Steps to Success
Пътят към успеха

ИНФОРМАЦИОННА СИГУРНОСТ И ТЕХНОЛОГИИ ЗА ЗАЩИТА В IP МРЕЖИТЕ

Цветан Митов[1)]
Висше училище по телекомуникации и пощи

Резюме. В настоящата разработка са разгледани проблемите на информационната сигурност и технологиите за защита в IP мрежите, като са изследвани съществуващите заплахи за тях.
Keywords: security; information security; networks; systems; threats

В началото на XXI век информационните технологии навлязоха във всички сфери на обществения живот. Те предизвикаха глобална интеграция на информационното пространство на човечеството. В него се появиха нови средства на труда и нови обществени отношения. Това наложи ad hoc да се развие регулиращото тази материя законодателство, което се оказа сериозно предизвикателство за работещите в тази сфера специалисти и в частност – за заетите с нормативната регулация в областта на информационната сигурност и защитата на класифицираната информация.

С възникването на информационното общество и глобализацията на информационните технологии се създадоха условия и възможности за разкриване на държавни, ведомствени и корпоративни тайни чрез несанкциониран достъп на неупълномощени лица до данни и информация. За противодействие на нежелания достъп до информационните системи са разработени множес-тво методи за защита на информацията.

„Сигурност“ е едно от най-често употребяваните, но многозначни съвременни понятия. Сигурността е увлекателна тема, защото засяга фундаментални проблеми на оцеляването на нациите и държавите, може да бъде свързвана едновременно с високите етажи на международните отношения и практически с всеки от аспектите на вътрешната политика, притежава широко дискутирана публична страна и в същото време често е обвита в мистицизъм и секретност.

Информационна сигурност. Значение на информационната сигурност за сигурността и отбраната на държавата

Информационната сигурност е защитеност на държавата на стратегическо, оперативно и тактическо равнище от всякакви опити: да се нарушат неприкосновеността, достоверността, конфиденциалността, селективността и отказоустойчивостта на достъпа до информационните ѝ ресурси (сигнали,

данни, знания, култура) и инфраструктури; несанкционирано да се ползват, манипулират или разрушат тези ресурси; да се отслабят в каквато и да е степен или премахнат възможностите за създаване, събиране, разпространение, обработка, съхранение и ползване на информация от граждани, организации и органите за държавно управление; несанкционирано да се ползва, манипулира или разруши информационната ѝ инфраструктура; да се манипулира или разруши държавната система от правила, процедури и стандарти, регулиращи обществените отношения в информационното пространство; целенасочено да се дезинформират обществото или вземащите решения лица и структури.

Това схващане за информационната сигурност (Semerdzhiev, 2007) се използва най-често за формиране на държавна политика в информационната сфера, за усъвършенстване на нейното правно, методическо, научно-техническо и организационно гарантиране и за разработка на целеви програми в тази област. То е основа за стратегическо ръководство на националната сигурност във всички сфери на практическата ѝ реализация, а именно защита на националната сигурност; противодейс-твие на престъпността и опазване на обществения ред; организация, строителство и използване на въоръжени сили; подготовка на страната за отбрана; управление при бедствия, аварии и катастрофи. На тази основа се разработват концепции за водене на информационни операции и се формулират изискванията към системите от по-горно йерархично равнище, т.е. към системата за мениджмънт на националната сигурност и стратегическо ръководство на отбраната и въоръжените сили.

Заплахи за компютърните мрежи и информационните системи в съвременния свят

Уязвимост на ИС или мрежи е слабост в системата от мерки за сигурност или в контрола за тяхното изпълнение, които могат да доведат до компрометиране или да улеснят компрометирането на сигурността. Уязвимостта може да бъде пропуск или да се дължи на недостатъчно ефективен надзор, недобра комплектуваност и устойчивост на работата или на неефективна физическа защита. Уязвимостта може да бъде от техническо, програмно, технологично или процедурно естество. Наличието на уязвимост създава възможности за реализация на събития или действия, поставящи в опасност организацията (т.е. заплахи), в резултат на което могат да настъпят вреди.

