ინფორმაციული უსაფრთხოების სისტემები

კონსტანტინე ობოლაძე
საქართველოს ტექნიკური უნივერსიტეტი

რეზიუმე

აღნიშნული თემა მოიცავს ინფორმაციის უსაფრთხოების სისტემებს მობილური მოწყობილო-ბებისთვის. მასში მოყვანილია უსაფრთხოების დონის გაზრდის შემუშავებული მეთოდები. ასევე განხილულია კონკრეტული ამოცანები და მათი გადაწყვეტის მაგალითები.

საკვანძო სიტყვები: მობილური მოწყობილობა. უსაფრთხოება. Exchange Activesync.

1. შესავალი

მობილური მოწყობილობები დღევანდელ სწრაფად განვითარებად მსოფლიოში გახდა ტექნოლოგიების მამოძრავებელი ძალა. თუ დაუჯერებთ GSM Association Press-ის მიერ მომზადებულ სტატისტიკას, უახლოეს მომავალში მსოფლიოს მოსახლეობის 90% დაფარული იქნება მობილური ქსელებით. ასევე მობილური მოწყობილობების გაყიდვების მონაცემებზე დაყრდნობით შეგვიძლია ვთქვათ, რომ მოთხოვნა წინა წლების მაჩვენებლებთან შედარებით სწრაფი ტემპებით იზრდება. ამ ზრდის ტემპის ერთ-ერთი მიზეზი გახლავთ მობილურ მოწყობილობებში რიგი ფუნქციების დამატება და არსებულის გაუჯობესება. ისინი აღჭურვილნი არიან მრავალი სერვისით, რაც მომხმარებელს საშუალებას აძლევს ისარგებლოს მომსახურების დიდ არჩევანით, მათ შორის პირადი მონაცემების მართვითა და გასართობი შესაძლებლობებით.

2. ძირითადი ნაწილი

მობილური მოწყობილობების ასეთმა განვითარებამ, მომხმარებელი მასზე დამოკიდებული გახადა. ხალხის უმეტესობას მობილური მოწყობილობის გარეშე გადაადგილება ვერც კი წარმოუდგენია. უბრალო მაგალითი რომ მოვიყვანოთ, აღნიშნული მოწყობილობით საბანკო ოპერაციების შესრულებაც თავისუფლადაა შესაძლებელი. ასევე შეგვიძლია ვისარგებლოთ კორპორატიული ელექტრონული ფოსტით, ან შეტყობინებების მიმოცვლის მოქნილი სისტემით, თუნდაც სინქრონიზაცია ვაწარმოოთ მრავალ პროგრამულ უზრუნველყოფასთან და აშ.

წინა წლებთან შედარებით მობილური მოწყობილობების მკვეთრმა განვითარებამ დღის წესრიგში დააყენა უსაფრთხოების საკითხი. გამომდინარე იქიდან, რომ ზემოაღნიშნული მოწყობილობები თავის-უფლად ურთიერთქმედებენ ინტერნეტთან და ყოფელდღიურად მომხმარებელი აწარმოებს უამრავი პროგრამული უზრუნველყოფის ჩამოტვირთვას, სტუმრობს ვებგვერდებს ან უკაბელო ქსელის საშუალებით (Wi-Fi, Bluetooth, Infrared, და აშ.) ახორციელებს ინფორმაციის მიმოცვლას. ამის გათვალისწინებით მაღალია იმის ალბათობა, რომ მობილურ მოწყობილობაზე ოპერაციული სისტემა დაინფიცირდეს და დაზიანდეს.

ამ სფეროს განვითარება ასევე ქმნის სხვა სახის საფრთხეებს. ერთ-ერთ ასეთ საფრთხეს წარმოადგენს მფლობელის მიერ მობილური მოწყობილობის შემთხვევით დაკარგვა. გამომდინარე იქიდან, რომ მას ამ მოწყობილობაზე შეიძლება ჰქონდეს პირადი ინფორმაცია, აუცილებელია მათი მაქსიმალურად დაცვა მსგავსი საფრთხეებისგანაც.

