

ОБЗОР, ИЗВОДИ И ПРЕПОРЪКИ

От кръгла маса на тема:

„СЪСТОЯНИЕ И ПРОБЛЕМИ НА СИГУРНОСТТА В КИБЕРПРОСТРАНСТВОТО НА БЪЛГАРИЯ”

28.09.2010 г.

организирана от:

*Съюза на офицерите от резерва „Атлантик” и Асоциацията на
комуникационните и информационните специалисти*

О.р. ген. м-р Стефан Димитров - откри кръглата маса и изнесе встъпително слово, в което накратко обрисова настоящите и бъдещи заплахи за обществото в кибернетичното пространство, както и различните решения прилагани от напредналите страни за защита на своето киберпространство.

Приветствие поднесоха:

- Заместник-министърът на МО - г-н Валентин Радев;
- Заместник-министърът на МВнР - г-н Милен Люцканов;
- Народният представител - г-н Красимир Минчев;
- Секретарят на съвета по сигурността в МС - ген. Румен Миланов;

Първи панел: „Кибер сигурност и гражданското общество”

Модератор: о.р. ген. м-р Стефан Димитров

1. Доц. д-р Златогор Минчев (ИИКТ-БАН) представи темата „Нови заплахи в киберпространството“, като запозна аудиторията с резултатите от европейския проект „Forward“, в който е направен анализ на бъдещите заплахи към кибернетичното пространство, в зависимост от неговото технологично и практично развитие, очертани са основните заплахи (мощно технологично развитие и човешкия фактор) и насоки на бъдещата работа (осъзнаване, обучение, превенция, контрол). Накратко проблемите са групирани в следните категории: (а) развитие на **паралелното ползване** на големи системи (свързано с разработването и прилагането на паралелни кодове и задачи, където една минимална грешка/нарушение води до големи поражения); (б) експонентно **нарастване на информационните потоци**; (в) развитие на **зловреден и измамнически софтуер** (резултат от сивата и престъпна икономика); (г) навлизане на **мобилните системи** (все още незащитени от атаки и информацията може лесно да се

порази); (д) бурно развитие на **социалните мрежи** (Facebook, Twitter, в т.ч. и чатове: Skype, ICQ), чрез които могат да се придобият лични данни, да се влезе в личния компютър, да се направят големи поражения и т.н.

Развитието на тези изследвания доц. Минчев очерта в рамките на нов европейски проект *SySSec* на мрежа от центрове по компетентност в областта на информационните технологии с акцент киберсигурност (в т.ч. с участие и на индустрията от най-високо ниво: Google, Symantec и др.), както и някои активности в НАТО свързани с мултинационалната програма на NC3A по киберсигурност и работната рамка на АСТ в това направление, целяща създаване на единна система по киберсигурност на НАТО.

2. Гл. инспектор Явор Колев (МВР - ГДБОП) темата „Организираната киберпрестъпност - заплаха за националната сигурност“, представи работата на сектора, работещ по организираната киберпрестъпност. Тенденциите в България - над 1 млн. точки за достъп в Интернет, до 40 % от населението на страната има достъп до киберпространството. Нормативната уредба не е конкретизирана все още. Работи се основно по Конвенцията за престъпления в киберпространството, приета от Съвета на Европа на 23.11.2001 г. Доставчиците на Интернет в страната са повече от 1000. Към момента няма ограничения или правила за тях - те само се регистрират и това позволява на много престъпници да извършват такава дейност и по този начин да контролират цялата информация на ползвателите, преминаваща през тях.

Представи накратко структурата на сектора и разказа за някои от реализациите. Една от от тях бе за източване на банкови сертификати на ползвачи електронно банкиране, осъществявано чрез заразяване на личното РС с троянски кон (Trojan.Pws.Sinowal) през мейл или от социална мрежа. След това, с ползването на „мулета“, намирани чрез обяви в Интернет, парите се източват и прехвърлят в нови сметки. Това е било осъществявано от руски престъпни групи.

