დანართი 1

სისტემური ადმინისტრატორების, მათი სააღრიცხვო ჩანაწერების, სესიების დაცვისა და კონტროლის სისტემა

(ტექნიკური დავალება)

CVP 48732000

სისტემური ადმინისტრატორების, მათი სააღრიცხვო ჩანაწერებისა და სესიების კონტროლის პროგრამული უზრუნველყოფა შემდეგში მოხსენიებული როგორც «პროგრამული უზრუნველყოფა», უნდა წარმოადგენდეს ორგანიზებულ პროგრამულ-აპარატული საშუალებების ერთობლიობას. იგი უნდა წარმოადგენდეს მრავალმომხმარებლიან სისტემას დაშვების სხვადასხვა დონეებით. სისტემასთან დაშვების რეგულირების მექანიზმი უნდა იყოს უზრუნველყოფილი დისკრეტული მოდელით რომელიც მოიცავს დაშვების დონეების დაყოფას როლების მიხედვით. მომხმარებლების დაშვების დონეები უნდა განისაზღვრებოდეს შეზღუდული ობიექტებით (პაროლები, კონტროლირებადი აღრიცხვის ჩანაწერები, ჩანაწერების ფაილები და სესიების ჩანაწერები) და ასევე მოვლენათა აღრიცხვის ჩანაწერებთან გამიჯნული წვდომა. მიმწოდებელმა უნდა უზრუნველყოს პროგრამული უზრუნევყოფის ინტეგრაცია 5 სამუშაო დღის განმავლობაში.

პროგრამა უნდა უზრუნველყოფდეს გამოყენებული აღრიცხვის ჩანაწერების დაცვას საქაერონავიგაციის სისტემებთან მუშაობის დროს.

პროგრამულ უზრუნველყოფას უნდა ჰქონდეს სამომავლოდ დამატებითი მოდულების შეძენის შემთხვევაში ფუქციუონალის გაფართოების შესაძლებლობა. იგი ასევე უნდა იყოს მოქნილი და ერგებოდეს საქაერონავიგაციის ავტომატიზირებული მართვის სისტემის ცვლილებას.

მოთხოვნები პროგრამული უზრუნველყოფის მიმართ

პროგრამული უზრუნველყოფა უნდა უზრუნველყოფდეს შემდეგ პროცედურებს:

მართვის ობიექტებზე პაროლების ავტომატიზირებული ცვლილება განსაზღვრული პოლიტიკის შესაბამისად.

ინფორმაციული ტექნოლოგიების ინფრასტრუქტურასთან მოშორებული მართვის სეანსების ვიდეო და ტექსტურ ჩაწერას.

მართვის ობიექტებთან დაშვების შეთანხმების პროცესის განხორციელება

პროგრამული უზრუნველყოფა უნდა პასუხობდეს შემდეგ ფუნქციონალურ მოთხოვნებს:

მართვის ობიექტებზე პაროლების ცვლილების პროცედურების აწყობადი ბრძანებები.

დაშვების მინიჭების შეთანხმების აწყობადი პროცედურების მხარდაჭერა.

გამოყოფილი იზოლირებული სერვერი მართვის ობიექტების პაროლების შესანახად.

პრივილეგირებული მომხმარებლის სააღრიცხვო ჩანაწერის არსებობა სისტემასთან წვდომისათვის ამოღებადი გაზიარებადი გასაღების გამოყენების შესაძლებლობით.

არცერთ მომხმარებელს არ უნდა ჰქონდეს აღრიცხვის ფაილების წაშლის შესაძლებლობა.

30 დღის განმავლობაში დაცული ფაილების საცავიდან არცერთ მომხმარებელს არ უნდა ჰქონდეს ფაილის წაშლის უფლება.

ფაილების საცავი უნდა უზრუნველყოფდეს ყოველი ფაილის ინდივიდულაური გასაღებით დაშიფვრას.

კონტროლირებადი ადმინისტრატორების სესიების ჩანაწერების შენახვის ვადა უნდა შეადგენდეს მინიმუმ 6 თვეს მითითებული სესიების რაოდენობის გათვალისწინებით (5 დღე სამუშაო კვირა, 8 საათიანი სამუშაო დღე).

პროგრამული უზრუნველყოფა უნდა უზრუნველყოფდეს მინიმუმ 10 მომხმარებლის წვდომას საქაერონავიგაციის შიდა ინფრასტრუქტურის მართვის ობიექტებთან.

