყობილობაზე მოდის.

Ghosting

VPN- ები დიდი ხნის მანძილზე იყვნენ, რომ ზოგიერთი ვებსაიტი ან თუნდაც მთავრობებს გამოცდილება აქვთ VPN- ის აქტივობის აღიარებაში. VPNs- ის მომსახურების მიმწოდებლებმა ასევე იციან ეს ფუნქცია, რომლებმაც გააცნეს Stealth, Ghosting ან VPN Obfuscation (ტერმინოლოგია მერყეობს, მაგრამ ისინი ზოგადად ნიშნავს იგივე). ეს ხელს უწყობს სისტემებს, რომლებიც აქტიურად ეძებენ VPN მომხმარებლებს.

ორმაგი VPN

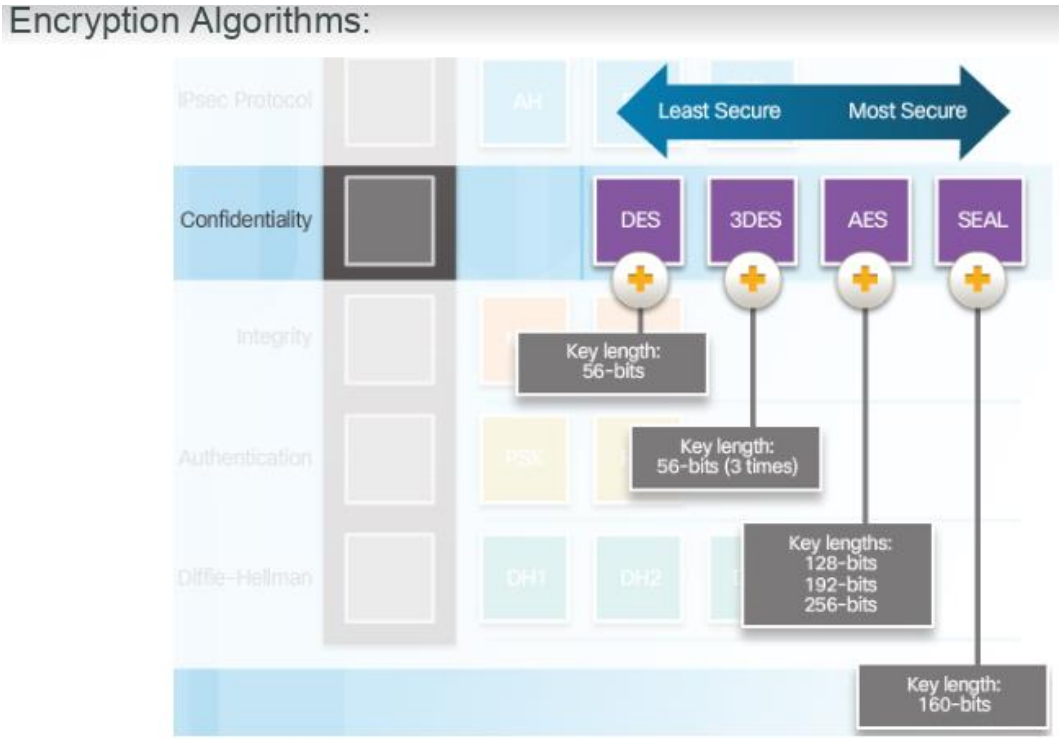
ზოგიერთი VPNs წასვლა დიდი lengths, რათა დაეხმაროს მათ მომხმარებელს დამალვა მათი ვინაობა და არ მოდის ერთად ფუნქცია მოუწოდა ორმაგი VPN. ეს იმას ნიშნავს, რომ თქვენ დაუკავშირდით ერთ VPN სერვერს და კავშირი შემდეგ როუტერის მეშვეობით სხვა VPN სერვერზე ადრე დარტყმის ინტერნეტში. გარდა მარშრუტიზაციისა, შიფრაცია ორჯერ გაორმაგებულია, რაც დამატებით უსაფრთხოების დამატებით ფენას ქმნის.

1) PPთP (Pოინტ-ტო-Pოინტ თუნნელინგ Pროტოცოლ) – `წერტილი-წერტილი" გვირაბული პროტოკოლია და გამოიყენება როგორც გამფართოებელი PPP (Pოინტ-ტო-Pოინტ Pროტოცოლ). გამოიყენება ინფორმაციის შეკუმშვისა და გაშიფრვისათვის. პროტოკოლის სტანდარტული ამორჩევისას შესაძლებელია

გამოვიყენოთ გაშიფრვის მეთოდი MPPE (Microsoft Point-to-Point Encryption).

შესაძლებელია მონაცემების გადაცემა გაშიფრვის გარეშე, გახსნილი სახით. მოცემული პროტოკოლით ინკაპსულაცია ხდება სათაურის დამატებით GrE (Generic Routing Encapsulation) და IP-ს სათაური, რომელიც მუშავდება PPP პროტოკოლით.

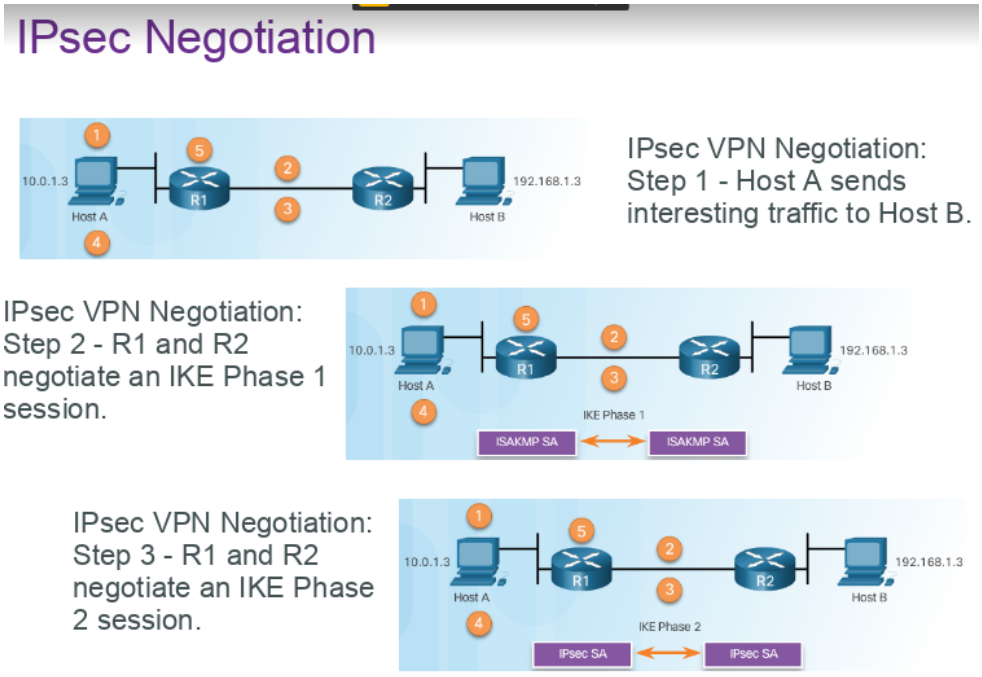
2) L2P – რომელიც შექმნილია PPP (Microsoft) და L2F (Cisco) პროტოკოლების გაერთიანებით, წარმოადგენს უფრო დაცულ შეერთებას. გაშიფრვა ხდება IPsec პროტოკოლით. L2P წარმოადგენს დაშორებული დაშვების კლიენტისათვის ჩაშენებულს კლიენტი დასაწყისში ცდილობს მიუერთდეს სერვერს ამ პროტოკოლით, როგორც უფრო უსაფრთხო. მონაცემების ინკაპსულაცია ხდება სათაურის დამატებით L2 და IP მონაცემებთან რომელიც დამუშავებულია PPP პროტოკოლით. მონაცემთა გაშიფვრა ხდება ალგორითმით DES (Data) ან 3DES, რის შედეგადაც მიიღწევა გადაცემული



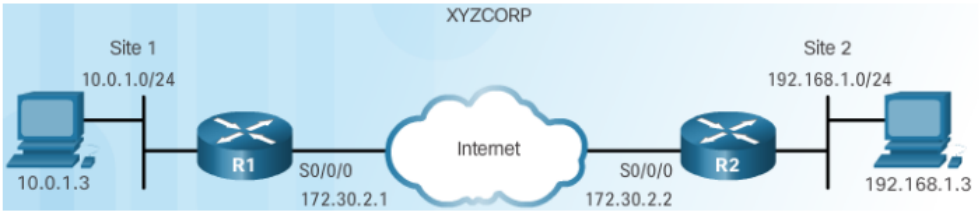
ინფორმაციული ტექნოლოგიების განვითარების თანამედროვე პირობებში კომპიუტერული ვირტუალური კერძო ქსელების შექმნის აუცილებლობა კონკურენტგარეშეა. კომპიუტერული VPN ძირითად უპირატესობას წარმოადგენს: – სისტემის მასშტაბურობა. ახალი ფილიალის გახსნისას ან ფირმის ახალი თანამშრომლისთვის, რომელსაც უფლება აქვს ისარგებლოს დაშორებულ დაშვებასთან, არ სჭირდება დამატებითი ხარჯები კომუნიკაციისათვის; – სისტემის მოქნილობა. კომპიუტერულ VPN-თვის მნიშვნელობა არ აქვს ფირმის თანამშრომელი საიდან

ახორციელებს დაშვებას. გამოიყენება მობილური ოფისები, სადაც არ არის საჭირო განსაზღვრული ადგილის შერჩევა; სამუშაო ადგილის ორგანიზაციისათვის თანამშრომელი გეოგრაფიულად არ არის შემოსაზღვრული კერძო ქსელის გამოყენებაზე.

კიბერთავდაცვის პრევენციული სისტემის (IPS) დანერგვა



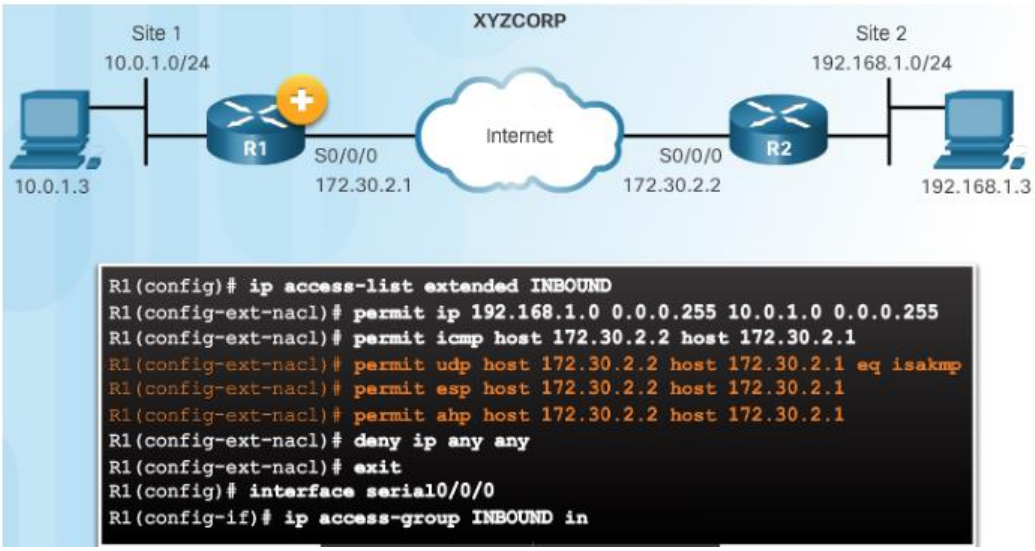
IPsec VPN Configuration Tasks



XYZCORP Security Policy	Configuration Tasks
Encrypt traffic with AES 256 and SHA	1. Configure the ISAKMP policy for IKE Phase 1
Authentication with PSK	2. Configure the IPsec policy for IKE Phase 2
Exchange keys with group 24	3. Configure the crypto map for IPsec policy
ISAKMP tunnel lifetime is 1 hour	4. Apply the IPsec policy
IPsec tunnel uses ESP with a 15-min. lifetime	5. Verify the IPsec tunnel is operational

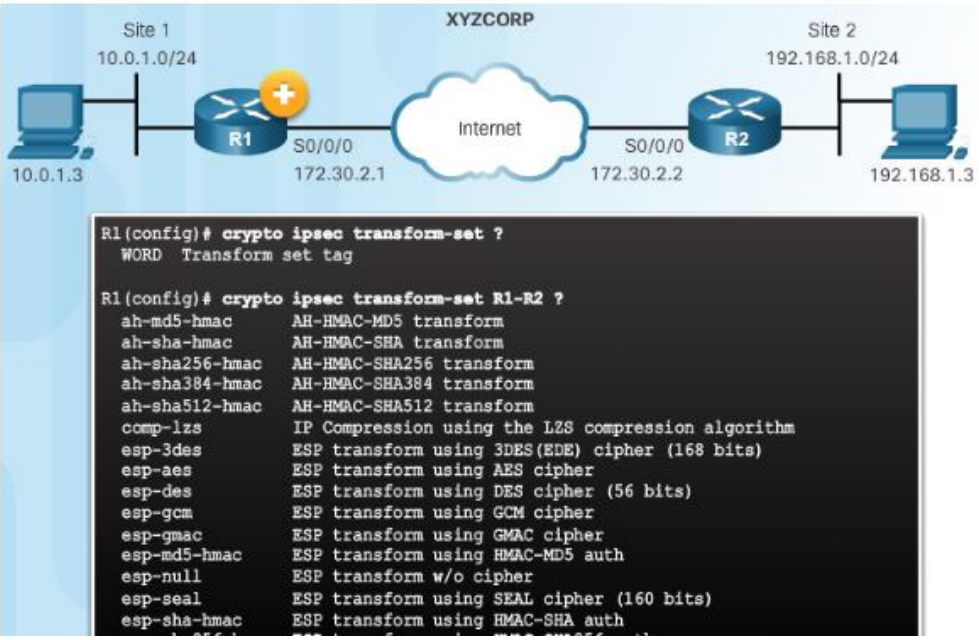
Existing ACL Configurations (Cont.)