მობილური ტელეფონის უსაფრთხოების ფონის გამყარების მიზნით Juniper Networks-მა (ერთ-ერთი ლიდერი კომპანია საინფორმაციო და საკომუნიკაციო ტექნოლოგიების სივრცეში) 16 ქვეყანაში მობილერი მოწყობილობების საფრთხეებთან დაკავშირებით ჩაატარა კვლევა, რომელშიც მონაწილეობდა 6000-ზე მეტი მომხმარებელი. კვლევის შედეგი იყო შემდეგნაირი:

- ბოლო წლებში მავნე პროგრამების რაოდენობა 2.5 ჯერ გაიზარდა.
- მომხმარებლის 44% მობილურ მოწყობილობას იყენებს როგორც სამსახურებრივი, ასევე პირა-დი მიზნებისთვისაც.
- მომხმარებლების 80% მობილურ მოწყობილობებს უნებართვოდ იყენებს სამსახურის ქსელთან დასაკავშირებლად.
- 10 დან 9 მობილურ მოწყობილობაზე საერთოდ არ იყო არანაირი დაცვის მექანიზმი.

- ინფიცირებული მობილური მოწყობილობების 60%-ზე დარეგისტრირებული იყო ჯაშუშური პროგრამმები, რომლებიც მრავალი გზით ცდილობდნენ მომხმარებლისთვის როგორც პროგრამული, ასევე ფინანსური ზარალის მიყენებას.

როგორც შედეგები ცხადყოფს, აუცილებელია გაიზარდოს მობილური მოყწობილობების უსაფრთხოების დონე. არსებობს რამოდენიმე საშუალება, რითაც შეგვიძლია დავიცვათ მობილური ტელეფონები მოსალოდნელი საფრთხისგან. ზოგიერთი მობილური ტელეფონის ოპერაციულ სისტემაში ინტეგრირებულია უსაფრთხოებაზე პასუხისმგებელი პროგრამული უზრუნველყოფა.

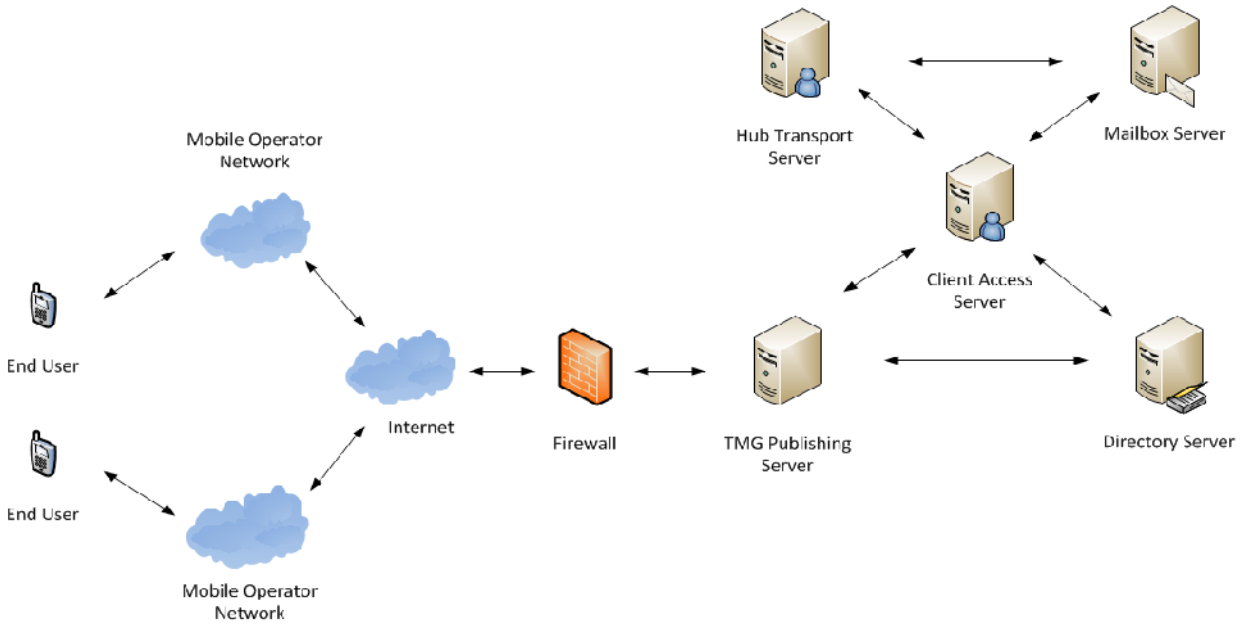
უპირველეს ყოვლისა ვსაზღვრავთ უსაფრთხოების პოლიტიკებს, რომლებიც უნდა გავრცელდეს მობილურ მოწყობილობებზე. თავიდანვე ვსვამთ ამოცანას, თუ რა დონის უსაფრთხოება უნდა გატარდეს:

