Ванчо КЕНКОВ
Тони НАУМОВСКИ

УДК: 007:004.056

БЕЗБЕДНОСТА НА ИНФОРМАЦИИТЕ И ИНФОРМАЦИСКИТЕ СИСТЕМИ КАКО ПРЕДИЗВИК

Кратка содржина

Во трудот авторите ја истакнуваат исклучително важната улога на безбедноста на информациите и информациските системи. Денес, благодарение на масовната компјутеризација и примена на новите информациски технологии, информациите и информациските системи станаа достапни, ранливи и подложни на закани и напади. Оттука, државите самостојно или во рамките на колективните системи за безбедност развиваат систем на безбедност на информациите со потребно ниво на доверливост, интегритет и достапност на информациите.

Клучни зборови: *БЕЗБЕДНОСТ, ИНФОРМАЦИСКА БЕЗБЕДНОСТ, ИНФОРМАЦИСКИ СИСТЕМИ, ИНФОРМАЦИСКА СИГУРНОСТ, ЗАШТИТА НА ИНФОРМАЦИСКАТА СТРУКТУРА, САЈБЕР-ОДБРАНА*

Вовед

Технолошката револуција во областа на информациските и комуникациските системи услови промени во поглед на светот на почетокот на третиот милениум. Масовната компјутеризација и примена на новите информациски технологии доведоа до огромен напредок во сферата на масовни медии, бизнисот, индустриското производство, научните истражувања, образование, но и, за жал, и во војувањето.

Употребата на информациските технологии (IT) драстично го смени начинот на функционирање на општествата. Сè поголема е зависноста од употребата на и-мејл, интернетот и мрежно поврзување на владините институции кои сè повеќе користат информациски технологии. Во денешно време интернетот овозможи меѓусебно поврзување на милиони компјутерски мрежи и нивна меѓусебна комуникација и размена на информации. Сè поголемата примена на електронската трансмисија на податоците и употребата на видеотелеконференцијата како начин на комуникација и размена на податоци и доставувањето на информациите во реално време стана начин на секојдневно комуницирање, што ја зголеми вулнерабилноста на таквите системи.

Основи на информацискатa безбедност

Во денешни услови, протокот на информацијата е толку обемен и постојан што често информацијата може да биде преземена и обработена до разбирлив формат, врз чија основа може да се преземе некоја активност (Фридман Л., 2009). Нападот на системите базирани на информациските технологии може да предизвика оштетување на системот и губење информации, а како последица на сè поголемата вулнерабилност на системите поврзани во мрежи. Сето тоа ја зголеми претпазливоста и потребата од поголема информациска безбедност и имплементација на информацискатa безбедност како важен сегмент на националната безбедност. Под информациска безбедност се подразбира заштита на информациите и информациските системи од неовластен пристап, искористување, обелоденување, прекин, модификација, проучување, испитување, снимање или уништување (http://en.wikipedia). За да се разбере информацискатa безбедност, неопходно е да се објасни информацискиот систем и од кој елементи се состои. Имено, информацискиот систем е многу повеќе од компјутерски хардвер, тој е комплексен сет на софтвер, хардвер, податоци, луѓе и процедури неопходни да ја користат информацијата и ресурсите во организацијата (војска, полиција или некоја друга владина институција или, пак, организација во приватниот сектор). Информациите се јавуваат во повеќе форми: испечатени или напишани на хартија, запишани во електронска форма (компјутер, хард-диск, ЦД), испратена преку пошта или електронски врски, кажани во разговори (директно или преку средство за комуникација - телефон). Информацискатa безбедност ја штити информацијата од низа закани со цел да се обезбеди непрекинатост на информацсискиот систем. За постигнување соодветно ниво на безбедност е потребно градење систем на информациска безбедност кој ќе обезбеди **доверливост, интегритет и достапност** на информацискатa инфраструктура, соодветно чување, обработка и пренос на податоците независно од нивната форма - електронска, печатена или некоја друга форма. Тоа ќе се постигне со примена на соодветни политики, едукација и тренинг на персоналот, зголемување на свесноста за ова прашање, како и примена на соодветни технологии. Доверливоста на информацијата се однесува на достапноста до неа само за лицата кои се овластени да имаат пристап до нив, интегритетот обезбедува точност на информациите во однос на методите на нивата обработка, додека достапноста ќе обезбеди непречен пристап до информацијата на оние за кои е наменета, секогаш кога ќе биде тоа потребно.