Permitting Traffic for IPsec Negotiations



Configure IPsec Transform Set

The `crypto ipsec transform-set` Command



Syntax to Configure a Crypto Map

```
Router(config)#
crypto map map-name seq-num [ipsec-isakmp | ipsec-manual]
```

Parameter	Description
map-name	Identifies the crypto map set.
seq-num	Sequence number you assign to the crypto map entry. Use the crypto map map-name seq-num command without any keyword to modify the existing crypto map entry or profile
ipsec-isakmp	Indicates that IKE will be used to establish the IPsec for protecting the traffic specified by this crypto map entry.
ipsec-manual	Indicates that IKE will not be used to establish the IPsec SAs for protecting the traffic specified by this crypto map entry

XYZCORP Crypto Map Configuration

Crypto Map Configuration:


```
R1(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# set transform-set R1-R2
R1(config-crypto-map)# set peer 172.30.2.2
R1(config-crypto-map)# set pfs group24
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
R1(config)#
```

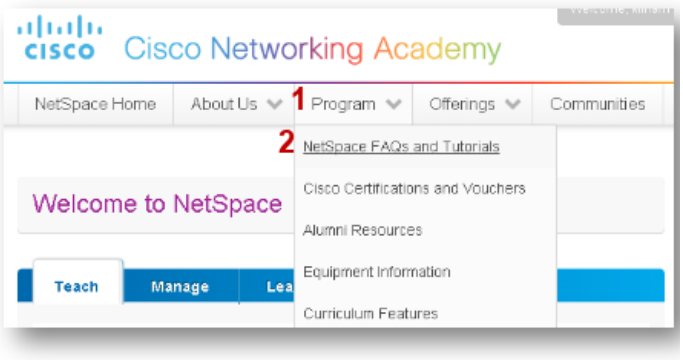

```
R2(config)# crypto map R1-R2_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R2(config-crypto-map)# match address 102
R2(config-crypto-map)# set transform-set R1-R2
R2(config-crypto-map)# set peer 172.30.2.1
R2(config-crypto-map)# set pfs group24
R2(config-crypto-map)# set security-association lifetime seconds 900
R2(config-crypto-map)# exit
R2(config)#
```

Apply the Crypto Map


```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map R1-R2_MAP
R1(config-if)#
*Mar 19 19:36:36.273: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)# end
R1# show crypto map
Interfaces using crypto map NiStTeSt1:

Crypto Map IPv4 "R1-R2_MAP" 10 ipsec-isakmp
Peer = 172.30.2.2
Extended IP access list 101
    access-list 101 permit ip 10.0.1.0 0.0.0.255 192.168.1.0 0.0.0.255
Current peer: 172.30.2.2
Security association lifetime: 4608000 kilobytes/900 seconds
Responder-Only (Y/N): N
PFS (Y/N): Y
DH group:  group24
Mixed-mode : Disabled
Transform sets={
R1-R2:  { esp-aes esp-sha-hmac  } ,
}
Interfaces using crypto map R1-R2_MAP:
Serial0/0/0
```

- **Remember**, there are helpful tutorials and user guides available via your NetSpace home page. (https://www.netacad.com)
- These resources cover a variety of topics including navigation, assessments, and assignments.
- A screenshot has been provided here highlighting the tutorials related to activating exams, managing assessments, and creating quizzes.



ინფორმაციული უსაფრთხოების პრობლემები და დაცვის კრიპტოგრაფიული ტექნოლოგიები

ეს არის ყველაზე ეფექტური საშუალება სნიფინგის საწინააღმდეგოდ საბრძოლველად, თუმცა ის ვერ უზრუნველყოფს ტრაფიკის დაჭერის აღკვეთას და ვერ ცნობს სნიფერის მუშაობას, თუმცა მისთვის ამ მუშაობის შესრულება გამოუსადეგარია. თუ არხი კრიპტოგრაფიულად დაცულია მაშინ ჰაკერი იჭერს არა შეტყობინებას არამედ დაშიფრულ ტექსტს (ე.ი ბიტების გაუგებარ თანმიმდევრობას). Cisco კრიპტოგრაფია იყენებს ქსელურ დონეზე IPSec პროტოკოლს, რომელიც წარმოადგენს სტანდარტულ მეთოდს, ქსელურ მოწყობიილობებს შორის დაცული კავშირის შესაქმნელად. სხვა კრიპტოგრაფიული პროტო- კოლები, რომელსაც იყენებენ ქსელური მართვისათვის არის SSh (Secure Shell) და SSL (Secure Socket Layer)

კოდირების სისტემები

ინფორმაციის კრიპტოგრაფიული დაცვის მეთოდები საინფორმაციო უსაფრთხოების საფუძველს წარმოადგენს. კრიპტოგრაფიული მეთოდები დაფუძნებულია ინფორმაციის კრიპტოგრაფიულ გარდაქმნებზე, რომლებიც ცვლიან საწყის ინფორმაციას ისე, რომ გამორიცხული იქნეს ამ ინფორმაციის არა- სანქცირებული წაკითხვა და მოდიფიკაცია.

არსებობს ინფორნმაციის შემდეგი სახის კრიპტოგრაფიული გარდაქმნები:

1. დაშიფრვა - ღია გზავნილების კრიპტოგრაფიული გარდაქმნა დახურულ გზავნილებად.

2. გაშიფრვა - დახურული გზავნილების კრიპტოგრაფიული გარდაქმნა ღია გზავნილებად.

3. კრიპტოანალიზი - დახურული გზავნილიდან ღია გზავნილის მიღება იმ დროს, როცა უცნობია კრიპტოგრაფიული გარდაქმნა.

ღია გზავნილი შეიძლება იყოს ბიტების ნაკადის, ქსელური ფრეიმის, ფაილის ან სხვა სახით წარმოდგენილი.

ჩვეულებრივ daშიფრვის და გაშიფრვის პროცესი წარმოებს სპეციალური გასაღებების და კრიპტოგრაფიული ალგორითმების გამოყენებით.

კრიპტოგრაფიული გარდაქმნების დროს გამოიყენება **შეცვლის** და **გადასმის** მეთოდები. ჩვეულებრივ კრიპტოგრაფიულ ალგორითმებში ორივე გარდაქმნაა კომბინირებული.

შეცვლის გარდაქმნა გულისხმობს ერთი სიმბოლოს (ბიტური კომბინაციის) შეცვლას სხვა სიმბოლოთი (ბიტური კომბინაციით). მაგ., თუ ღია გზავნილია $A_1A_2A_3A_4...A_N$, დახურული გზავნილი შეიძლება იყოს $B_1B_2B_3B_4...B_N$, ხოლო გადასმის Sემთხვევაში ვთქვათ $A_3A_NA_4A_1... A_2$.

შიფრვის ალგორითმები შემდეგნაირად კლასიფიცირდება: 1. სიმეტრიული ა. ბლოკური ბ. ნაკადური.

2. ასიმეტრიული

სიმეტრიული ალგორითმები ხასიათდება შიფრვის და გაშიფრვის ერთი გასაღებით, რომელიც საიდუმლოდ ინახება და გადაიცემა ჩვეულებრივ უსაფრთხო კავშირის გამოყენებით. ბლოკური შიფრვის ალგორითმები გარდაქმნებს გზავნილის თითოეულ ბლოკზე ცალცალკე ახდენენ. ეს ალგორითმები ძირითადად ცალკე აღებული მთლიანი გზავნილის, რომელიც წარმოდგენილია მაგალითად ფაილის სახით, შიფრვის დროს გამოიყენება. ნაკადური ალგორითმები გზავნილის თითოეულ სიმბოლოს ცალკე შიფრავენ, მათი

შიფრატორზე მოსვლისთანავე. ასეთი ალგორითმები გამოიყენება მაგალითად გასაიდუმლოებული სატელეფონო კავშირის დროს.

ასიმეტრიული ალგორითმები ხასიათდება ორი, ღია და დახურული გასაღებით. პირველი მათგანი გამოიყენება შიფრვის, ხოლო მეორე გაშიფრვის დროს. ეს ალგორითმები იძლევა საშუალებას გადავცეთ ღია გასაღებები კავშირის ღია არხებით. შვეულებრივ გასაღებების გენერაციას ახდენს მიმღები მხარე და უგზავნის ღია გასაღებს გადამცემ მხარეს. ხოლო დახურულგასაღებს ინახავს საიდუმლოდ.

სიმეტრიული შიფრვის ალგორითმები. არსებობს შემდეგი სახის სიმეტრიული შიფრვის ალგორითმები:

1. მარტივი შეცვლის ანუ ელექტრონული კოდური წიგნის ალგორითმი;

2.გამირების ალგორითმები.

მარტივი შეცვლის ანუ ელექტრონული კოდური წიგნის ალგორითმი. ამ მეთოდით შიფრვის დროს ხდება ღია გზავნილის თითო ბლოკის შეცვლა დახურული გზავნილის თითო ბლოკით. თეორიულად შესაძლებელია ე.წ. კოდური წიგნის ანუ ყველა ღია ბლოკის შესაბამისი დახურული ბლოკის ცხრილის შედგენა. თუ ბლოკის სიგრძეა 1 ბაიტი (8 ბიტი), მაშინ ასეთი წიგნის ზომა იქნება 2^8=256 ჩანაწერს.

დაშიფრვა შეიძლება აღვწეროთ ფორმულით:

$C_i=F(P_i)$, i=1N -თვის

სადაც C_i და P_i შესაბამისად დაშიფრული და გაშიფრული ტექსტის ბლოკებია, ხოლო F კრიპტოგრაფიული გარდაქმნა.

ეს მეთოდი ყველაზე ნაკლებად საიმედოა შიფრაციის სხვა მეთოდებს შორის.

მარტივი კრიპტოსისტემები. კრიპტოგრაფიული მეთოდები არის ყველაზე ეფექტური ინფორმაციის დაცვის საშუალება ავტომატიზირებულ სისტემებში. კომპიუტერულ ქსელებსში ინფორმაციის გადაცემის დროს ისინი არიან ერთადერთი არასანქცირებული შეღწევის აღკვეთის საშუალება.

შიფრაცია გადაადგილებით. გადაადგილების მეთოდით შიფრაციის დროს დასაშიფრი ტექსტის სიმბოლოები გადადგილდებიან გარკვეული წესების მიხედვით.

მარტივი გადაადგილების მეთოდი - ირჩევა შიფრაციის ბლოკი, რომელიც შედგება n სვეტებისგან და m სტრიქონებისგან და გასაღები რიცხვების თანმიმდევრობა, რომელიც ამოირჩევა ნატურალური რიცხვებიდან შემთხვევითი გადაადგილებით.

გამირების ალგორითმები. გამირების ალგორითმებში გამოიყენება სპეციალურად გენერირებული ბლოკების თანმიმდევრობა - გამა. გამის გენერაციისათვის ორივე მხარეს ჩვეულებრივ იყენებენ ერთ გასაღებს და გამის გენერაციის ერთ ალგორითმს.

დაშიფრვა შეიძლება აღვწეროთ შემდეგი ფორმულით:

$C_i = P_i \oplus F(Y_i), i=1..N$ -თვის

სადაც Y_i გამომუშავებული გამაა.

მაგალითისათვის შეგვიძლია მოვიყვანოთ შემდეგი სახის გარდაქმნა:

$C[i]=P[i] \oplus K[i \bmod len(K)]$

$P[i]=C[i] \oplus K[i \bmod len(K)]$

K[n] - კოდური სიტყვის n-ური სიმბოლოა C[i] -

დაშიფრული ტექსტის i-ური სიმბოლო P[i] - საწყისი

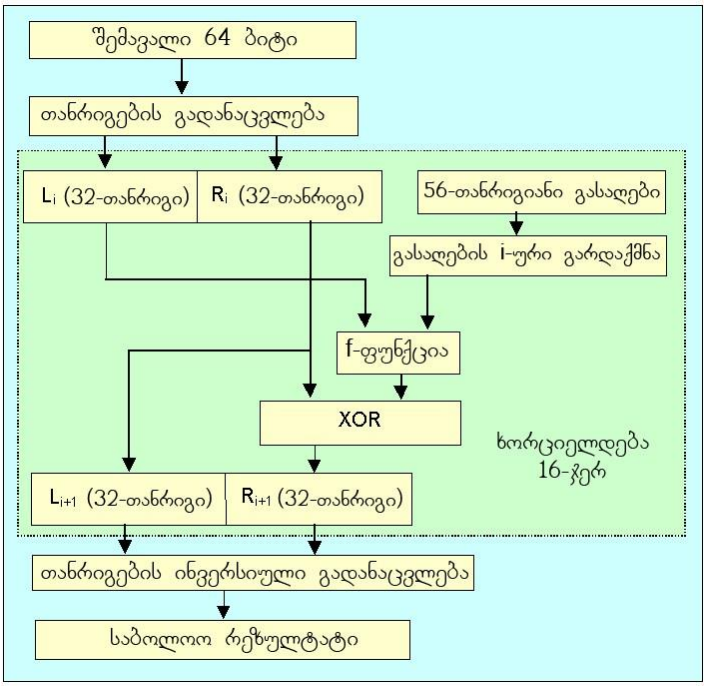
ტექსტის i-ური სიმბოლოა

len(K) - კოდური სიტყვის სიგრძეა

ალგორითმი DES. აშშ-ს სტანდარტების ეროვნული ბიუროს მიერ როგორც სახელმწიფო სტრუქტურებში ასევე კომერციულ ორგანიზაციებში რეკომენდირებული შიფრვის ალგორითმია Data Encryprion Standard (DES). ის შექმნილია 1977 წელს, თუმცა მისი მოდიფიკაცია გრძელდება და იქმნება მის საფუძველზე უფრო რთული და საიმედოალგორითმები.