Вреда в областта на ИС или мрежи е увреждане на интересите на техните потребители (или на интересите, които тя защитава), вредните последици от което не могат да бъдат елиминирани или смекчени само с последващи мерки. В зависимост от значимостта на интересите и сериозността на причинените вредни последици вредите са непоправими или изключително големи, трудно поправими или големи и ограничени.

Непоправими или изключително големи вреди са тези, при които е настъпило (или би могло да настъпи) цялостно или частично разрушаване на ИС или мрежата или е извършено непоправимо посегателство върху интересите на свързаните с тях потребители.

Трудно поправими или големи вреди са тези, при които е оказано (или би могло да се окаже) значително негативно въздействие върху ИС или мрежата (или върху

интересите на свързани с тях потребители), което не може да се компенсира без настъпване на вредни последици, или вредните последици могат да бъдат смекчени само със значителни последващи мерки.

Ограничени вреди са тези, при които е оказано (или би могло да се окаже) краткотрайно негативно въздействие върху ИС или мрежата (или върху интересите на свързани с тях потребители), което може да се компенсира без настъпване на вредни последици или вредните последици могат да бъдат смекчени с незначителни последващи мерки. Заплаха за ИС или мрежи могат да бъдат всички техни обекти (пасивни елементи, съдържащи или приемащи информация) и субекти (активни елементи – лице, процес или устройство, обменящи информация между обектите или внасящи изменения в състоянието на ИС или мрежата). Тези заплахи могат да се класифицират на четири йерархично подредени нива, всяко от които включва стоящото под него, както следва.

1 ниво: обхваща възможностите за водене на диалога в ИС или мрежи, изпълнение на ограничено множество задачи (програми), реализиращи предвидени функции по обработка на информация.

2 ниво: обхваща възможностите за създаване и изпълнение на собствени програми с нови функции по обработка на информация.

3 ниво: обхваща възможностите за управление функционирането на ИС или мрежа, с които се въздейства върху базовото ѝ програмно осигуряване и върху състава и конфигурацията на оборудването.

4 ниво: обхваща възможностите на лицата, заети с проектиране, разработка, внедряване, експлоатация и ремонт на ИС или мрежи, включително възможностите за включване на собствени програмни или технически средства с нови функции за обработка на информацията.

Особено опасни са действията на така наречени „обидени служители“ – настоящи и бивши, които са ръководени от желание да нанесат вреда на организацията, като например да повредят оборудването; да внедрят логическа бомба, която да разруши програми или данни; да въведат неверни данни; да променят данни и т.н.

Необходимо е да се следи при напускане на служители, запознати с порядките в организацията, правата им за достъп до информационните ресурси да бъдат анулирани или прекратени своевременно.

Заплахите, които идват от физическата среда, в която е разположена и работи една информационна система, се отличават с голямо разнообразие. На първо място, трябва да бъдат посочени нарушенията на инфраструктурата: аварии в електрозахранването; временна липса на връзка; пробив във водоснабдяването и пр.

Природните бедствия (пожари, наводнения, земетресения, урагани, ниско качество и сривове в електрозахранването) по статистически данни допринасят за 13% от загубите в информационните системи.

Модел на заплахите за сигурността в информационните системи и компютърните мрежи

Условно ще разглеждаме четири различни варианта на модела на заплахата, като са дефинирани и четири категории атаки срещу автоматизираните информационни системи или мрежи