Да се зачува доверливоста, интегритетот и достапноста на пренесената информација, претставува вистински предизвик, со оглед на тоа што нападот на информациските системи станува сè полесно – постојат книги кои на многу едноставен начин опишуваат како да се направи тоа. Треба да се има предвид дека не е возможно да се постигне апсолутна информациска безбедност, бидејќи тоа е процес, а не цел (Withman E. M., Mattord J. H., 2011). Се доведуваме во ситуација релацијата помеѓу информацискатa безбедност и нападите на IT-системите да се сведува на играта на мачка и глушец. Затоа најдобра безбедност на информациите се постигнува со примена и имплементација на најновите трендови во оваа област.

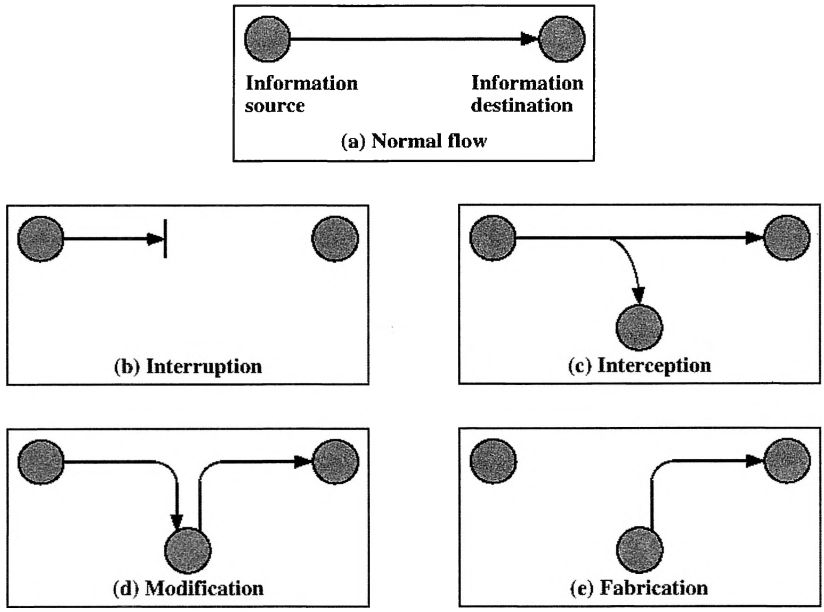
Покрај примената на соодветни техники за одбрана, добро обучениот персонал ќе придонесе во решавањето на многу безбедносни проблеми, што претставува многу комплексна област. Може да се издвојат три основни типа информациска безбедност: компјутерска безбедност, безбедноста на мрежи и интернет-безбедност. Компјутерската безбедност претставува збир на мерки и постапки за заштита на податоците од можен напад на хакери, безбедноста на мрежи се однесува на заштита на информациите при нивниот пренос и интернет-безбедноста се однесува на заштита на информациите во меѓусебно поврзаните мрежи. Постојат три аспекти на информацискатa безбедност: **безбедносен напад, безбедносен механизам и безбедносен сервис.**

- Нападот претставува акција (активна или пасивна), која ја компромитира безбедноста на информацијата.
- Безбедносниот механизам е систем кој е дизајниран да ја детектира, спречи или да ја „покрие“ опасноста од безбедносен напад.
- Безбедносен сервис претставува сервис кој ја подобрува безбедноста на податоците при нивниот пренос. Тие користат еден или повеќе безбедносни механизми.

Безбедноста на информациските системи е нарушена од заканите и нападите врз информацискатa инфраструктура. Притоа, треба да се има предвид дека постои постојана опасност од нарушување на безбедноста, при што нападот претставува удар врз системот на безбедност во насока на нарушување на безбедносната политика и онеспособување на функционирањето на информацискиот систем.

Разликуваме неколку основни вида закани од можните напади врз информациските системи, прикажани на Слика 1:

- Во услови на непостоење опасност од напад, информацијата има нормален тек со што се задоволени безбедносните барања: доверливост, интегритет и достапност, Слика 1-a.
- Прекин (Interruption) - ова претставува напад на достапноста на информацијата, а како резултат на физички прекин на медиумот за пренос или прекин на сообраќајот, Слика 1-b.
- Следење (Interception) - ова претставува напад на доверливоста на информацијата, а како резултат на прислушување на медиумот за пренос, Слика 1-c.
- Промена (Modification) - ова претставува напад на интегритетот на информацијата, а како резултат на упадот во медиумот за пренос на информацијата пред таа да дојде до крајната дестинација, Слика 1-d.
- Измислена информација (Fabrication) - ова претставува напад на автентичноста на информацијата, а како резултат на креирање информација од нелегитимни групи, Слика 1-e.