DES ბლოკური შიფრირების ალგორითმია. მასში გამოყენებულია როგორც შეცვლის, ასევე გადასმის მეთოდები. ბლოკის სიგრძე 64 ბიტია, ხოლო გასაღების 56 ბიტი. პრაქტიკაში გასაღები 64 ბიტია, თუმცა აქედან 8 ბიტი საკონტროლო ჯამებია.

ალგორითმი შემდეგნაირად სრულდება:



თავიდან ხდება ბლოკის ბიტების არევა. ბიტები ლაგდება შემდეგი თანმიმდევრობით: (ციფრები მიუთითებს ბლოკის თანრიგის ნომერს)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

- შემდეგ 16-ჯერ მეორდება: ითვლება ბლოკის მარჯვენა ნახევარი

$R_{i+1} = R_i \oplus f(L_i, K_i)$

- ბლოკის მარცხენა ნახევარში იწერება მარჯვენა ნახევარი

$L_{i+1} = R_i$

- ბოლოს ხდება თანრიგების ინვერსიული გადანაცვლება შემდეგი თანმიმდევრობით:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

გასაღებების გენერაცია. ვირჩევთ ორ ძალიან დიდ მარტივ რიცხვს p-ს დაq-ს

1. $n=p*q$; $\varphi(n)=(p-1)*(q-1)$.
2. ვირჩევთ დიდ შემთხვევით რიცხვს d-ს ისეთს, რომ ის იყოს ურთიერთ მარტივი $\varphi(n)$-თან (ანუ არ ჰქონდეს არცერთი მთელი საერთო გამყოფი გარდა 1-ისა)
3. ვსაზღვრავთ ისეთ მთელ რიცხვს e-ს, რომლისთვისაც ჭეშმარიტია შემდეგი ტოლობა: $(e*d) \bmod \varphi(n)=1$ ღია გასაღებია (e,n), ხოლო დახურული (d,n).

საკუთრივ დაშიფრვა.

1. დასაშიფრი გზავნილი იყოფა ბლოკებად M_i ისე, რომ მისი ზომა k აკმაყოფილებდეს შემდეგ პირობას $10^{k-1}<n<10^k$
2. დაშიფრული გზავნილის შესაბამისი ბლოკის მნიშვნელობაა: $C_i=M_i^e \bmod n$

გზავნილის გაშიფრვისათვის ვიყენებთ დახურულ გასაღებს (d,n) და ვითვლით გაშიფრული გზავნილის ბლოკის მნიშვნელობას შემდეგი ფორმულით:

$M_i=C_i^e \bmod n$

ბლოკური შიფრი წარმოადგენს პოლიალფაბეტური შიფრის მოდიფიკაციას, რომლის პრინციპი არის შემდეგი: აიღება საწყისი ტექსტის გარკვეული სიგრძის ნაწილი (ბლოკი) და გასაღები, შედეგად მიიღება იგივე (იშვიათად განსხვავებული) სიგრძის შიფროტექსტი. შიფროტექსტის შემადგენელი ბლოკების ერთმანეთთან შერწყმისათვის გამოიყენება სხვადასხვა მეთოდები, რომლებსაც მთლიანობაში ქმედების რეჟიმი ეწოდებათ. მონაცემთა შიფრაციის სტანდარტი (Data Encryption Standard — DES) და გაუმჯობესებული შიფრაციის სტანდარტი (Advanced Encryption Standard — AES) წარმოადგენენ ბლოკურ შიფრებს. DES (და მისი ნაირსახეობა 3DES) ჯერ კიდევ რჩება ერთ-ერთ ყველაზე პოპულარულ ალგორითმად და ფართოდ გამოიყენება. თუმცა მისი გასაღების სიგრძის არასაკმარისობის გამო, ხდება მისი ჩანაცვლება სხვა, უფრო თანამედროვე ალგორითმებით.

ჰეშ-ფუნქციების როლი თანამედროვე კრიპტოგრაფიაში. კრიპტოგრაფიულად საიმედო ჰეშ-ფუნქციები, მათი გამოთვლის ალგორითმები

ჰეშ–ფუნქციები

ნაშთიანი გაყოფის მეთოდით

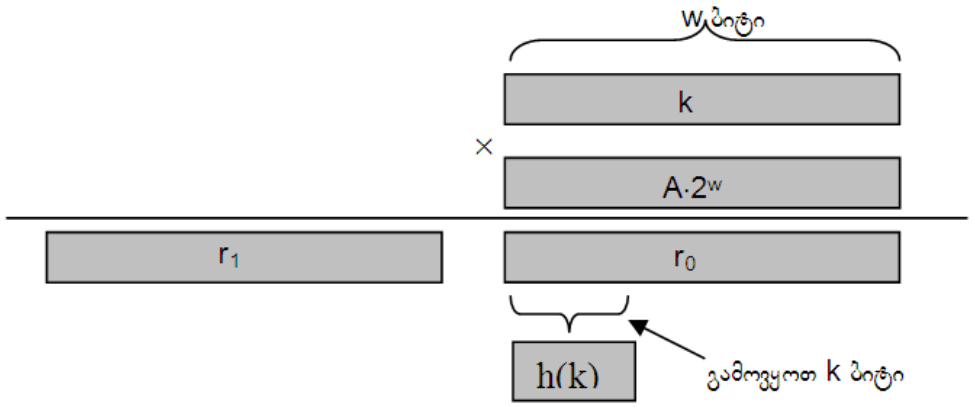
ჰეშ-ფუნქციის აგება **ნაშთიანი გაყოფის მეთოდით** (division method) მდგომარეობს იმაში, რომ k სიდიდის მქონე გასაღებს ეთანადება k-ს m-ზე გაყოფის ნაშთი, სადაც m წარმოადგენს შესაძლო ჰეშ-მნიშვნელობების რაოდენობას:

$h(k)= k \% m$

მაგალითად, თუკი ჰეშ-ცხრილის ზომა m=12-ის ტოლია და გასაღები უდრის 100-ს, მაშინ შესაბამისი ჰეშ-მნიშვნელობა იქნება 4.

კარგ შედეგებს იძლევა m-ის როლში ისეთი მარტივი რიცხვის აღება, რომელიც შორს დგას 2-ის ხარისხებისაგან. მაგალითად, თუ ჰეშ-ცხრილში შესატანია 2000-მდე ჩანაწერი და დაახლოებით სამი ვარიანტის გადარჩევა პრობლემას არ ჰქმნის ელემენტთა ძებნისას, m-ის მნიშვნელობად შეგვიძლია ავიღოთ 701. რიცხვი 701 მარტივია, 701≈2000/3 და ორის ხარისხებისგანაც შორს დგას. ყოველოვე ამის გამო მიზანშეწონილია ავირჩიოთ ჰეშ-ფუნქცია h(k)=k mod 701.

გამრავლების მეთოდი



გამრავლების მეთოდი მუშაობს A მუდმივის ნებისმიერი მნიშვნელობისათვის, მაგრამ ზოგიერთმა მნიშვნელობამ შეიძლება უკეთესი შედეგი მოგვცეს. დონალდ კნუტის აზრით

$$A \approx \left(\sqrt{5}-1\right)/2 = 0.6180339887$$

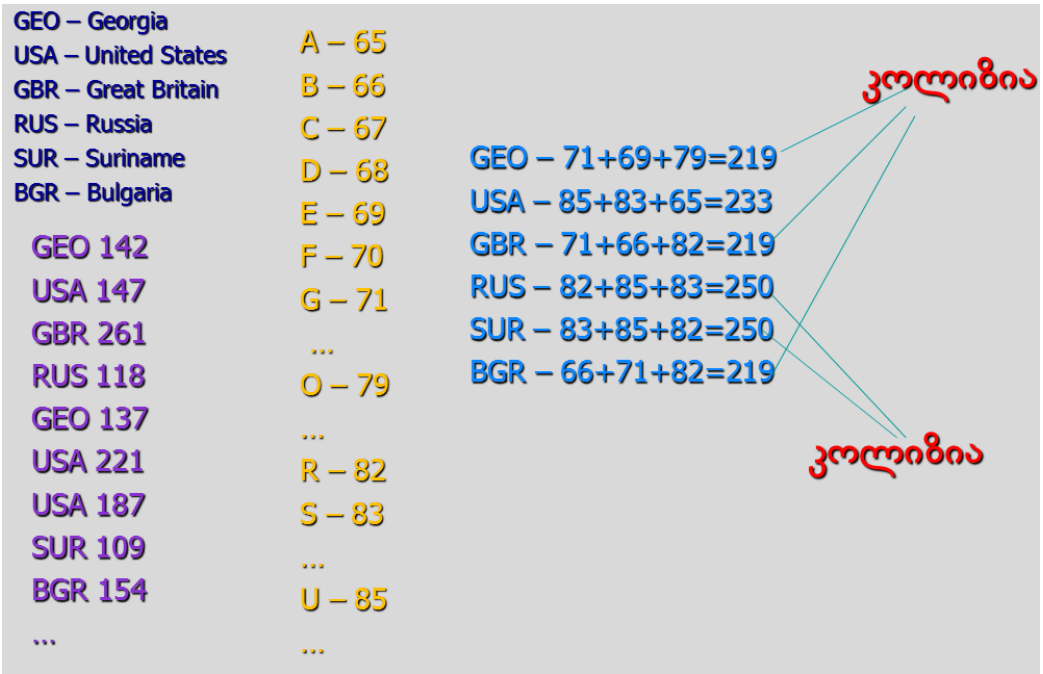
მნიშვნელობა საკმაოდ ეფექტურია.

მოვიყვანოთ მაგალითი: ვთქვათ, k=123456, m=10000 და A განსაზღვრულია ფორმულით, მაშინ
h(k) = ⌊10000·(123456·0.61803… mod 1⌋ = ⌊10000·(76300.0041151… mod 1⌋ =
= ⌊10000·0.0041151…⌋=⌊41.151…⌋=41.

უნივერსალური ჰეშირება

თუკი ჰეშ-ფუნქცია ცნობილია, მაშინ, რა თქმა უნდა, ყოველთვის შესაძლებელია ისეთი მონაცემების შერჩევა, რომ ყველა n გასაღები შეესაბამებოდეს ჰეშ-ცხრილის ერთ პოზიციას, რის გამოც ძებნის დრო გახდება Θ(n)-ის ტოლი. ასეთი გზით ნებისმიერი ფიქსირებული ჰეშ-ფუნქციის დისკრედიტირება შეიძლება. ერთადერთი გამოსავალი ამ სიტუაციიდან არის ის, რომ ჰეშ-ფუნქცია შევარჩიოთ შემთხვევითად, იმის მიუხედავად თუ რა სახის მონაცემებზეა ჰეშირება ჩასატარებელი. ასეთ მეთოდს უწოდებენ **უნივერსალურ ჰეშირებას** (universal lashing). უნივერსალური ჰეშირების ძირითადი იდეაა, შევარჩიოთ ჰეშ-ფუნქცია შემთხვევითად რაღაც სიმრავლიდან პროგრამის შესრულების დროს. ცხადია, რომ პროგრამის იმავე მონაცემებით ხელმეორედ გაშვებისას ჰეშირება სხვაგვარად მოხდება. შემთხვევითი ფუნქციის გამოყენება გარანტიას იძლევა, რომ შეუძლებელია ისეთი საწყისი მონაცემების მოფიქრება, რომ ალგორითმმა ყოველთვის ნელა იმუშაოს.