Вариантите на модела са, както следва: трафикът протича нормално, без да има наличие на външно вмешателство или нерегламентирано подслушване; налице е прекъсване на нормалния трафик – едно от ценните (жизнените) качества на системата е разрушено или е невъзможно използването му. Прекъсването може да бъде причинено от най-различни неща, например проникване в глобалната среда за сигурност, довело до прекратяване на нормалния трафик; регистрирано е подслушване на трафика или пресрещане (прихващане) – едно неоторизирано действие дава достъп до системата. Подслушването може да се осъществява отдалечено, като чрез подходяща апаратура се прихваща излъчваният сигнал, моделира се и се привежда в удобен четящ вид. Подслушване може да се реализира и при непосредствен достъп до комуникационната система, било то до кабели, компютри, комутатори, сървъри и маршрутизатори; има модифициране на трафика. При този вариант, един път прихванало трафика, третото лице подправя трафика и го изпраща на крайния му потребител; изфабрикуван (подменен) е оригиналният трафик. При него има симулиране на трафик, като се подменят данните от изпращача, по този начин крайният потребител губи реална представа за истинския автор на получения трафик. Прихващането е пасивна атака, когато няма намеса в комуникационните канали. Единственото нещо, което се осъществява, е постоянно наблюдение на преминаващата информация, докато прекъсването, модифицирането и изфабрикуването са активни атаки, тъй като там се регистрира намеса от трети лица.

Типове атаки

Най-често използваните атаки срещу автоматизираните информационни системи и мрежи могат да се обобщят в седем категории: кражба на пароли – методи за получаване на други потребителски пароли; социален инженеринг – придобиване на информация, до която нямате достъп; грешки и черни врати (bugs and backdoors) – получаване (използване) на преимущества посредством използване на системни грешки; възможностите за автентификация – използване на дефектите (противоречивост и непълнота) на механизмите за автентикация; грешки (провали) в някои протоколи – протоколи с грешки в проектирането и реализацията; изтичане на информация – използване на системи, като системата за подписване (finger) или системата за именуване (DNS) за информация, необходима на администратора или необходима за функционирането на мрежата, но която може да се използва за мрежови атаки; отказ от обслужване – опити за лишаване на потребителите от услугите на тяхната компютърна система.

След разглеждане на засегнатите въпросите от настоящата разработка можем да обобщим следното. В нашето съвремие информационната сигурност е една от ключовите области на системата за национална сигурност, като тя е важна не само за отбраната на държавата, но и по отношение на социалната област. В условията на информационното общество на нея трябва да се обърне значително внимание, за да се обезпечи сигурността на обществото, като цяло. Сигурността е силно комплексно понятие. Тя не трябва да се разглежда само от гледна точка на даден аспект, на нея трябва да се гледа като на система от множество области, влияещи на държавата, обществото и конкретната личност. Ефективната защита на системата принуждава злосторниците да влагат такива усилия, ресурси и разходи за проникване, които ги принуждават да се откажат от намеренията си. И все пак трябва да се знае, че не съществува система за пълна защита.Човешкият фактор може да бъде най-опасната от всички уязвимости за една информационна система или мрежа.

NOTES/БЕЛЕЖКИ

1. Авторът е студент във Висшето училище по телекомуникации и пощи.

REFERENCES/ЛИТЕРАТУРА

Semerdzhiev, Tsv. (2002). *Natsionalna i mezhdunarodna sigurnost.* Sofia: Voenno izdatelstvo. [Семерджиев, Цв. (2002). *Национална и международна сигурност.* София: ВИ.]

Semerdzhiev, Tsv. (2007). *Sigurnost i zashtita na informatsiyata.* Sofia: Klasika i stil. [Семерджиев, Цв. (2007). *Сигурност и защита на информацията.* София: Класика и стил.]

Milev, P., Tsonev, I. & Hristov, Kr. (2006). *Informatsionni sistemi i sigurnost. Uchebnik za distantsionno obuchenie.* Shumen: Episkop Konstantin Preslavski. [Милев, П., Цонев, И. & Христов, Кр. (2006). *Информационни системи и сигурност. Учебник за дистанционно обучение.* Шумен: Епископ Константин Преславски.]

INFORMATION SECURITY AND PROTECTION TECHNOLOGIES IN IP NETWORKS

Abstract. This paper discusses issues of information security and protection technologies in IP networks and studies existing threats to them.

✉ **Mr. Tzvetan Mitov**
University of Telecommunications and Post
Sofia, Bulgaria
E-mail: c.mitov@abv.bg