За борба с такива престъпления е необходимо международно сътрудничество, обмен на информация за престъпленията и разработване на общоевропейски закони срещу този вид престъпления, които да се прилагат и от България.

3. О.р. ген. м-р Съби Събев (СОР Атлантик), Представи темата „*НАТО и киберсигурността*“. Маркира новата политика на НАТО след атаките на мрежите в Естония (2007) и Грузия (2008). Представи NCIRC и работата му по преодоляване на слабите места в мрежите на Алианса и достигане на пълните оперативни възможности. Изграждането на Център за подготовка в Естония (2008). Създаване на орган за управление по кибер отбраната - NCDMA. Поставен за обсъждане е и въпросът за разработване на Стратегия по киберотбраната.

Отбелязана бе работата по киберсигурност в страни членки на Алианса: USA (създадено е кибер командване и това е приоритетна национална задача); UK (създаден е център за безопасност на виртуалните операции); Италия (създадена е команда и контролна структура за противодействие); Германия (създаден е Департамент по информация и компютри, както и военна структура на активно действащи хакери за проникване в противникови информационни системи).

В България има определен национален координатор, приоритет на МО е изграждане на надеждна способност за киберзащита, но все още дейността в тази

посока е твърда бавна и не се получава подкрепа на ниво МС. Още няма разработена Национална стратегия по кибер сигурност и е необходимо изграждане на национална структура, отговаряща за реакция при кибер атаки към мрежите на държавните структури.

4. Г-н Александър Кирков (лаборатория по кибер сигурност към МВР) представи темата „Сигурност на електронните платежни инструменти и разплащания - особености на измами с банкови карти и интернет банкиране“. Банковата магнитна карта е по стандарт ISO 7811. Въведени мерки за сигурност - от сигурност на пластмасата (релефен номер на сметката и името на лидера на сметката), през код за достъп и криптографска защита на преноса на данните (стандарт PCI DSS), до въвеждане на правила за задържане на преводите до три дни при работа с POS (информацията се прехвърля от POS към банката обслужваща терминала в магазина, след това от нея към към банката обслужваща сметката на картата), в които може да се обжалва тегленето на пари от лидера на банковата карта. При теглене от банкомат са въведени по - дълги срокове - 35 дни за VISA и 45 за Master Card (според наредба на БНБ), в които преводите могат да се обжалват с аргументи от лидера на банковата карта.

Системата на защита непрекъснато се усъвършенства (въвждат се карти с микрочип), но и престъпниците непрекъснато търсят пробиви в системите за сигурност. Регистрирани са повече от 3 млрд. евро загуби от кражби в банковите системи.

5. Проф. Антоний Гълъбов (Нов Български Университет), социолог, представи едно изследване на тема „Електронно гражданство и ефективност на публичния контрол. Киберсигурност, достъп до информация и лично съдържание“. Разгледа няколко тези, които са пропагандирани като основни, но при изследването се доказва тяхната несъстоятелност: 1 теза - противопоставяне на сигурността със свободата на гражданите (разпространява се идеята, че анонимността в мрежата гарантира сигурност - точно там се получава най-големия пробив, анонимността е фалшива); 2 теза - правото на достъп до информация е исконно право на всеки (чрез социалните мрежи се осигурява достъп до много лични данни, което води до нарушаване на сигурността на отделния човек); 3 теза - електронното правителство не можеш да подкупиш, защото контактуваш с терминала и сървъра, които са неподкупни (забравя се, че техниката се обслужва от хора и те могат да извлекат цялата информация от нея или да я настроят така както решат); 4 теза - електронното гласуване е най-точното и вярно и има сигурност на вота (не се отчита възможността от управление на техниката и по този начин манипулирането на вота, не се отчита и неграмотността на голяма част от хората по отношение на съвременната техника и липсата на гражданска култура у най-младите и ползващи електронните мрежи); 5 теза - приравняват се технологични постижения с политически решения (много грешно решение, което води до загуба на реална гражданска позиция).