	დაბალი უსაფრთხოების დონე	საშუალო უსაფრთხოების დონე	მაღალი უსაფრთხოების დონე
PIN ან პაროლის დაყენება	√	√	√
ავტომატური ბლოკირების დრო	√	√	√
არასწორი პაროლის შეყვანის მცდელობა	x	√	√
პაროლის ამოწურვის დრო	x	√	√
წერილზე მიმაგრებული ფაილის ჩამოტვირთვის უფლება	x	√	√
წერილის ზომა	x	√	√
პროგრამების მართვა	x	x	√
დაუდასტურებელი პროგრამების გამოყენება	x	x	√
მოწყობილობების ფუნქციის გამოყენება	x	x	√
მობილური მოწყობილობის დაშიფვრა	x	x	√
მობილური მოწყობილობის სანახი ბარათის დაშიფვრა	x	x	√
მხოლოდ ავტორიზებული მოწყობილობების გამოყენება	x	x	√

ნახ.1 უსაფრთხოების დონეები მობილური მოწყობილობებისთვის

როგორც მოცემული ცხრილიდანაც ჩანს, შემუშავებულ იქნა დაცვის სამი სხვადასხვა მოდელი, რომლის განსახორციელებლადაც ჩვენს შემთხვევაში გამოვიყენებთ Exchange ActiveSync-ს. ეს არის სინქრონიზაციის პროტოკოლი, რომელიც მომხმარებელს აძლევს საშუალებას, მობილური მოწყობილობების საშუალებით მოახდინონ Exchange Server საფოსტო ყუთის სინქრონიზაცია, რომელიც ელექტრონულ წერილებთან ერთად შეიცავს კალენდარს, კონტაქტებს და სხვა კომპონენტებს. ქვემოთ არის იმ მობილურ მოწყობილობათა ოპერაციული სისტემების ჩამონათვალი, რომლებიც თავსებადია Exchange ActiveSync -თან: Windows mobile, Symbian, Android, Apple, Palm , Blackberry.

Windows mobile მქონე მობილურებს აქვს იმ პოლისების სრული მხარდაჭერა, რომელსაც გვთავაზობს Exchange ActiveSync. ქვემოთ ნაჩვენებია Exchange Activesync-ის სქემა, თუ როგორ ხდება კომუნიკაცია მობილურ მოწყობილობებს შორის.



ნახ.2. Exchange Activesync-ის არქიტექტურა

წინამორბედი ვერსიებისგან განსხვავებით, Exchange Server 2010 Activesync-ში მოხდა ფუნქციების დამატება და ასევე არსებულის გაუმჯობესება. მაგალითად, HTML შეტყობინებების მხარდაჭერა, გაუმჯობესდა შეტყობინების სწრაფად მოძიების ფუნქცია, მთლიანი მიმოწერის სინქრონიზაცია, დავალებების სინქრონიზაცია, ასევე დაიხვეწა მობილური მოწყობილობის უსაფრთხოება პაროლის პოლისების საშუალებით და აშ.

ახალი უსაფრთხოების ფუნქციები მობილურ მოწყობილობების ეფექტური მართვის საშუალებას აძლევს სისტემის ადმინისტრატორებს. ამ პროცესში კი დიდ როლს ასრულებენ უსაფრთხოების (პაროლის გამოყენება, რაოდენობა არასწორი პაროლის შეყვანის, მობილური მოწყობილობის ავტომატური დაბლოკვა, მობილური მოწყობილობის დაშიფვრა, მხოლოდ ჩიპის დაშიფვრა და სხვა), შიგა მოწყობილობების (მართვა Bluetooth, Wi-Fi, Video Camera, Infrared, ჩიპის გამოყენება და აშ), საფოსტო ყუთის (შეტყობინების ზომის მართვა, Attachment -ის ჩამოტვირთვის შესაძლებლობა და სხვა) და მოწყობილობის პროგრამების პოლისები (ბროუზერის მართვა, არასერთიფიცირებული პროგრამების დაყენება, დაბლოკილი პროგრამების მართვა და სხვა) რაც მოქნილს ხდის სისტემის მართვას.