მაგალითი



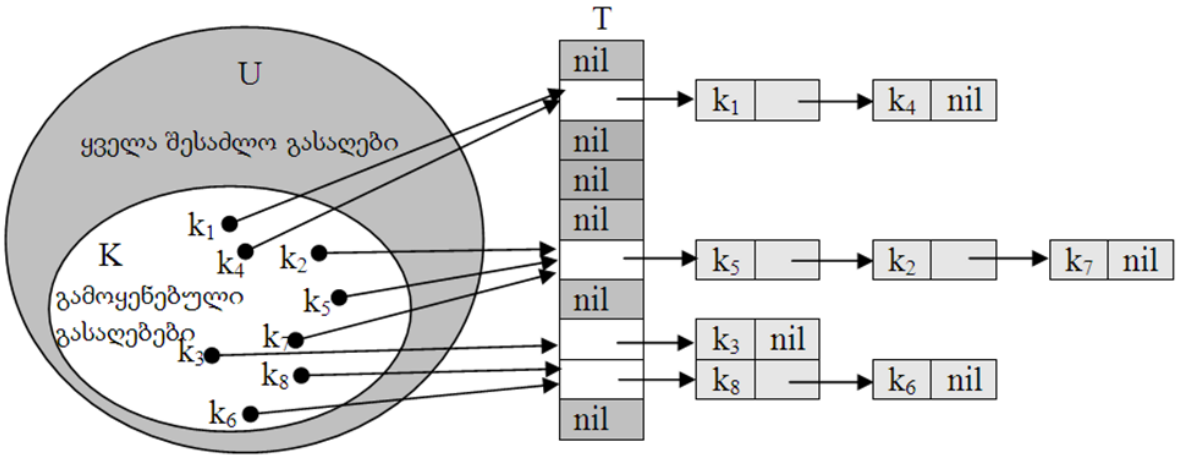
კოლიზია

GEO – $71+69*26+79*26^2 = 55269$
USA – $85+83*26+65*26^2 = 46186$
GBR – $71+66*26+82*26^2 = 57219$
RUS – $82+85*26+83*26^2 = 58400$
SUR – $83+85*26+82*26^2 = 57725$
BGR – $66+71*26+82*26^2 = 57344$

GEO – $6+4*26+14*26^2 = 9574$
USA – $20+18*26+0*26^2 = 488$
GBR – $6+1*26+17*26^2 = 11524$
RUS – $17+20*26+18*26^2 = 12705$
SUR – $18+20*26+17*26^2 = 12030$
BGR – $1+6*26+17*26^2 = 11649$

ელემენტთა გადაბმა

კოლიზიის პრობლემის გადაჭრის ერთ-ერთი გზაა **ელემენტთა გადაბმა** (chaining). ამ მეთოდს ასევე ეწოდება **ჰეშირება ჯაჭვებით**. მისი არსი იმაში მდგომარეობს, ერთნაირი ჰეშ-მნიშვნელობის მქონე ელემენტებისაგან ყალიბდება ბმული სია



მუშაობის დრო

ვთქვათ T არის m პოზიციის მქონე ჰეშ-ცხრილი, რომელშიც შეტანილია n ელემენტი. ცხრილის **შევსების კოეფიციენტი** (load factor) ეწოდება $\alpha=n/m$ რიცხვს (ეს რიცხვი შეიძლება იყოს 1-ზე მეტიც და 1-ზე ნაკლებიც). გამოვსახოთ ოპერაციათა ღირებულება α-ს საშუალებით.

უარეს შემთხვევაში ყველა n გასაღების ჰეშ-მნიშვნელობა შეიძლება ერთმანეთს დაემთხვეს, მაშინ ცხრილი წარმოდგენილი იქნება n სიგრძის მქონე ერთი სიით და ელემენტის ძებნაზე დაიხარჯება იგივე $\Theta(n)$ დრო, რაც დაიხარჯებოდა სიაში ძებნისას. ამას დაემატება კიდევ ჰეშ-ფუნქციის გამოთვლის დრო. ცხადია, რომ ასეთ შემთხვევაში ჰეშირებას აზრი არა აქვს.

ძებნის საშუალო ღირებულება დამოკიდებულია იმაზე, თუ რამდენად თანაბრად გაანაწილებს ჰეშ-ფუნქცია ჰეშ-მნიშვნელობებს ცხრილის პოზიციებში. დავუშვათ, რომ თითოეულ ელემენტს თანაბარი ალბათობით შეუძლია მოხვდეს ცხრილის ნებისმიერ m პოზიციაში და არაა დამოკიდებული იმაზე, თუ რა პოზიციაში მოხვდა სხვა ელემენტი. ამ დაშვებას ვუწოდოთ **თანაბარი ჰეშირების** (simple uniform hashing) ჰიპოთეზა.

თეორემა . ვთქვათ T ჯაჭვების შემცველი ჰეშ-ცხრილია, რომლის შევსების კოეფიციენტია α. დავუშვათ, რომ ჰეშირება თანაბარია. მაშინ ცხრილში არარსებული ელემენტის ძებნისას საშუალოდ განხილული იქნება ცხრილის α ელემენტი, ხოლო ასეთი ძებნის საშუალო დრო (ჰეშ-ფუნქციის გამოთვლის დროის ჩათვლით) იქნება $\Theta(1+\alpha)$.

თეორემა . თანაბარი ჰეშირებისას ჯაჭვების შემცველ ჰეშ-ცხრილში, წარმატებული ძებნის საშუალო დროა $\Theta(1+\alpha)$, სადაც α შევსების კოეფიციენტია.

ასიმეტრიული კრიპტოსისტემები და მათი მათემატიკური ალგორითმები

1976 წელი ისტორიული თარიღია, რომელიც აღნიშნავს ახალ ერას კრიპტოგრაფიაში. უ.დიფის და მ.ჰელმანის ნაშრომით დასაბამი დაედო ასიმეტრიული სისტემების განვითარებას, როდესაც კრიპტოგრაფიული სისტემა არ საჭიროებს საიდუმლო კურიერს; როდესაც გასაღების ფორმირება-გადაცემა და ინფორმაციის დაშიფვრა ხდება ღია არხის მეშვეობით, მაგრამ საჭირო საიდუმლოების დაცვით.

ასიმეტრიული კრიპტოგრაფიის გამოყენების ორი ძირითადი სფეროა:

1. ღია გასაღებით შიფრაცია — ღია გასაღებით დაშიფრული ტექსტის დეშიფრაცია შეუძლია მხოლოდ მას, ვისაც აქვს პირადი გასაღები. ანუ ნებისმიერს შეუძლია გაუგზავნოს გასაღების მფლობელს საიდუმლო ინფორმაცია. თუ ქსელში არსებობს N პირი, მათ შორის ინფრომაციის გასაცვლელად საჭირო ხდება მხოლოდ N-1 გასაღებების წყვილი. ღია გასაღებები თავისუფლად იცვლება ერთმანეთში ან მოთავსდება საერთო ბაზაში.

2. ციფრული ხელმოწერა — ფარული გასაღებით დაშიფრული ტექსტის დეშიფრაცია შეუძლია ნებისმიერს, ანუ ყველას შეუძლია მიმართოს საერთო ბაზას და დარწმუნდეს იმაში, რომ ეს ინფორმაცია ნამდვილად გამგზავნის მიერ იქნა დაშიფრული (ხელმოწერილი).

დიფი-ჰელმანის მეთოდი: X და Y ორი სუბიექტი (Z სუბიექტის არსებობის პირობებში) ღია არხით კურიერის გარეშე ამყარებს შემდეგ ინფორმაციულ კავშირს.

ამყარებს შემდეგ ინფორმაციულ კავშირს. დავუშვათ, რომ p მარტივი და a ნატურალური რიცხვები გაცხადებულია, ანუ ღიაა (p მაღალი რიგის, $\approx 2^{500}$ სიდიდის მარტივი რიცხვია; $1 < a < p$). ინფორმაციის გაცვლას X და Y მხარეებს შორის აქვს შემდეგი სახე:

X მხარე საიდუმლო (კერძო) გასაღებად შეირჩევს x ნატურალურ რიცხვს ($1 < x < p$); გამოთვლის

$$a^x \equiv c_1 \bmod p$$

რიცხვს და ღია არხით გადააგზავნის Y მხარეზე.

Y მხარე საიდუმლო (კერძო) გასაღების სახით შეირჩევს y ნატურალურ რიცხვს ($1 < y < p$); გამოთვლის

$$c_1^{\ y} \equiv a^{xy} \equiv k_1 \bmod p$$

რიცხვს. k_1 რიცხვს Y მხარე მიიჩნევს საერთო გასაღებად.

Y მხარე გამოთვლის

$$a^y \equiv c_2 \bmod p$$

რიცხვს და ღია არხით გადააგზავნის X მხარეზე.

X მხარე გამოთვლის

$$c_2^{\ x} \equiv a^{yx} \equiv k_2 \bmod p$$

რიცხვს. k_2 რიცხვს X მხარე მიიჩნევს საერთო გასაღებად.

რადგან $k_1 \equiv k_2 \equiv k$, მაშასადამე ორივე მხარე შეირჩევს ერთსა და იმავე გასაღებს.

დიფი-ჰელმანის მეთოდში გამოყენებულია გალუას $GF(p)$ სასრულ ველებზე ლოგარითმის გამოთვლის ცნობილი სირთულე. ვთქვათ,

$$c \equiv a^x \bmod p,\ 1 \le x \le p,$$

სადაც $a \in GF(p)$ ველის პრიმიტიული ელემენტია (ე.ი. ელემენტის ხარისხები წარმოადგენს $GF(p)$ ველის ელემენტებს; ამბობენ, რომ x არის c ელემენტის ლოგარითმი $GF(p)$ ველზე):

$$x = \log_a c \quad GF(p) \text{ ველზე}, 1 \le c \le p.$$

c ელემენტის გამოთვლა x ელემენტის მიხედვით არ წარმოადგენს სირთულეს და საჭიროებს მაქსიმუმ $2\log_2 p$ გამრავლების ოპერაციას. მაგალითად, $a^{34} = ((((a^2)^2)^2)^2)^2 \cdot a^2$.

მაგრამ, პირიქით, x ელემენტის გამოთვლა c ელემენტის მიხედვით გაცილებით რთულია და მოითხოვს დაახლოებით $p^{1/2}$ ოპერაციას.

თუ p მარტივი რიცხვია და p შედარებით ნაკლებია 2^n რიცხვზე (სადაც n ინფორმაციული ორობითი სიტყვის სიგრძეა, ანუ შეტყობინების ვექტორის განზომილებაა), მაშინ ახარისხებას დასჭირდება არა უმეტეს $2n$ ოპერაცია $GF(p)$ ველზე, ხოლო გალოგარითმებას უკეთეს შემთხვევაში- $2^{n/2}$ ოპერაცია.

როდესაც X მხარე Y მხარეს ღია არხით გადასცემს c_1 შეტყობინებას, მაშინ ანალიტიკოსს (ან ჰაკერს) x საიდუმლო გასაღების გამოსათვლელად დასჭირდება $2^{n/2}$ ოპერაციის შესრულება, რასაც ის ვერ შეძლებს (მაგალითად, თუ $n = 200$, მაშინ საჭიროა 2^{100}, ანუ დაახლოებით 10^{30} ოპერაცია, რისი განხორციელებაც პრაქტიკულად შეუძლებელია).

დიფი-ჰელმანის ალგორითმი გამოიყენება როგორც გასაღებების გაცვლის, დაშიფვრის, აგრეთვე, აუტენტიფიკაციის მიზნით კრიპტოგრაფიული პროტოკოლების ამოცანებში და სხვ.

მაგალითი. დავუშვათ, რომ $p = 11$, $a = 2$, $x = 2$, $y = 4$, მაშინ

$$c_1 = 2^2 \equiv 4 (\mathrm{mod} 11),$$
$$c_2 = 2^4 \equiv 5 (\mathrm{mod} 11),$$
$$K_1 = 4^4 \equiv 5 \cdot 5 \equiv 3 (\mathrm{mod} 11),$$
$$K_2 = 5^2 \equiv 3 (\mathrm{mod} 11),$$

ე.ი. $K = 3$.

გასაღების ფორმირების შემდეგ შეიძლება განხორციელდეს დაშიფვრის ოპერაცია.

ვთქვათ, $n = 4$, ხოლო ორობითი ინფორმაციაა $m = (0111)$, ანუ $M = 7$. X მხარე გამოიყენებს $K = 3$ გასაღებს, რაც, ცხადია, ცნობილია Y მხარესათვისაც. დავუშვათ, რომ X მხარე დაშიფრავს ინფორმაციას, ხოლო Y მხარე გაშიფრავს მას. ამისათვის Y მხარე წინასწარ გამოთვლის K' გასაღებს იმ პირობით, რომ (ფერმას მცირე თეორემა)

$$KK' \equiv 1(\mathrm{mod}(p-1))$$

ე.ი.

$$3 \cdot x \equiv 1(\mathrm{mod}10).$$

X მხარე დაშიფრავს $m = (0111)$ ღია ტექსტს თავისი $K = 3$ გასაღებით:

$$C = M^K = 7^3 \equiv 2\ (\mathrm{mod}11);$$

მიღებულ C შიფროტექტს გადაუგზავნის Y მხარეს, რომელიც თავისი $K' = 7$ გასაღებით გაშიფრავს მას:

$$M = C^{K'} \equiv 2^7 \equiv 7\ (\mathrm{mod}11).$$

1.2.3. რივესტ-შამირ-ეიდლმენის კრიპტოსისტემა (RSA)

1977 წელს რ. რივესტმა, ა. შამირმა და ლ. ეიდლმენმა დაამუშავეს შიფრაციისა და ნამდვილობის (აუტენტიფიკაციის) ახალი მეთოდი. RSA დაპატენტებულია შეერთებულ შტატებში, ლიცენზირებულია სხვა ქვეყნებში და წარმოადგენს ფაქტიურ სტანდარტს მსოფლიოს მრავალ ქვეყანაში [1, 2, 3, 14, 38, 41].

კრიპტოგრაფიული მეთოდი შემდეგში მდგომარეობს.

დავუშვათ, რომ X სუბიექტი საიდუმლოდ ირჩევს ძალიან დიდ მარტივ p და q რიცხვებს, გამოთვლის $N = pq$ ნამრავლს და N რიცხვს

აცხადებს (N რიცხვი ღიაა), მაგრამ p და q რიცხვებს ინახავს საიდუმლოდ (p და q დასაიდუმლოებულია); გამოითვლება ეილერის ფუნქცია:

$$\varphi(N) = (p-1)(q-1)$$

და $\varphi(N)$ რიცხვს დაასაიდუმლოებს.