Дискусия по първи панел:

Издаване на инж. Станислав Видев (проектанско бюро ВителКом) по въпроса за техническата сигурност на мрежата, която е основа за киберсигурността. В света

управлението на Интернет е контролируемо, у нас няма нито система, нито регулация. След продажбата на БТК няма единна държавна политика за осигуряване защитени и надеждни комуникации на държавното управление. Частните мрежи не са осигурили управленска връзка с малките населени пунктове и тяхното управление.

Въпрос на проф. Бантутов: „Осигурена ли е еднаква сигурност от НАТО за силните и слабите страни-членки в Алианса?“

Отговори ген. Събев: „НАТО създава способност за колективна сигурност на всички в Алианса, но от своя страна всяка членка трябва да изгражда и укрепва своята сигурност.“

В дискусиата се включи и доц. Минчев, който поясни, че в момента няма унифицирана единна система за киберсигурност на НАТО, но обясни, че се работи активно по този проблем както в АСТ, така и на индустриално ниво чрез НСЗА и това ще залегне в новата Стратегия за сигурност на Алианса, която се очаква да бъде огласена през м. Ноември, 2010 г.

Въпрос на проф. Бантутов: „Създава ли НАТО възможност за провеждане на кибер атака срещу евентуални противници?“

Отговори отново ген. Събев: „В USA се регистрират повече от 200 х. атаки на час към всички мрежи на Пентагона, което показва изключителна активност на хакерите по целия свят към американските секрети. Отделни страни (USA, Германия, UK, Италия) развиват сили за активно действие срещу противника, но са необходими обсъждането и приемането на правни решения по този въпрос.“

Втори панел: „Кибер сигурност в държавните структури на Р. България“

Модератор: о.р. полк. инж. Иван Кьосев

1. Д-р инж. Чавдар Пенков (АКИС) представи „*Аспекти на защитата на служебната информация*“. Разгледан бе обхвата на служебната информация (класифицирана и неклассифицирана), нормативната база на Р. България и паралелно на НАТО и ЕС, заплахите (вътрешни и външни) за информацията при обмена ѝ по КИС, изисквания към сигурността на КИС и съвременни решения за сигурност на КИС без криптография и с ползване на криптографски решения.

2. Инж. Милена Христова (ДКСИ) направи доклад по киберсигурността в национален аспект. Все още липсват документи (не са разработени обща Стратегия по кибер сигурността и Единна политика като част от нея), няма и отговорни органи, които да работят в изграждането и прилагането на кибер сигурност. Необходимо е да се работи по: (а) разработване на Политики и норми; (б) избистряне на задачите към държавните органи; (в) създаване на принципи и препоръки; (г) създаване на Център за подготовка по проблемите на кибер сигурността; (д) създаване на Група за реагиране, преодоляване и възстановяване на мрежите след кибератаки; (е) подписване на Меморандум за разбирателство и взаимодействие между отделните страни.

3. Подполк. д-р Николай Стоянов (Институт по отбраната към МО) изнесе доклад „Кибератаките - новият инструмент в арсенала на нашата армия”. Направи обзор за състоянието както в НАТО, така и в нашата страна. Посочи определени примери за кибернетични атаки, с ползването на значително количество хакери от една страна. Цитира проекти на НАТО и ЕС по кибернетичната отбрана.

Развитие на изследванията на научните среди по проблемите на информационната сигурност обхващат широк спектър от проблеми, отнасящи се до създаване и защитата от кибернетични атаки, които обхващат организационни, програмни и технически методи. Създаден е Център за Управление и Реагиране при Компютърни Инциденти (ЦУРКИ), който е съвместим с NCIRC на НАТО и непосредствено изпълнява задачи по *защита, откриване, реакция и възстановяване* на аномалии или кибератаки срещу комуникационните и информационните системи на МО и БА. Планира се достигане на пълната функционалност на ЦУРКИ през 2012 г. Разработва се Меморандум за разбирателство между Република България и НАТО, за създаване на правната рамка за сътрудничество в областта на киберзащитата, обхващаш: (а) разширяване на националните възможности за киберзащита; (б) повишаване на оперативната съвместимост между Националния орган за киберзащита и този на НАТО (NCDMA); (в) подобряване на възможностите за предсказване, откриване и реагиране срещу кибератаки; (г) обмен на информация за киберзащита на реципрочна и балансирана основа.