Слика 1. Безбедносни предизвици/напади

Постои и друга класификација на нападите според која тие можат да бидат пасивни и активни. Имено, пасивниот напад претставува обид да се преземе и искористи информацијата од информацискиот систем, при што не се нанесува штета на информацискатa инфраструктура. Кај активниот напад имаме ситуација кога се менува содржината на пораката и постои обид да се менува или влијае на операциите во информацискиот систем.

Информациска безбедност, информациска сигурност или сајбер-одбрана

Секоја земја, самостојно или во рамките на колективните системи за безбедност, развива систем на безбедност на информациите со потребно ниво на доверливост, интегритет и достапност на информациите.

Со цел заштита на системите на база на информациските технологии, постојат безбедносни политики чија имплементација зависи од безбедносните сервиси и безбедните механизми што ги користат тие сервиси, како што се, на пример, енкрипцијата и криптографските протоколи и техники. Согласно со тоа, постигнувањето соодветен степен на безбедност на информациите во електронско општество бара низа техники, вештини и постапки. Безбедноста на информациите покрај заштита на информацијата од директен напад, треба да обезбеди безбедност на информацијата и комуникациско-информацискатa инфраструктура и од природни непогоди, катастрофи и од појавата на човечка грешка.

Темпото на технолошките промени и зголемувањето на зависноста од компјутерската технологија претставува императив за безбедноста на информациите. Потпирањето на општествата на сè поголемата компјутеризација и фактот дека комуникациско-информациските системи се многу критична инфраструктура, евидентно е дека тоа претставува безбедносен проблем. Ако технологијата им помага на државите да воспостават подобра одбрана, исто така, на потенцијалните непријатели им помага да развијат способности за напад на нивните комуникациско-информациски системи. Најчести закани за безбедноста на информациите се луѓето и нивната недоволна свесност за безбедносните аспекти на информациите, сè поголемата компјутеризација на сите процеси во државите и нивно вмрежување, интернетот и електронската пошта, нападот од хакери и вируси, тероризмот. Сè понагласени се размислувањата дека војувањето, по сè изгледа, ќе премине во сајбер-просторот. Реализацијата на потенцијалната војна во сајбер-просторот ќе доведе до формирање нови организации, концепти и елементи на конфликти, кои се паралелни, но, сепак, различни од конвенционалните начини на војување (Џон Бејлис, Џејмс Вирц, Колин Гре и Елиот Коен, 2009). Сето тоа придонесува за комплексноста на предизвикот, а како резултат на технолошката експанзија. Сајбер-просторот претставува глобален домен во областа на информациите и се состои од независна мрежа на информациски системи и инфраструктура, вклучувајќи интернет, телекомуникациски и компјутерски мрежи (Kissel R.(ed), 2011). Со зголемување на зависноста од информатичката технологија, сите државни витални инфраструктури се ранливи на некој вид надворешен напад. Дури и ако експертите не се согласуваат за степенот и природата на заканата, државите, сепак, треба да усвојат мерки за зајакнување на заштитата на информациските системи. Подигањето на свеста и поттикнувањето на обуката во областа на безбедноста на информациите и заштитата на инфраструктурата ќе биде исклучително корисно. Тоа треба да вклучува тесна соработка изразена преку изведување заеднички вежби преку кои ќе се врши симулација и моделирање способност да се разбере влијанието на можен напад врз меѓусебно поврзаната и меѓусебно зависната информациска инфраструктура. Тоа ќе придонесе за развој на нови можности за детекција и идентификација на можните негативни импликации врз информацискатa инфраструктура. Безбедноста на информациите е главен императив на информацискатa безбедност (Information Security), информацискатa сигурност (Information Assurance) и сајбер-одбраната (Cyber Defence), или како и да ја наречеме оваа област која се занимава со сè поголемото нарушување на доверливоста, достапноста и интегритетот на информациите. Сите овие називи меѓусебно се преклопуваат и делат еден заеднички предизвик, безбедност на информациите. Според речникот на клучни термини од информациска безбедност (Glossary of Key Information Security Terms, Kissel R.(ed),2011), информацискатa безбедност претставува заштита на информациите и информациските системи од неовластен пристап, употреба, откривање, нарушување, модификација или уништување, со цел да се обезбеди доверливост, достапност и интегритет. Според истиот извор, информацискатa сигурност опфаќа мерки и постапки за одбрана и заштита на информациите и информациските системи преку