პროგრამული უზრუნველყოფა უნდა იყოს თავსებადი საქაერონავიგაციაში არსებულ შემდეგ სისტემებთან :

ინფორმაციული სისტემა	პლატფორმა	რაოდენობა
სერვერი Windows	Server 2012R2	1
სერვერები Unix	RedHat Linux 5.6,5.7,5.8, 6.5	8
მეტეოროლოგიური რადარი	DWSR-2001X SIDPOL	1

პროგრამული უზრუნველყოფის არქიტექტურა

პროგრამულ უზრუნველყოფას უნდა ჰქონდეს კლასტერირების შესაძლებლობა და ვირტუალურ სისტემებთან თავსებადობა. პროგრამული უზრუნველყოფა უნდა შედგებოდეს შემდეგი კომპონენტებისაგან:

ავტორიზაციის მოდული – კონტროლირებადი ადმინისტრატორების დაშვების კონტროლის WEB ინტერფეისი, აუტენტიფიკაციის უზრუნველყოფით, მართვის ობიექტის შერჩევითა და შესაბამისი კლიენტის გაშვებით;

ტერმინალის მოდული – ადმინისტრირების ინსტრუმენტების შესასრულებელი სივრცე და კონტროლირებადი ადმინისტრატორის მიერ შესრულებული ოპერაციების ჩაწერა.

პოლიტიკის მართვის მოდული – უზრუნველყოფს პრივილეგირებული აღრიცხვის ჩანაწერების პაროლების მართვას დაშვების ობიექტებზე (მართვად სისტემებზე);

უსაფრთხო საცავის მოდული – უზრუნველყოფს პრივილეგირებული სააღრიცხვო ჩანაწერების პარამეტრების შენახვას ასევე უზრუნველყოფს მართვადი ადმინისტრატორების მიერ ყველა მართვად სისტემაზე განხორციელებული ოპერაციების არქივის ორგანიზებას.

პროგრამული უზრუნველყოფის ფუნქციონალური სტრუქტურის მოთხოვნები

პროგრამული უზრუნველყოფა უნდა შედგებოდეს შემდეგი ფუნქციონალური ქვესისტემებისაგან:

პაროლების პოლიტიკის ქვესისტემა;

პრივილეგირებული მომხმარებლების სესიების ჩამწერი ქვესისტემა;

პაროლების, კონტროლირებადი სისტემის ადმინისტრატორების სესიების ვიდეოჩანაწერებისა და ჟურნალირების დაცული შენახვის ქვესისტემა.

სისტემის ფუნქციონირების რეჟიმები

პროგრამული უზრუნველყოფა ფუნქციონირებს უწყვეტ რეჟიმში (24 საათი 7 დღე კვირაში) გარდა დაგეგმილი ტექნიკური სამუშაოებისა.

პროგრამული უზრუნველყოფა უნდა უზრუნველყოფდეს შემდეგ რეჟიმებში ფუნქციონირებას:

ჩვეული რეჟიმი - ამ რეჟიმში ხელმისაწვდომია პროგრამული უზრუნველყოფის კომპონენტების მიერ უზრუნველყოფილი ყველა სერვისი;

ავარიული რეჟიმი - ამ რეჟიმში პროგრამული უზრუნველყოფის ექსპლუატაცია ხორციელდება მართვის ობიექტების ან მათთან დამაკავშირებელი ინფრასტრუქტურის მტყუნების შემთხვევაში.

ფუნქციონალური მოთხოვნები:

	მოთხოვნის აღწერა
1	აღრიცხვის ჩანაწერების პაროლების ავტომატიზებული მართვა შემდეგი ტიპის ოპარაციულ სისტემებზე: Windows; Unix.
2	დაცული აღრიცხვის ჩანაწერების პაროლების ხელის რეჟიმში მართვა.
3	ადმინისტრატიული (პრივილეგირებული) სესიების მართვა შემდეგი ტიპის ოპარაციულ სისტემებზე: Windows; Unix.
4	სესიის ჩაწერის შესახებ კონტროლირებადი ადმინისტრატორის ინფორმირების შესაძლებლობა.
5	რეალური დროის რეჟიმში უსაფრთხოების ადმინისტრატორისათვის ნებისმიერი კონტროლირებადი ადმინისტრატორის სესიაში ჩართვის შესაძლებლობა.
6	უსაფრთხოების ადმინისტრატორის მიერ სესიაში ჩართვის შესახებ კონტროლირებადი ადმინისტრატორის ინფორმირების შესაძლებლობა.
7	უსაფრთხოების ადმინისტრატორს უნდა ჰქონდეს მოქნილად აწყობადი უფლებების დონეები კონტროლირებადი ადმინისტრატორის სესიასთან მისაერთებლად, მაგალიოთად: მხოლოდ დაკვირვება; სესიის შეწყვეტის უფლება; მიმდინარე სესიის ფარგლებში ჩარევის უფლება.
8	ჩანაწერების ექსპორტის და სისტემის გარეთ აღწარმოების შესაძლებლობა.
9	პრივილეგიურებული აღრიცხვისჩანაწერების პაროლების ექსპორტირების შესაძლებლობა.
10	ვიდეოჩანაწერის შესაბამისი ფრაგმენტის სწრაფად გამოსაძახებლად შეტყობიონებების ტექსტური მიმოცვლის სისტემებისათვის (telnet, ssh) ბრძანებების ჟურნალირების შესაძლებლობა.