შემდეგ 2-დან $(\varphi(N)-1)$-დე ინტერვალში შეირჩევს e რიცხვს (როგორც შემთხვევით რიცხვს; თუ $(e,\varphi(N)) \neq 1$, მაშინ შეირჩევს e რიცხვის სხვა მნიშვნელობას), რომელსაც აცხადებს (e რიცხვი ღიაა); $ed \equiv 1 \bmod \varphi(N)$ შედარებიდან გამოთვლის d რიცხვს და მას საიდუმლოდ ინახავს (d გასაღები დასაიდუმლოებულია). შეიძლება მივიღოთ d რიცხვი როგორც

$$ed \equiv 1 \bmod k\varphi(N), \qquad (1.1)$$

შედარებიდან, აგრეთვე

$$ed = k\varphi(N) + 1$$

შესაბამისომიდანაც.

ამის შემდეგ Y სუბიექტს შეუძლია M შეტყობინება გადაუგზავნოს X სუბიექტს დაშიფრული სახით:

$$M^e \equiv c \bmod N.$$

c შიფროტექსტს გაშიფრავს მხოლოდ X სუბიექტი, რადგან d გასაღებს Z მხარე ვერ გამოთვლის:

$$c^d \equiv M \bmod N.$$

Z მხარე d რიცხვის მნიშვნელობას ვერ გამოთვლის, რადგან ამისათვის მან უნდა გადაწყვიტოს ერთ-ერთი ამოცანა: ან გამოთვალოს $\varphi(N)$ ფუნქციის მნიშვნელობა ან იპოვოს N რიცხვის ერთ-ერთი მარტივი მამრავლი (ფაქტორიზაციის ამოცანა), რაც დროის რეალურ მასშტაბში თანამედროვე კომპიუტერული სიმძლავრეებით შეუძლებელია.

მაგალითი. დავუშვათ, რომ $p = 3$, $q = 5$, $M = 3$, მაშინ

$$N = pq = 15;\ \ \varphi(N) = (p-1)(q-1) = 8.$$

(1.1) თანაფარდობიდან

$$ed = \varphi(N) + 1 = 9\ ,$$

ანუ

$$e = 3,\ \ d = 3.$$

Y მხარე გაშიფრავს მას:

$$M = C^d \equiv 12^3 \equiv 3\ (\mathrm{mod}15)\,.$$

1.2.4. ელგამალის კრიპტოსისტემა

მოცემული სისტემა წარმოადგენს RSA-ს ალტერნატივას და მისგან განსხვავებით ეყრდნობა დისკრეტული ლოგარითმის პრობლემას. ამით იგი წააგავს დიფფი-ჰელმანის ალგორითმს. თუ რიცხვის აყვანა ხარისხში სასრულ ველში საკმაოდ მარტივია, პირიქით, არგუმენტის აღდგენა (ე.ი. ლოგარითმის აღება) საკმაოდ რთულია.

ელგამალის სისტემის საფუძველს წარმოადგენენ p და $g < p$ რიცხვები, სადაც პირველი მარტივია, ხოლო მეორე- მთელი.

X აგენერირებს საიდუმლო x გასაღებს და გამოთვლის ღია გასაღებს $y = g^x \bmod p$. თუ Y მხარეს სურს გაუგზავნოს X მხარეს m ტექსტი, ის ირჩევს შემთხვევით k რიცხვს ($k < p$) და გამოთვლის

$$y_1 = g^k \bmod p$$

და

$$y_2 = m \oplus y^k,$$

სადაც $\oplus$ არის ბიტური შეკრება მოდულით 2. ამის შემდეგ Y მხარე X მხარეს უგზავნის (y_1, y_2)-ს.

X მხარე მიღებულ დაშიფრულ შეტყობინებას აღადგენს:

$$m = (y_1^x \bmod p) \oplus y_2.$$

1.2.5. ელიფსური ფუნქციების გამოყენება კრიპტოგრაფიაში

ელიფსური წირები (ფუნქციები)- მათემატიკური ობიექტია, რომელიც შეიძლება განსაზღვრულ იქნეს ნებისმიერ ველზე (სასრულ, ნამდვილ, რაციონალურ და კომპლესურ ველზე). კრიპტოგრაფიაში ძირითადად გამოიყენება სასრული ველები. ელიფსური წირი არის (x, y) წერტილთა სიმრავლე, რომელიც აკმაყოფილებს შემდეგ განტოლებას [56]:

$$y^2 = x^3 + ax + b,$$

და ამასთან უსასრულოდ დაშორებული წერტილი. საკმაოდ ადვილია წირზე წერტილების შეკრება, რომელიც იგივე როლს თამაშობს რაც გამრავლების ოპერაცია RSA-სა და ელგამალის კრიპტოსისტემებში.

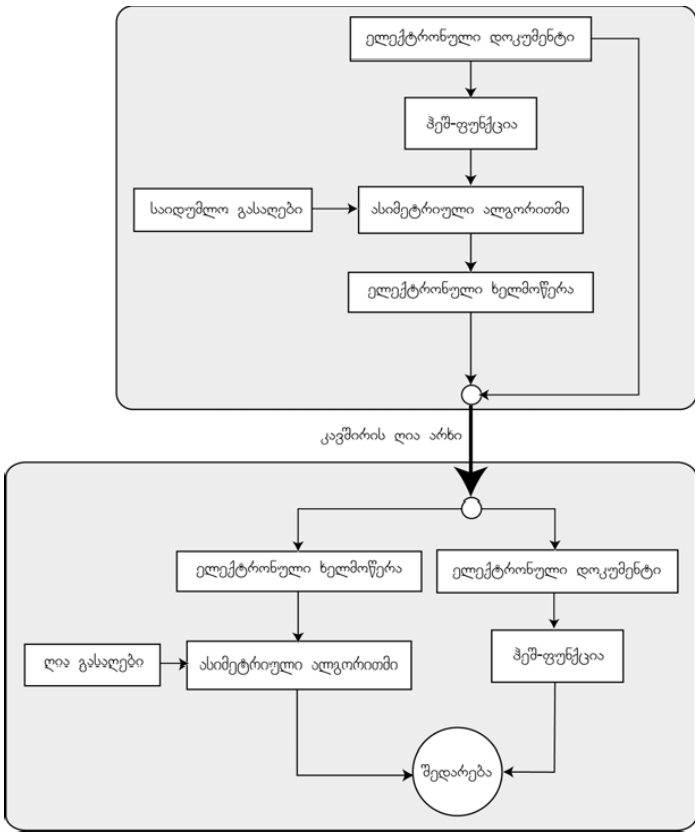
რეალურ კრიპტოსისტემებში ელიფსური ფუნქციების დროს გამოიყენება შემდეგი განტოლება:

$$y^2 = x^3 + ax + b \bmod p,$$

სადაც p მარტივი რიცხვია.

ციფრული ხელმოწერის სტანდარტი

ელექტრონული ხელმოწერა. ელექტრონული დოკუმენტების სარწმუნოების დასაბუთების საშუალებას ელექტრონული ხელმოწერა წარმოადგენს. ელექტრონული ხელმოწერის რეალიზაცია ხორციელდება შიფრვის ასიმეტრიული ალგორითმით, ოღონდ ამ შემთხვევაში ღიაა ის გასაღები, რომლითაც ხდება გაშიფრვა, ხოლო დახურულია დაშიფრვის გასაღები. იმისათვის, რომ ხელმოწერა მიბმული იყოს დოკუმენტზე, გამოიყენება დოკუმენტის ჰეშ-კოდი. ელექტრონული დოკუმენტიდა ჰეშ-ფუნქციის გამოყენებით გენერირდება ჰეშ-კოდი, რომელიც საიდუმლო გასაღების გამოყენებით შიფრვის ასიმეტრიული ალგორითმით იშიფრება და მიიღება ელექტრონული ხელმოწერა, რომელიც ებმება დოკუმენტს და იგზავნება ღია არხით ადრესატთან. ელექტრონული ხელმოწერა შემდეგი სქემით ხორციელდება:



ადრესატი გამოყოფს ელექტრონულ ხელმოწერას, ახდენს მის გაშიფრვას ღია გასაღების გამოყენებით და ადარებს დოკუმენტის ჰეშ კოდს. თუ ისინი არ დაემთხვა, ე.ი. დოკუმენტი ან გაყალბებულია, ან შეცდომებით გადმოიცა კავშირის არხის საშუალებით.

განვიხილოთ ელექტრონული ხელმოწერის სტანდარტი DSA.

ელექტრონული ხელმოწერის სტანდარტი DSA

გასაღებების გენერაცია.

1. ვირჩევთ მარტივ რიცხვს q-ს, ისეთს, რომ $2^{159}<q<2^{160}$

2. ვირჩევთ t-ს ისეთს, რომ $0 \square t \square 8$, და ვირჩევთ მარტივ რიცხვს

p-ს, ისეთს, რომ $2^{511+64t}<p<2^{512+64t}$, თან q უნდა ყოფდეს (p-1)-ს

3. ვითვლით $g=h^{p-1/q} \bmod p$, სადაც h ნებისმიერი მთელი რიცხვია ისე, რომ $0<h<p$ და რომელიც აკმაყოფილებს პირობას $h^{p-1/q} \bmod p>1$

საიდუმლო გასაღები x ირჩევა შუალედიდან [1,q], ხოლო ღია გასაღები $y=g^x \bmod p$.

ყველა მომხმარებლისათვის ქვეყნდება p, q, g და y.

ელექტრონული ხელმოწერის გენერირება ხდება შემდეგნაირად:

1. ვითვლით დოკუმენტის ჰეშ-კოდს h=H(m)

2. შუალედიდან [1, q] შემთხვევით ვირჩევთ k-ს და ვითვლით

$r=(g^k \bmod p) \bmod q$

3. ვითვლით $s=(k^{-1}(h+x*r)) \bmod q$, სადაც ელექტრონულ ხელმოწერას წარმოადგენს r და s.

მიღებული m დოკუმენტის და (r,s) ხელმოწერის შემოწმებისათვის:

1. ვამოწმებთ პირობას $0<r<q$ და $0<s<q$, და თუ ერთი მათგანი მაინც არ სრულდება ხელმოწერა ყალბია.

2. ვითვლით:

$w=s_1^{-1} \bmod q$; $u1=(H(m)*w) \bmod q$; $u2=((r/w) \bmod q$; $v=((g^{u1}y^{u2}) \bmod p) \bmod q$

3. მოწმდება ტოლობა v=r. თუ ტოლობა სრულდება ელექტრონული ხელმოწერა მისაღებია.

მოცემულ ალგორითმში რეკომენდირებულია p-ს სიგრძე არა ნაკლებ 768 ბიტი. მაქსიმალური საიმედოობისათვის სასურველია 1024 ბიტის გამოყენება.

ომარ აბშილავა - ინფორმაციული უსაფრთხოების მენეჯერი

ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონის მიმოხილვა

ვის და რაში სჭირდება ინფორმაციული უსაფრთხოება?

2008 წლის კიბერ-ომი რუსეთთან და მისი შედეგები. ამონარიდი საქართველოს ეროვნული უსაფრთხოების კონცეფციიდან:

საქართველოს ეროვნული ინტერესი N12. ***საქართველოსთვის მეტად მნიშვნელოვანია ინფორმაციული სივრცის უსაფრთხოება და ელექტრონული ინფორმაციის დაცულობა. ინფორმაციული ტექნოლოგიების სწრაფ განვითარებასთან ერთად იზრდება მათზე სახელმწიფოს კრიტიკული ინფრასტრუქტურის დამოკიდებულება. ამის გათვალისწინებით, დიდი მნიშვნელობა ენიჭება კიბერდანაშაულთან ბრძოლას და კიბერსივრცეში დივერსიული აქტებისგან თავდაცვას.***

კანონი ინფორმაციული უსაფრთხოების შესახებ

კრიტიკული ინფორმაციული სისტემის სუბიექტების შემდეგი ნუსხა:

1. საქართველოს იუსტიციის სამინისტრო;

2. საქართველოს სასჯელაღსრულებისა და პრობაციის სამინისტრო;

3. საქართველოს საგარეო საქმეთა სამინისტრო;

4. საქართველოს ფინანსთა სამინისტრო;

5. საქართველოს შინაგან საქმეთა სამინისტრო;

6. საქართველოს რეგიონული განვითარებისა და ინფრასტრუქტურის სამინისტრო;

7. საქართველოს შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო;

8. საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო;

9. საქართველოს პარლამენტი;

10. საქართველოს პრეზიდენტის ადმინისტრაცია;

11. საქართველოს მთავრობის კანცელარია;

12. საქართველოს ეროვნული ბანკი;

13. საქართველოს მთავარი პროკურატურა;

14. ქალაქ თბილისის მერია;

15. საქართველოს ცენტრალური საარჩევნო კომისიის აპარატი;

16. საჯარო სამართლის იურიდიული პირი – „სმართ ლოჯიქი“ (SMART LOGIC);

17. საჯარო სამართლის იურიდიული პირი – სახელმწიფო შესყიდვების სააგენტო;

18. საჯარო სამართლის იურიდიული პირი – სოციალური მომსახურების სააგენტო;

19. საჯარო სამართლის იურიდიული პირი – შეფასებისა და გამოცდების ეროვნული ცენტრი;

20. საჯარო სამართლის იურიდიული პირი – სახელმწიფო სერვისების განვითარების სააგენტო;