обезбедување нивна достапност, интегритет, автентичност, доверливост. Овие мерки вклучуваат постојаност на функционирањето на информациските системи, преку обезбедување заштита, детекција и способности за реакција на можни напади на информацискатa инфраструктура. Сајбер-одбраната, пак, претставува способност за заштита и одбрана на сајбер-просторот од можни сајбер-напади. Сајбер-нападот претставува напад на сајбер-просторот заради негово попречување, оневозможување, уништување и контролирање на компјутерската инфраструктура или уништување на интегритетот на податоците и информациите или нивно крадење. Сите посочени термини имаат повеќе сличности отколку разлики во однос на начинот на перцепција на безбедноста на информациите и информациските системи. Но, сепак, постојат настојувања за нивно претставување како посебни дисциплини. Имено, информацискатa безбедност се претставува како подмножество на информацискатa сигурност. Исто така, информацискатa сигурност се претставува како подмножество на сајбер-одбраната, односно сајбер-безбедноста и обратно. Можноста од забуна произлегува од сличностите и фактот дека сајбер-безбедноста е релативно нова дисциплина.(Withman E. M., Mattord J. H., 2011). Според тоа, се настојува да се прифати мислењето дека сајбер-одбраната го опфаќа само сајбер-просторот, или дека сајбер-одбраната, всушност, е информацискатa сигурност плус безбедноста на мрежите. Но, како и да е, зголемувањето на заканата од нападите врз безбедноста на информациите ги натера владите да ги земат предвид и ризиците од таквите напади на нивните комуникациско-информациски системи и другата критична инфраструктура. Исто така, се зголеми и вниманието во однос на вклучувањето на државите во информацискoто војување и можноста од колапс на комуникацискатa инфраструктура доколку таа не се брани (Pindar J., Rigelsford J., 2011). Во таа насока, покрај националниот предизвик за заштита на информациите, заштитата на информацискиот систем на НАТО претставува интегрален дел во функционирањето на Алијансата. По случувањата во Естонија во мај и април 2007 година, кога беше нападнатa информацискатa инфраструктура на земјата, НАТО започна со континуиран развој и подобрување на заштитата на своите комуникациски и информациски системи од напади и неовластен пристап. Алијансата, исто така, ги насочи своите активности во поддршка на индивидуалните напори за заштита на информацискатa инфраструктура на секоја земја-членка.

На самитот на НАТО во Лисабон во 2010 година, сајбер- одбраната беше претставена како еден од најважните предизвици на Алијансата во иднина. Посебно беше истакнатa важноста од заштита на информацискатa и комуникацискатa инфраструктура на НАТО.

Квалитетот на цивилните информациски системи е толку добар што ги користат и безбедносните структури (војска и полиција), при што има ситуација информацискиот сообраќај на Пентагон да се потпира 95% на комерцијалните телекомуникации (Фридман Л., 2009). Повеќето експерти сметаат дека комерцијалните информациски системи сега се повеќе подложни на надворешните напади, оттука од суштинско значење е да се поттикне соработка помеѓу воениот и цивилниот сектор во областа на заштита на инфраструктурата и информациските

системи, бидејќи тие споделуваат заедничките цели за обезбедување на безбедноста и сигурноста на информациските системи. Се разбира дека таа соработка треба да има свои граници во однос на заштита на класифицирани и тајни информации во безбедносниот сектор или комерцијални и конкурентни чувствителни информации во приватниот, односно цивилниот сектор. Присутна е констатацијата дека преку таа соработка полесно се идентификуваат ризикот и слабите точки на информацискиот систем, што иницира развој на соодветни планови и технологии во насока на спречување и елиминирање на опасностите за комуникациско-информацискиот систем. Со оглед на степенот на ерозија на бариерите на цивилните и воените мрежи, може да се претпостави дека офанзивните и дефанзивните операции ќе имаат многу заеднички карактеристики, во зависност од тоа дали активностите се насочени против ривалските корпорации, групи вмешани во меѓународен криминал или кон безбедносните институции на државата. Исто така, со поголемата употреба на комерцијалните решенија за воени потреби, се зголеми и ризикот од напад на вируси. Од друга страна, пак, сè понагласена е потребата од зачувување на најчувствителниот проток на информации, како и клучните командни и контролни односи во одделни мрежи (Фридман Л., 2009). Тоа е потребно бидејќи нападите на информациите и информациските системи е комплетно непредвидливо. Потребно е појасно разбирање на новите закани во ерата на информации во однос на актерите, мотивите и способностите. Можеби напредните западни држави не се земјите кои се под постојана закана од информациски напади, туку оние земји кои сè повеќе стануваат зависни од информацискатa технологија, но сè уште не ги развиле доволно капацитетите за заштита на информацискатa инфраструктура (Фридман Л., 2009). Постоењето соодветни капацитети и способности за заштита на информациските системи и инфраструктура претставува вистински предизвик.