Exchange ActiveSync-ს აქვს მნიშვნელოვანი ფუნქცია ActiveSync Remote Wipe, რომელიც შლის მონაცემებს მოწყობილობიდან. გამოყენებითი პროგრამები რჩება სისტემაში, მხოლოდ მონაცემები იშლება. Exchange Management Console შეგვიძლია გამოვიყენოთ მოწყობილობის გასასუფთავებლად. ეს კი კეთდება ადმინისტრატორის მიერ მას შემდეგ, რაც განაცხადებენ რომ მოწყობილობა არის დაკარგული. მოწყობილობის გასუფთავება იწყება ხელახალი სინქრონიზაციის დროს.

ჩვენ შეგვიძლია დავაკონფიგურიროთ Exchange ActiveSync რომ გამოვიყენოთ Secure Sockets Layer (SSL) კავშირის დაშიფრვისთვის, Exchange server-ს და მობილურ მოწყობილობას შორის. სერთიფიკატზე დაფუძნებული აუტენტიფიკაცია მუშაობს self-signed სერტიფიკატებთან, PKI-ის სერთიფიკატებთან და ასევე third-party სერთიფიკატთან. დახურული გასაღები და სერთიფიკატი კლიენტის აუტენტიფიკაციისათვის არის შენახული მობილური ტელეფონის მოწყობილობაში. თუ არაავტორიზირებული მოხმარებელი შეეცდება გვერდი

აუაროს მობილური ტელეფონის პაროლს, მთლიანი მონაცემები იქნება წაშლილი (თავისთავად სერთიფიკატი და დახურული გასაღებიც).

ზემოაღნიშნული სერვისის საშუალებით, მთლიანობაში ვიღებთ შემდეგ შედეგს: მომხმარებლები არიან მუდამ ინფორმირებულნი თანამშრომლებთან, კლიენტებთან ან ბიზნეს პარტნიორებთან. ეს მათ დროული რეაგირების საშუალებას მისცემს. უპირატესობას აძლევს მომხმარებლებს იყვნენ მუდმივ კავშირზე, როცა შორს არიან თავიანთ სამსახურებიდან. ეძლევათ შეტყობინებების მიმოცვლის მოქნილი სისტემის გამოყენების საშუალება. პოლისების ეფექტურად გამოყენების საშუალებით იზარდება უსაფრთხოების დონე. ასევე არასასურველი მობილური მოწყობილობების შიგა კომპონენტების გათიშვის ხარჯზე, გაცილებით მეტი ენერგია რჩება მობილურ მოწყობილობას სამუშაოდ.

3. დასკვნა

მობილურ მოწყობილობებზე ინფორმაციის დაკარგვის თავიდან აცილების ერთ-ერთი გზა არის უსაფრთხოების პოლიტიკის მართებულად გატარება და შემდგომში მისი რეალიზება. ეს კი საჭიროა, რათა დავიცვათ ჩვენი ორგანიზაციის მომხმარებლების ინფორმაცია.

ლიტერატურა:

1. http://ilocalmobile.com/
2. http://ezinearticles.com/?Smartphone-Security:-Today-and-Tomorrow&id=6189672
3. http://technet.microsoft.com/en-us/library/aa998357.aspx
4. http://www.ehow.com/how_5702297_protect-smartphone-malware-attacks.html
5. http://us.norton.com/security_response/threatexplorer/index.jsp
6. http://www.nyu.edu/its/connect/w11/mobilesecurity-print.html
7. http://www.isaserver.org/tutorials/publishing-exchange-2007-owa-exchange-activesync-rpchttp-using-2006-isa-firewall-part1.html
8. http://technet.microsoft.com/en-us/library/bb232162.aspx

INFORMATION SECURITY SYSTEMS

Oboladze Konstantine
Georgian Technical University

Summary

This article is about information security systems for mobile devices. It describes different methods of improving security level. An article also reviews specific cases and offers their solutions.

СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Оболадзе К.
Грузинский Технический Университет

Резюме

Данная работа охватывает системы информационной безопасности для мобильных устроиств. Приведены разработанные методы для повышения уровня безопасности, а также рассмотрены конкретные задачи и примеры их решения.