საქაერონავიგაციის ქსელური ინფრასტრუქტურის ვირუსებისაგან დაცვის პროგრამული უზრუნველყოფა

(ტექნიკური დავალება)

CVP 48761000

მოთხოვნები მართვის კონსოლისათვის (პანელისთვის):

სისტემის ყველა კომპონენტის მართვა უნდა ხდებოდეს მართვის ერთიანი ვებ კონსოლის მეშვეობით;

კონსოლის ოპერატორების აუთენთიფიკაცია უნდა ხდებოდეს ადგილობრივი მონაცემთა ბაზის ან დომენური აუთენთიფიკაციის მეშვეობით;

სისტემასთან დაშვების როლური მოდელი;

კონსოლის ოპერატორების მოქმედებების სავალდებულო ჟურნალირება (აღრიცხვა);

ჩაშენებული მონაცემთა რეზერვირების შესაძლებლობა Disaster Recovery-ს მეშვეობით;

კონსოლში სისტემების სიის ფორმირება ჯგუფების მიხედვით, როგორც ხელით მართვის რეჟიმში, ისე კატალოგების სტრუქტურის სინქრონიზაციის მეშვეობით;

დაცვის მოდულების გაშლა ავტომატურ და ხელით მართვის რეჟიმში;

ფუნქციონირებადი (გაშლილ მდგომარეობაში) სისტემების მუშა მდგომარეობაში მხარდაჭერა (პროგრამული უზრუნველყოფის განახლება, პოლიტიკების სინქრონიზაცია);

საბოლოო წვდომის წერტილების (სამართავი წერტილები, ენდფოინთი) მდგომარეობის კონტროლი რეალური დროის რეჟიმში;

საინსტალაციო პაკეტების სამი განშტოების მხარდაჭერა (მიმდინარე, წინა, სატესტო);

სისტემების ავტომატური სორტირება ტიპის, ჯგუფის, აპარატული რესურსების და სხვა კრიტერიუმების მიხედვით;

მონაცემთა ვიზუალიზაციის გზით აღრიცხვის წარმოება;

განახლების წყაროების ხისებრი სტრუქტურის გაკეთების შესაძლებლობა (SMB, HTTP, FTP);

ცალკეული ჯგუფების და სისტემების დონეზე სხვადასხვა პოლიტიკების გამოყენების შესაძლებლობა;

დაცვის მოდულების გაშლასთან, განახლებასთან და კონტროლთან დაკავშირებული დავალებების დაგეგმვის ჩაშენებული მექანიზმი;

კომპანიის სტრუქტურის, ჯგუფების, ქვეჯგუფების და ცალკეული სისტემების დონეზე ცალკეული დავალებების მიცემის შესაძლებლობა;

საბოლოო წვდომის წერტილსა და კონსოლს შორის არაგეგმიური სეანსის ინიციალიზაციის შესაძლებლობა;

კომპანიის სტრუქტურის, ჯგუფების, ქვეჯგუფების და ცალკეული სისტემების დონეზე საბოლოო წვდომის წერტილსა და კონსოლს შორის კავშირის ინტერვალის დაკონფიგურირების შესაძლებლობა;

განახლების ძირითადი რეპოზიტორიების სარკეების შექმნის შესაძლებლობა;

სისტემის ფუნქციონალის გაზრდის შესაძლებლობა ახალი სერვერების დამატების გარეშე;

მოთხოვნები სისტემის სამომავლო გაფართოების შესაძლებლობასთან დაკავშირებით.

სისტემას უნდა ჰქონდეს შემდეგი მოდულების მხარდაჭერა სამომავლო გაფართოებისათვის: მონაცემთა დაშიფრვა, მონაცემთა გაჟონვის თავიდან აცილება (DLP),უკანონო შეღწევის თავიდან აცილება (IPS), ვებ გასასვლელი (მარშრუტიზატორი, Web Gateway).