21. საჯარო სამართლის იურიდიული პირი – საფინანსო-ანალიტიკური სამსახური;

22. საჯარო სამართლის იურიდიული პირი – საჯარო რეესტრის ეროვნული სააგენტო;

23. საჯარო სამართლის იურიდიული პირი – შემოსავლების სამსახური;

24. საჯარო სამართლის იურიდიული პირი – საქართველოს ფინანსური მონიტორინგის სამსახური;

25. საჯარო სამართლის იურიდიული პირი – სამედიცინო საქმიანობის სახელმწიფო რეგულირების სააგენტო;

26. საჯარო სამართლის იურიდიული პირი – ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრი;

27. საჯარო სამართლის იურიდიული პირი – სამედიცინო მედიაციის სამსახური;

28. საჯარო სამართლის იურიდიული პირი – სამოქალაქო ავიაციის სააგენტო;

29. საჯარო სამართლის იურიდიული პირი – საზღვაო ტრანსპორტის სააგენტო;

30. საჯარო სამართლის იურიდიული პირი – სახმელეთო ტრანსპორტის სააგენტო;

31. საჯარო სამართლის იურიდიული პირი – განათლების მართვის საინფორმაციო სისტემა;

32. სააქციო საზოგადოება „საქართველოს რკინიგზა“;

33. შეზღუდული პასუხისმგებლობის საზოგადოება „საქაერონავიგაცია“;

34. შეზღუდული პასუხისმგებლობის საზოგადოება „საქართველოს აეროპორტების გაერთიანება“;

35. საჯარო სამართლის იურიდიული პირი – განათლების ხარისხის განვითარების ეროვნული ცენტრი;

36. საქართველოს შინაგან საქმეთა სამინისტროს სახელმწიფო საქვეუწყებო დაწესებულება - საქართველოს სასაზღვრო პოლიცია;

37. საჯარო სამართლის იურიდიული პირი – საქართველოს შინაგან საქმეთა სამინისტროს მომსახურების სააგენტო;

38. საქართველოს შინაგან საქმეთა სამინისტროს საჯარო სამართლის იურიდიული პირი - „112“;

39. საჯარო სამართლის იურიდიული პირი - გარემოს ეროვნული სააგენტო.

მუხლი 7. ინფორმაციული უსაფრთხოების მენეჯერი

1. კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციის სისტემის სუბიექტის ინფორმაციული უსაფრთხოების მოთხოვნების შესრულებისათვის (ინფორმაციული უსაფრთხოების მენეჯერი).

2. ინფორმაციული უსაფრთხოების მენეჯერის ძირითადი მოვალეობებია:

ა) ინფორმაციული უსაფრთხოების პოლიტიკის მოთხოვნების შესრულების ყოველდღიური მონიტორინგი;

ბ) ინფორმაციული აქტივებისა და მათი წვდომის აღწერა;

გ) ინფორმაციული უსაფრთხოების პოლიტიკის შინაუწყებრივი დოკუმენტაციის მომზადება;

დ) ინფორმაციული უსაფრთხოების ინციდენტების შესახებ ინფორმაციის შეგროვება და მათზე რეაგირების მონიტორინგი;

ე) ინფორმაციული უსაფრთხოების საკითხებზე ანგარიშგება და სხვა სახის ადმინისტრაციული/საორგანიზაციო საქმიანობა;

ვ) ინფორმაციული უსაფრთხოების ზოგადი და დარგობრივი ტრენინგების ორგანიზება და ჩატარება;

ზ) სხვა მოვალეობები, რომლებსაც განსაზღვრავს კრიტიკული ინფორმაციული სისტემის სუბიექტი.

3. ინფორმაციული უსაფრთხოების მენეჯერი ანგარიშვალდებულია კრიტიკული ინფორმაციული სისტემის სუბიექტის ხელმძღვანელის ან მის მიერ შესაბამისად უფლებამოსილი თანამშრომლის ან ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელების უფლებამოსილების მქონე პირთა ჯგუფის (კოლეგიური ორგანოს) წინაშე. ყველა მნიშვნელოვანი გადაწყვეტილება, რომლებიც შეეხება ინფორმაციული უსაფრთხოების პოლიტიკის განხორციელებას, მიიღება ამ პუნქტით განსაზღვრული პირის (პირების) მიერ ან მასთან (მათთან) წინასწარი შეთანხმებით.

4. ინფორმაციული უსაფრთხოების მენეჯერი ადგენს ინფორმაციული უსაფრთხოების სამოქმედო გეგმას და ამ გეგმის შესრულების შესახებ ყოველწლიურ ანგარიშს წარუდგენს ამ მუხლის მე-3პუნქტით განსაზღვრულ პირს (პირებს) და მონაცემთა გაცვლის სააგენტოს.

კომპიუტერული უსაფრთხოების სპეციალისტი

მუხლი 9. კომპიუტერული უსაფრთხოების სპეციალისტი

•კრიტიკული ინფორმაციული სისტემის სუბიექტი ვალდებულია განსაზღვროს კონკრეტული პირი (პირები) ან თანამშრომელი (თანამშრომლები), რომელიც (რომლებიც) პასუხისმგებელია (პასუხისმგებელი არიან) კრიტიკული ინფორმაციული სისტემის სუბიექტის კომპიუტერული სისტემების უსაფრთხოების პრაქტიკული უზრუნველყოფისათვის (კომპიუტერული უსაფრთხოების სპეციალისტი).

2. კომპიუტერული უსაფრთხოების სპეციალისტის ძირითადი მოვალეობებია:

ა) კომპიუტერული სისტემების ყოველდღიური მონიტორინგი და შეფასება;

ბ) კომპიუტერული ინციდენტების იდენტიფიცირება და მათზე რეაგირება;

გ) კომპიუტერული ინციდენტებისა და უსაფრთხოების ზომების ანალიზი და ანგარიშგება;

დ) დახმარების ჯგუფთან კოორდინაცია;

კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი(cert.gov.ge)

საქართველოს კიბერსივრცეში ინფორმაციული უსაფრთხოების წინააღმდეგ მიმართული ინციდენტების მართვა;

კიბერუსაფრთხოების პრიორიტეტული საფრთხეების აღმოფხვრა, რომელსაც მიეკუთვნება:

ა) კიბერშეტევა, რომელიც საფრთხეს უქმნის ადამიანთა სიცოცხლესა და ჯანმრთელობას, სახელმწიფო ინტერესებს ან ქვეყნის თავდაცვისუნარიანობას;

ბ) კიბერშეტევა კრიტიკული ინფორმაციული სისტემის სუბიექტის ინფორმაციული სისტემების წინააღმდეგ;

გ) კიბერშეტევა, რომელიც საფრთხეს უქმნის სახელმწიფოს, ორგანიზაციის ან კერძო პირის ფინანსურ რესურსებს ან/და საკუთრების უფლებას;

3. დახმარების ჯგუფის მოვალეობებია:

ა) კრიტიკული ინფორმაციული სისტემის ინფორმაციული უსაფრთხოების დაცვის შესახებ რეკომენდაციების გაცემა;

ბ) კომპიუტერული ინციდენტების დროული გამოვლენა;

გ) კომპიუტერულ ინციდენტებზე რეაგირება და მათზე რეაგირების კოორდინაცია;

დ) კომპიუტერული ინციდენტების აღრიცხვა და მათზე რეაგირების პრიორიტეტების დადგენა და კატეგორიზაცია;

ე) კომპიუტერული ინციდენტების ანალიზი;

კომპიუტერულ ინციდენტებზე დახმარების ჯგუფი(cert.gov.ge)

ვ) კომპიუტერული ინციდენტების შედეგების გამოსწორებისა და ზიანის მინიმიზაციის პროცესში დახმარების გაწევა;

ზ) კომპიუტერული ინციდენტების პრევენციისკენ მიმართული ზომების კოორდინაცია და ამგვარი ზომების დანერგვაში დახმარების გაწევა;

თ) ინფორმაციული უსაფრთხოების საკითხებზე ცნობიერების ამაღლება, მათ შორის, კრიტიკულ ინფორმაციულ სისტემაში არსებული საფრთხეებისა და სუსტი წერტილების შესახებ ინფორმაციის მიწოდება, თუ ინფორმაციის ამგვარი ხელმისაწვდომობა ზიანს არ აყენებს ინფორმაციულ უსაფრთხოებას;

ი) შესაძლო საფრთხეების შესახებ მომხმარებელთა ფართო წრის გაფრთხილება და მისთვის სათანადო ინფორმაციის მიწოდება;

კ) ინფორმაციული უსაფრთხოების საკითხებზე საგანმანათლებლო და ინფორმაციული უზრუნველყოფა;

ლ) საერთაშორისო დონეზე ინფორმაციული უსაფრთხოების საკითხებში წარმომადგენლობა და კოორდინაცია;

მ) სხვა მოვალეობები, რომლებიც დაკავშირებულია ინფორმაციული უსაფრთხოების მიზნებთან და განისაზღვრება კანონით ან სხვა ნორმატიული აქტით.

თავდაცვის სამინისტროს კიბერუსაფრთხოების ბიურო http://csbd.gov.ge. ინფორმაციული უსაფრთხოების მართვის სისტემა

რას ეფუძნება ინფორმაციული უსაფრთხოების მართვის სისტემის (იუმს) დანერგვა?

საქართველოს კანონს ინფორმაციული უსაფრთხოების შესახებ რომელიც მიღებულია 2012 წლის 5 ივნისს

მართვის სისტემები

ISO 9001 ხარისხის მართვის სისტემა

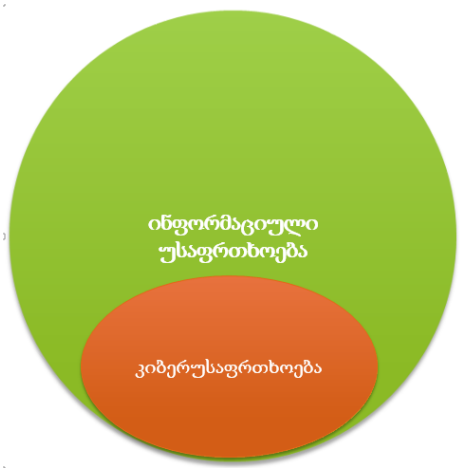
ISO 14000 გარემოს მართვის სისტემა

ISO 22000 ჯანმრთელობის დაცვის მართვის სისტემა

ISO 27000 ინფორმაციული უსაფრთხოების მართვის სისტემა

ხელმძღვანელობის როლი იუმს-ის დანერგვაში ყველა ხელმძღვანელი ცალსახად და მკაფიოდ უნდა ემხრობოდეს ინფორმაციული უსაფრთხოების მართვის იდეებს. უმაღლესი რანგის ხელმძღვანელობამ უნდა მოახდინოს საკუთარი მზაობისა და მხარდაჭერის დემონსტრირება PDCA (plan,do,check,act) ციკლი დაგეგმვა, დანერგვა, შემოწმება, გაუმჯობესება

- იუმს-ის ჩამოყალიბება
- იუმს-ის დანერგვა და ფუნქციონირება
- იუმს-ის მონიტორინგი და განხილვა
- იუმს-ის მხარდაჭერა და გაუმჯობესება
- ინფორმაციის არსებობის ფორმები
- ქაღალდზე არსებული ნაბეჭდი, ხელნაწერი
- ელექტრონული ფორმით კომპიუტერში
- მაგიდაზე, პრინტერში, ქსეროქსში დატოვებული დოკუმენტები
- შემთხვევით მოსმენილი/ გაგონილი საუბარი დერეფანში/ტრანსპორტში
- სანაგვე ყუთებში გადაყრილი და ა.შ.



ინფორმაციული უსაფრთხოება და კიბერუსაფრთხოება ინფორმაციის მახასიათებლები (კონფიდენციალურობა, მთლიანობა, ხელმისაწვდომობა) CIA (Confidentiality, Integrity, Availability) **კონფიდენციალურობა** - ინფორმაციის ხელმისაწვდომობის უზრუნველყოფა მხოლოდ ავტორიზებული პირებისთვის.

მთლიანობა-ინფორმაციის და მისი დამუშავების საშუალებების სიზუსტისა და მთლიანობის დაცვა

ხელმისაწვდომობა-საჭიროების შემთხვევაში, ავტორიზებული პირებისათვის შესაბამის აქტივებზე წვდომის უზრუნველყოფა

ინფორმაციის კლასები

კონფიდენციალური ინფორმაცია-ინფორმაცია, რომლის კონფიდენციალურობის, მთლიანობის ან ხელმისაწვდომობის ხელყოფას სავარაუდოდ მოჰყვება ორგანიზაციის ფუნქციებისათვის მნიშვნელოვანი ზიანი.

შინასამსახურებრივი-ინფორმაცია რომელიც განკუთვნილია მხოლოდ ორგანიზაციის თანამშრომლებისათვის.

ინფორმაციული უსაფრთხოების შესახებ კანონის თანახმად, ყველა ის ინფორმაცია რომელიც არ მოხვდება ზემოაღნიშნულ კლასებში ხდება საჯარო ინფორმაცია. ორგანიზაციას შეუძლია დამატებით ინფორმაციის კლასების განსაზღვრა (მაგ. პერსონალური მონაცემების კლასი და სხვა).