Заклучок

Безбедноста на информациите и информациските системи во технолошки сè поразвиениот свет е од примарна важност и веќе претставува висок приоритет на секоја држава. Опасноста од напади на информациските системи и, воопшто, на информацискатa инфраструктура е постојано присутна, со што се зголемува и веројатноста да се наруши достапноста, интегритетот, доверливоста или, пак, автентичноста на информацијата која се пренесува. За да се спречи сето ова, се користат безбедносни сервиси кои, користејќи повеќе безбедносни механизми, обезбедуваат заштита на информациите во системите базирани на информациските технологии. Од ден на ден, безбедноста на информациите станува сè покомплексна, а како резултат на сè поголемата технолошка експанзија и врз основа на сè понагласените размислувања дека војувањето ќе премине во сајбер-просторот. Веќе и не е толку важно како ќе се нарекува безбедноста на информациите и информациските системи, информациска безбедност, сигурност или сајбер-одбрана. Важно е да се развиваат и да се спроведуваат правилни безбедносни политики во

насока на зачувување на доверливоста, достапноста и интегритетот на информациите и информациските системи. Сепак, покрај настојувањата за постигнување поголема безбедност на информациските системи, ситуацијата е загрижувачка, а како резултат на сè поголемиот број напади на информациските системи и вклучувањето на државите во информациско војување.

Литература

Active Engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government in Lisbon, 19 Nov. 2010.

Alexander, B.J., Future War, Thomas Dunne Kooks, New York, 1999.

Џон Бејлис, Џејмс Вирц, Колин и Елиот Коен, Стратегија во современиот свет, НАМПРЕС, Скопје, 2009.

Ehlers J. V., Information Warfare and Information Security, NATO Parliamentary Assembly, Science and Technology Committee, 1999Diter Golman, Kompjuterska sigurnost, AD VERBUM, Skopje, 2010

Kissel R.(ed), Glossary of Key Information Security Terms, February 2011,

Pindar J., Rigelsford J., Cyber security and Information Assurance, The University of Sheffield, 2011.

Фридман Л., Револуцијата во стратешките работи, Магор, Скопје, 2009.

Withman E. M., Mattord J. H., Principles of Information Security Fourth Edition, Course Technology, Cengage Learning, Boston, 2011.

Szafranski R., A theory of information warfare: preparing 2020, Airpower Journal, Spring, 1995

http://en.wikipedia.org/wiki/Information_security

Vanco KENKOV
Toni NAUMOVSKI

INFORMATION AND INFORMATION SYSTEMS SECURITY AS A CHALLENGE

Summary

Security of information and information systems in current technology developed world is of prime importance and is already a high priority for every country. The danger of attacks on information systems and information infrastructure in general is constantly present, which increases the probability to disrupt the availability, integrity, confidentiality or authenticity of the information transmitted. In preventing all this, security services are being applied, that by using multiple security mechanisms can provide protection of information systems based on information technology. Day by day, information security is becoming more complex, as a result of increasing technological expansion and based on more anounced considerations that war will move into cyberspace. For not as important if is called information and information systems security, or information protection, or cyber defense, it is important to be developed and implemented the right security policies in order to preserve the confidentiality, integrity and availability of information and information systems. However, despite efforts to achieve greater security of information systems, the situation is worrying as a result of the increasing number of attacks on information systems and the involvement of states in information warfare.

Key words: *SECURITY, INFORMATION SYSTEMS, INFORMATION SECURITY, PROTECTION OF INFORMATION SYSTEMS, CYBER DEFENSE*