მოთხოვნები სისტემის შესაძლებლობებთან (ფუქციონალთან):

საბოლოო წვდომის წერტილზე ლოკალური ინტერფეისის სრულიად ან ნაწილობრივ ბლოკირების შესაძლებლობა;

კლიენტების შემდეგ ოპერციულ სისტემებთან თავსებადობის შესაძლებლობა: Widows, Linux, Mac;

ფაილების სკანირების შესაძლებლობა მათთან პროცესების მიმართვის დროს (On-Access Scan);

ფაილების გეგმიური სკანირების შესაძლებლობა, როგორც ცენტრალიზებულად დაგეგმილი, ისევე მომხმარებლის მიერ განსაზღვრული დროის შუალედში;

საფრთხის შემცველი პროგრამების ქმედების ანალიზი და შეკავება, მოშორებულ სერვერზე (“ღრუბელზე”) წვდომის გარეშე;

კლიენტების (აგენტების) მეშვეობით სისტემური რესურსების უტილიზაციის შესაძლებლობა;

ფაილების და პროცესების რეპუტაციის შემოწმების შესაძლებობა მოშორებული სერვერის (“ღრუბელის”) მეშვეობით;

ბრაუზერის პლაგინების მეშვეობით საბოლოო წვდომის წერტილებისათვის ინტერნეტ საფრთხეების ბლოკირების შესაძლებლობა;

რესურსის უნიფიცირებული მისამართების (URL) რეპუტაციის შემოწმების შესაძლებლობა;

სამუშაო სადგურების მიერ ვებ რესურსებთან და ვებ რესურსების ცალკეულ კატეგორიებთან წვდომის შეზღუდვა;

არაავტორიზებული ელემენტების ავტომატურ რეჟიმში გაშვების რეგისტრაციის ბლოკირება;

დროებითი საქაღალდეებიდან (ფოლდერებიდან) ფაილების/სკრიპტების გაშვების ბლოკირება;

საფოსტო სერვერების დაცვა წერილების შენაარსის ანალიზის მეშვეობით;

მოდულებისმუშაობაში ჩარევისაგან ავტომატური თვითდაცვა;

უკანონო შემოღწევისაგან გაფრთხილების ჩაშენებული სისტემა;

ექსპლოიტებისაგან დაცვის ჩაშენებული სისტემა;

ჩაშენებული ქსელური ეკრანი (ფაირვოლი);

ფაირვოლის დინამიური წესების შექმნის შესაძლებლობა;

სხვადასხვა ქსელებისათვის (ქსელური/უკაბელო/ვირტუალური) ფაერვოლის განსხვავებული წესების შექმნის შესაძლებლობა;

ინფორმაციის პორტატული შემნახველების და სხვა მოწყობილობების ბლოკირების შესაძლებლობა მოწყობილობების ჩაშენებული კონტროლის მეშვეობით;

ანტივირუსული მონაცემთა ბაზების და პროგრამული უზრუნველყოფის განახლების შესაძლებლობა ინტერნეტთან წვდომის გარეშე;

მომხმარებელთა უფლების შეზღუდვის შესაძლებლობა შეცვალონ ოპერაციული სისტემის და ინტერნეტ ბრაუზერების პარამეტრები;

ისეთი ინტერნეტ ბრაუზერების გაშვების ბლოკირების შესაძლებლობა, რომლებიც არ არის ნებადართული;

ისეთი პროგრამული უზრუნველყოფის გაშვების ბლოკირების შესაძლებლობა, რომელიც არ არის ნებადართული;

დროებითი საქაღალდეებიდან ფაილების ბლოკირების შესაძლებლობა;

ფაილების, საქაღალდეების და ავტომატურ რეჟიმში გაშვებადი ელემენტების მოშორებულად შექმნის აკრძალვის შესაძლებლობა;

ფაილების ახალი გაფართოების რეგისტრაციის აკრძალვის შესაძლებლობა;

საეჭვო შესრულებადი ფაილების ოპერაციული სისტემისაგან იზოლირებულ გარემოში გაშვების შესაძლებლობა;

საეჭვო შესრულებადი ფაილების განსაზღვრა შემდეგი მახასიათებლებით: სახელის ან მდებარეობის, MD5 ჰეშის, ციფრული ხელმოწერისა და რეპუტაციის მიხედვით;

საეჭვო შესრულებადი ფაილების რეპუტაციის ავტომატური განსაზღვრა მოშორებულ სერვერთან (“ღრუბელთან”) წვდომის მეშვეობით;

რეპუტაციათა ბაზაში შემდეგი რეპუტაციების დონის არსებობა: სანდო, საფრთხის შემცველი, უცნობი, მეტნაკლებად სანდო, მეტნაკლებად საფრთხის შემცველი.

პროგრამული პაკეტი უნდა უზრუნველყოფდეს 700 კომპიუტერის დაცვას.