აქტივები

- ინფორმაციული აქტივები (მონაცემები ელექტრონული ფორმით)
- ინფორმაცია არაელექტრონული ფორმით (ქაღალდზე არსებული)
- ფიზიკური აქტივები (აპარატურა, კომპიუტერები და ა.შ.)
- ადამიანები (თანამშრომლები)
- ორგანიზაციის იმიჯი და რეპუტაცია
- პროცესები/მომსახურებები
- პროგრამული აქტივები (ელექტრონული მონაცემების დამუშავების საშუალებები)
- ინფორმაციული აქტივის მფლობელი

„მფლობელი“ არის პირი ან სტრუქტურული ერთეული, რომელსაც გააჩნია აქტივის შემუშავების, განვითარების, მხარდაჭერის, გამოყენების და დაცვის დადასტურებული უფლება „მფლობელობა“ არ ნიშნავს, რომ მას გააჩნია აქტივზე რაიმე სახის საკუთრების უფლება

აქტივების მართვა

აქტივების აღწერა (აქტივების ინვენტარიზაცია, აქტივების მფლობელების დადგენა, აქტივების სათანადო გამოყენება)

აქტივების შეფასება (რისკების ანალიზის და შეფასების ჩატარება მოცემულ აქტივებთან მიმართებაში)

აქტივების კლასიფიცირება (კლასიფიცირების მიზანია ინფორმაციის დაცვის სათანადო დონის უზრუნველყოფა)

- რისკების მართვა
- რისკების შეფასების მიდგომის განსაზღვრა
- რისკების გამოვლენა და მათი გავლენის გაანალიზება
- რისკების მოპყრობის გზების გამოვლენა
- რისკების მოპყრობის მიზნით კონტროლის მიზნების და კონტროლის მექანიზმების შერჩევა
- ხელმძღვანელობის მიერ ნარჩენ რისკებზე თანხმობის დადასტურება

კონტროლის მექანიზმების გამოყენებადობის განაცხადი (Statement of Applicability) ორგანიზაციამ უნდა შეარჩიოს კონტროლის მიზნები და კონტროლის მექანიზმები აღწეროს უკვე დანერგილი კონტროლის მიზნები და კონტროლის მექანიზმები.

საქართველოს იუსტიციის სამინისტროს, მონაცემთა გაცვლის სააგენტოს კომპიუტერულ ინციდენტებზე სწრაფი რეაგირების ჯგუფის შესახებ(Cert.gov.ge)

თანამშრომლობა და პარტნიორობა

პარტნიორი ორგანიზაციები:

- International Multilateral Partnership Against Cyber Threats
- Global Forum of Incident Response and Security Teams
- Services for Security and Incident Response Teams
- Cert.gov.ge is authorized to use CERT Trademark

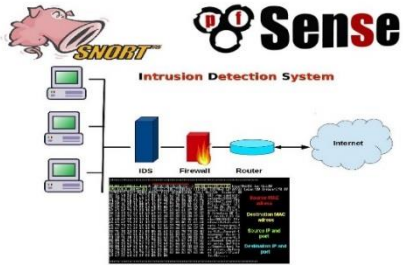
სერვისები

- Blacklists.cert.gov.ge IP, Domain, Malware ZONE

- SAFE DNS Georgia 5.159.16.16 5.59.20.20

- NetFlow Sensors(NfDump NfSen); Network Analyze;
- Detection: SSH Brute Force Attack, Botnet, DDoS Attack

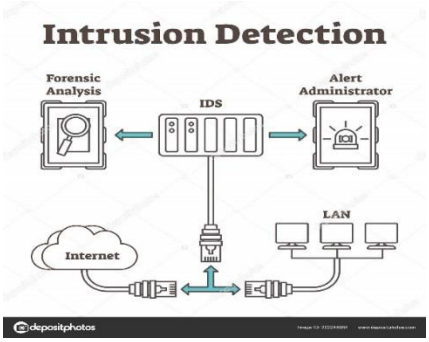
- Sensor Network Services(Snort):
- Automated analysis of the security of the network flow problems
- VRT rules of the securitues



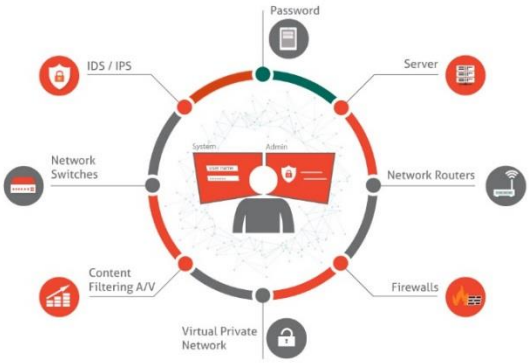
- HoneyPots. Emulation Of Popular Vulnerable Software
- Using Open Source Honeypot Software:
- Kippo(ssh)
- Dionaea(SMB, http, tftp, MSSQL, MySQL, SIP)
- Conpot(SCADA)
- Capturing Attacker IP Addresses

- More Than 2000 Attacks Per Day

- Website Intrusion Detection Monitor Web pages for Instrusions



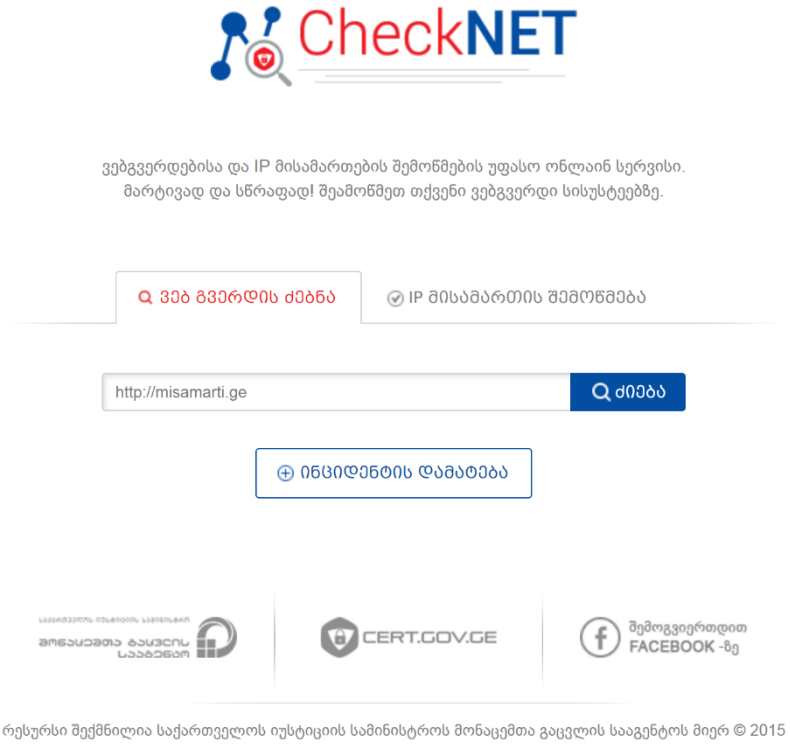
- Penetration Test



Phishing Attack Simulation

პარტნიორები

- ვებგვერდებისა და IP მისამართების შემოწმების უფასო ონლაინ სერვისი.

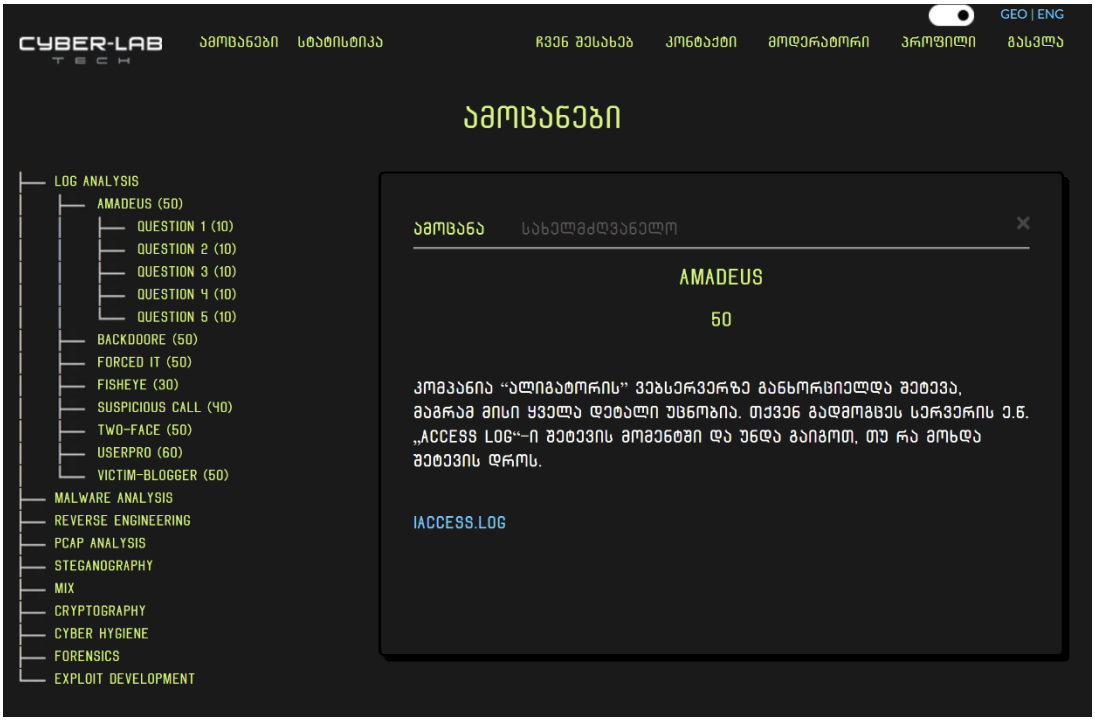


ტრენინგები და სწავლება

- CyberExe სავარჯიშოები კერძო დასაჯარო სექტორისთვის

- CyberCube ახალგაზრდებისთვის 25 წლამდე

Cyber-lab.tech



Cert.gov.ge-ს წარმატება

საქართველო რეიტინგებში

Europe

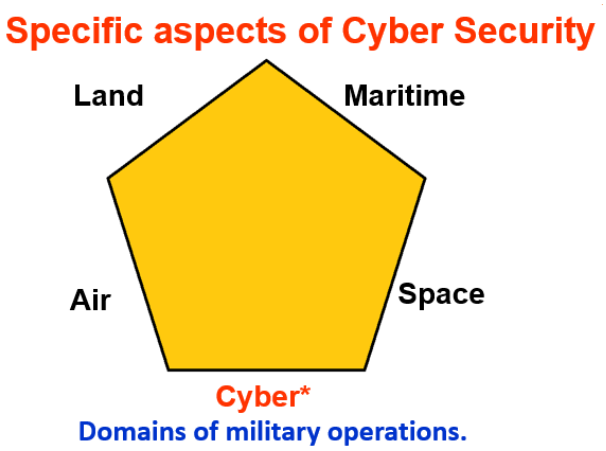
Member State	Score	Regional Rank	Global Rank
United Kingdom	0.931	1	1
France	0.918	2	3
Lithuania	0.908	3	4
Estonia	0.905	4	5
Spain	0.896	5	7
Norway	0.892	6	9
Luxembourg	0.886	7	11
Netherlands	0.885	8	12
Georgia	0.857	9	18
Finland	0.856	10	19
Turkey	0.853	11	20
Denmark	0.852	12	21
Germany	0.849	13	22
Croatia	0.840	14	24
Italy	0.837	15	25
Austria	0.826	16	28
Poland	0.815	17	29
Belgium	0.814	18	30

Cezar Vasilescu - PhD. Regional Department of Defense Resources Management Studies (DRESMARA), Brasov, ROMANIA

Specific aspects of Cyber Security

Definition*

- global domain within the information environment;
- consisting from interdependent networks of information technology infrastructures;
- Includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers



Characteristics

- It is created by humans - differs significantly from land, maritime, air and space domains;
- It is embedded in all other four domains;
- It's dynamic, evolving and in continuous expansion;
- Changes appear due to scientific research and development;
- Requires continuous attention and maintenance;

Cyber space (e-Space) components

Physical space

Sum of electronic connectivity

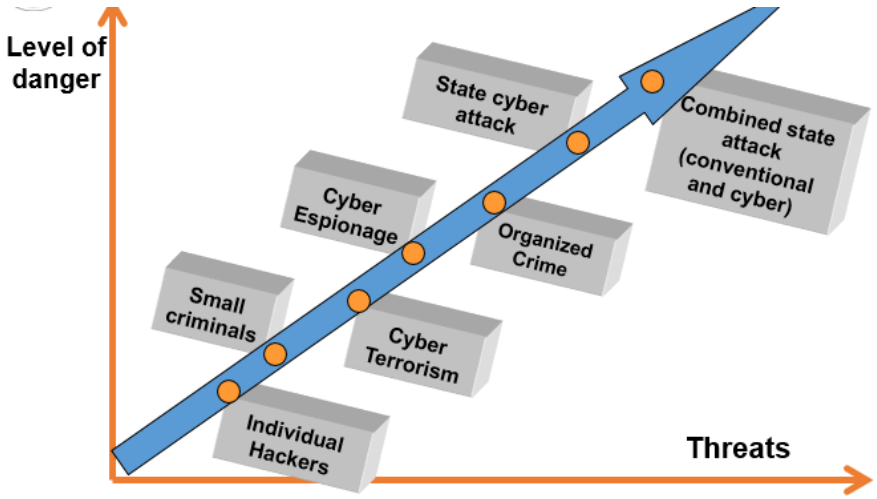
Virtual space

Electronic realm in which global connectivity exists, and in which computer networks function

Contextual space

Determined and influenced by human perception

"Cognitive environment" - ***what we know it what we believe***



Critical (Information) Infrastructures

Definition*

- assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety.

Key Resources*

- publicly or privately controlled resources essential to the minimal operations of the economy and government.

Definition*

- An asset, system or part located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions".
- Entities and infrastructures which process, store, exchange information required to provide the services that are crucial to a nation's existence and the wellbeing of the society.

CLASSIFICATION

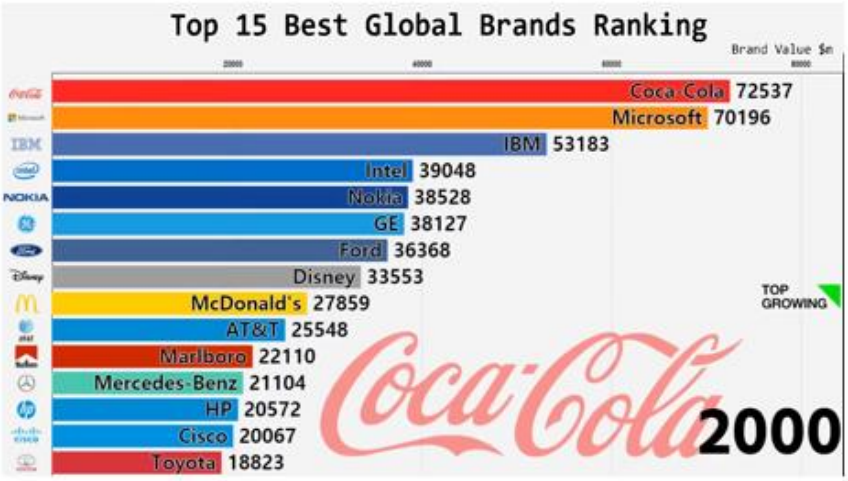
- **Core**: *Telecommunications, electric power, water*
  - Significant Failures = Crisis within hours
  - Limited or No "Local Reserves" in case of failure
- **Essential:** *Banking, transportation, public health*
  - Significant failures = Crisis within days
  - Some "local reserves" will be available
- The **Information Infrastructure** is a special case
- The most important "infrastructure" - people confidence

"If you lose the battle in protecting the Information Infrastructure, winning the other way may not matter"

STRATEGIC FRAGILITY

- **Automation of Nations' Infrastructure**
  - Information and communications
  - Electric power generation, transmission and distribution
  - Oil and gas storage and distribution
  - Banking and finance
  - Transportation
  - Water supply
  - Emergency assistance

Top 15 best global brands (2000-2018)

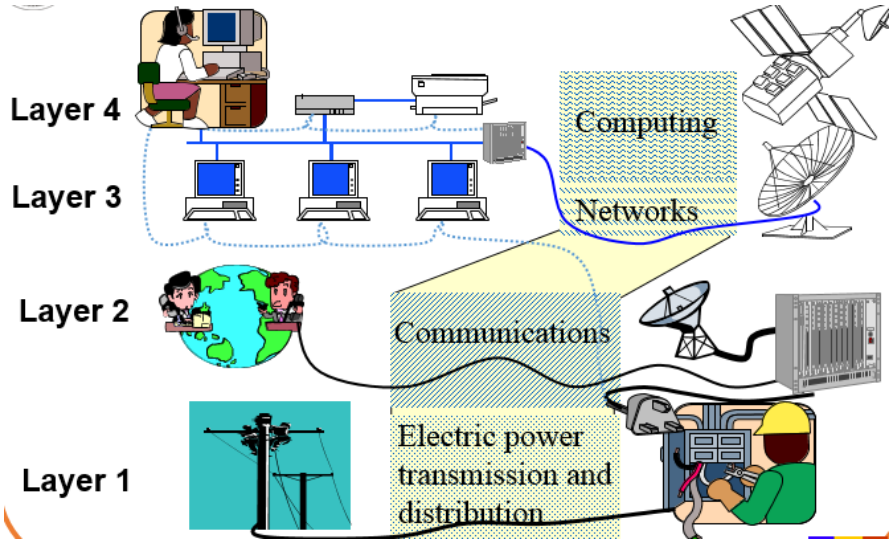


Critical Infrastructure Sectors for an EU state

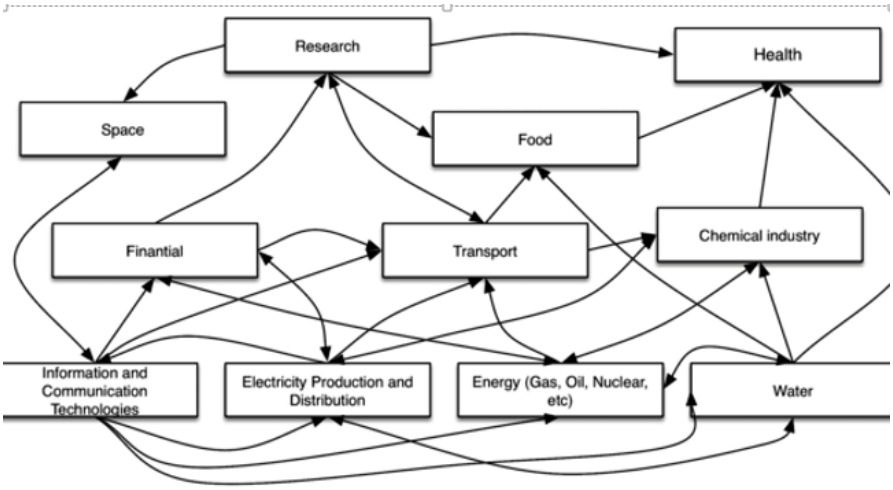
I. Energy	electrical power, oil, gas
II. Sanitation	water supply, waste water collection and processing
III. Transportation	roads, railway, traffic organisation, civil/military aviation
IV. Communications	information technology infrastructure, telecommunications, Internet access
V. Security / Safety	military, police, emergency services
VI. Medicine	health-care, hospitals
VII. Research	industrial and scientific developments

VIII. Finances	state treasury, banks, money wire transfers
IX. Politics	national secrets, foreign policy and affairs

Infrastructures – Dependencies and Vulnerabilities



Critical Infrastructure Sectors - Interdependencies



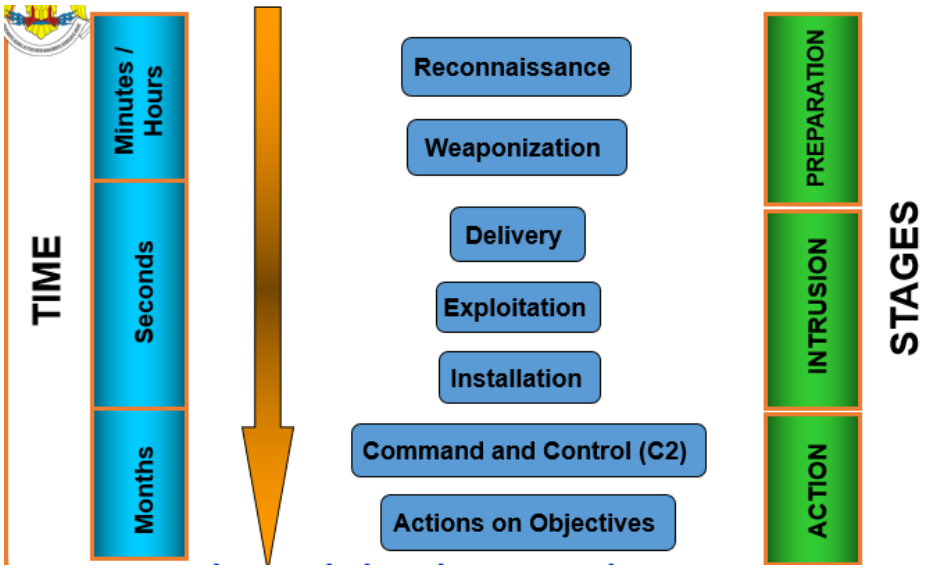
The Performance Metric of a Cyber Attack

The networked systems and the critical infrastructures they support are vulnerable to attacks.

*"For an attack to be successful it only has to cause **disruption to a significant number of citizens**.*

Such a focused attack would become an immediate, and overwhelming distraction for the national leadership."

Specific aspects of Cyber Security



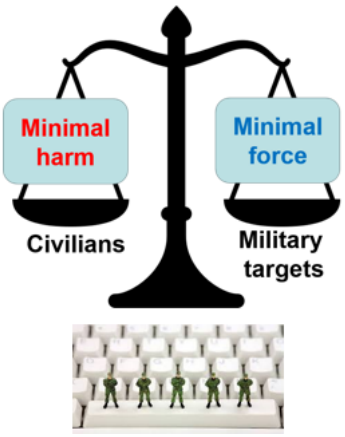
- **Observation**
  - *What network segments (components) are visible for an attacker*
- **Cover and Concealment**
  - *What can I hide from observation*
- **Obstacles**
  - *How can I make the network difficult to be attacked*
- **Key "terrain" analysis**
  - *What could provide an advantage*
- **Action measures**

Challenges to Traditional Concepts of War

Challenge war principles

1.Proportionality

- Unknown:
  - scale
  - scope
  - duration
  - intensity



SCADA Systems - (**S**upervisory **C**ontrol and **D**ata **A**cquisition)

Definition*

- Systems and networks designed for command and control of industrial processes.
- cyber systems for real time data analysis;
- represent a major component of Industrial Control Systems
- responsible for monitoring and controlling of a variety of processes and operations (e.g.: natural gas and energy distribution, oil refining or monitoring railway transportation).

Major risks:

- are connected to vulnerable legacy computer networks
- usage of standard hardware and software platforms with known vulnerabilities
- existence of vulnerable remote connections
- the functionality real time requirements contradict the information security measures - result in communication delays

RISI Online Incident Database

It includes:

- accidental cyber-related incidents

- incidents of a cyber security nature that directly affect industrial SCADA and process control systems
- deliberate events - external hacks, Denial of Service (DoS) attacks, and virus/worm infiltrations

The Performance Metric of a Cyber Attack

The impact of the attack (incident)

Negligible: Customers, users, and client systems are not affected

Tolerable: Customers, users or client systems are affected within given limits

Intolerable: Customers, users or client systems are affected beyond specified limits

Control modes required to handle the situation

Procedured Response

when incidents are minor, responders follow prescribed response & repair procedures to fix them

Supervised Incident Management

when incidents become complex, they usually need an Incident Management Team to coordinate the execution of one or several Disaster Recovery Plans.

Creative Solutioning

incidents are again rather minor but tricky (i.e. sources of failure and solutions are hard to find)

diagnosis procedures do not allow to find solutions

responders need to adapt or ignore prescribed procedures and must invent, create ad hoc solutions based on their experience, skills or knowledge.

Tactical Decision-Making

incidents are major or extreme

surprise makes disaster recovery plans useless

responders need to handle situations and (re)gain initiative over complex, agile and destabilizing circumstances

A crisis management team and a chain of command are usually necessary to coordinate the required set of expertise and actions.

Critical infrastructures are owned and operated by the private sector:

In U.S.A. - about 98%

In Romania – an increasing percentage (>75%)

Infrastructures are vulnerable to both physical and cyber attacks

Therefore, CIP depends on voluntary Public-Private Partnerships (PPPs)

prevention-focused - focus on preparation and planning

response-focused - focus on response and recovery

umbrella - cover both areas

Building Trust in Voluntary

Public-Private Partnerships (PPPs)

Issues between:

- ***private organizations*** – which may be competitors
- ***public organizations*** - in which there may be political challenges and competition for budget
- ***private and public sectors*** - in which the private sector may feel that the issues discussed may become the subject of penalties or regulation
- ***public and private sectors*** - in which the public sector may feel that that the private sector is being secretive about issues that may affect services provided by the public sector

Main issue

The need for PPP members to hold a specific level of security clearance

Mechanisms - classified information to be shared using an agreed protocol

"Traffic Light Protocol" - a simple color code to identify information (red, amber, green, white)

"Chatham House Rules" - providing anonymity to speakers and encourage openness and information sharing

The need for security is not new

New dimensions of the CIP problem:

Reliance on linked, inter-dependent IT networks

Vulnerability to physical as well as cyber attacks

Rapidity of damage

Globalization of networks and its consequences

Dependence on vulnerable infrastructures

Critical Infrastructure Protection

Steps

1. Identify Critical Systems and Infrastructures
2. Develop Clear Understanding of Mandates
3. Inventory and Audit Existing Capabilities
4. Develop an Organizational Roadmap
5. Identify Major Actions and Milestones
6. Major issue for most organizations (military or civilian)
7. Physical and cyber aspects

Importance of *specialists*

Importance of an *effective media strategy*

Reduce public anger by ensuring they are aware of the huge efforts being undertaken

Responders:

category 1 (e.g. police, fire and rescue, local councils, etc.) and

category 2 (e.g. utilities, transport and health bodies etc.)

Protection of *key operational (business) records*

Plans and exercises: Who does what?

Levels of awareness

Unconscious Incompetence

Staff are unaware of BC issues. They do not know what they don't know

Conscious Incompetence

Staff are aware of BC in general. They know little about its detailed requirements

Conscious Competence

Staff are cognizant of BC issues and are proficient (e.g. following documented procedures)

Unconscious Competence

Staff are instinctively fully competent in applying BC in a variety of circumstances

Ad-hoc approach

It is made up at the time of the incident

Requires little effort to set up or maintain

Most likely will fail, because: Individuals make incorrect assumptions, in respect to:

their own responsibilities

the responsibilities of others

what facilities and arrangements can be relied upon during the event