4. Владимир Кожухаров (МВР), с тема „Криптографска сигурност на информацията”. Направено бе определение на криптографската сигурност. Посочени бяха криптографските алгоритми, ползвани в съвременните системи (симетрични-поточни и блокови и асиметрични). Подробно бе разгледан въпросът за криптографските механизми, какво представляват, какви са изискванията към тях и как се осигурява правилната им реализация. Посочен бе пътят на съвместно ползване (в Алианса) на криптографските продукти (SCIP). Разгледано бе състоянието и проблемите на криптографската сигурност у нас - проблеми в нормативната уредба, проблеми в производството у нас и вноса на криптографски продукти, проблеми от статута, работата и структурата на Органа по криптографска сигурност.

Дискусия по втори панел:

Изказване на инж. Иля Христов (АКИС): „Важно е да се разработят определения за кибернетичната сигурност, да не се допуска срив на системите. Да се определи, кога една мрежа е сигурна и кога не е.“

По темата взе отношение д-р Пенков: „Определения по кибернетичната сигурност има направени от НАТО и е по-добре да използваме вече направените определения, като ги включим в новоразработваните документи, след съответната адаптация.“

Полк. Петров (КИС-МО): „Има ли правни ограничения за свързаност на нашите мрежи с мрежи на други държави?“

Отговори д-р Пенков: „Свързването на защитени мрежи на две държави, зависи само от договореностите между двете държави. Когато става въпрос за натовски мрежи - изграждането, поддържането, развитието, защитата и обмена на информация се осъществява само от съответните специалните органи на НАТО. “

Владимир Кожухаров добави, че за защитената взаимосвързаност на натовските мрежи има разработени редица документи и продължава работата в тази насока (SCIP) и нашата страна трябва да се съобразява с тези документи при взаимодействие по линия на НАТО.

Инж. Иван Кьосев (АКИС): „Има ли национален алгоритъм за защита?“

Отговори Владимир Кожухаров: „За всяко разработвано у нас устройство се разработва различен национален алгоритъм за съответното ниво на класифицирана информация. “

Ген. Събев (Атлантик) направи предложение към правителствените органи:

„Нормативната ни база в областта на защитата на информация е от преди приемането ни в НАТО и ЕС. Трябва да се направи всичко възможно за хармонизирането ѝ, защото Република България е длъжна да изпълнява политиките, за които гласува в НАТО и ЕС“.

Полк. Петров (КИС-МО) предложи този въпрос да се реши на високо ниво и криптографските средства да се одобряват само от една комисия.

Заклучение

Д-р Чавдар Пенков направи обобщение на Кръглата маса от направените презентации, доклади и изказвания:

Киберпространството се развива непрекъснато. Развиват се и заплахите в киберпространството. Често се ползват такива понятия, като: хакери, киберсистеми, DDoS-атака /отказ от обслужване/, фишинг /мошеничество с банкови карти/, шипинг, кибертормоз и кибершантаж /над деца, родители, граждани, фирми, конкуренти, дисиденти, политически противници/, киберзащита, отражение на кибератаки, киберотбрана, кибер-противодействие, кибернастъпление, кибервойски, надпревара в кибервъоръжаването, киберсигурност, кибербезопасност и т.н.

За обществото заплахите в киберпространството можем да систематизираме така:

Действителност	Заплахи	Последствия
Развитие на паралелна работа; Развитие на паралелни кодове	Грешки в софтуера	Големи поражения в базите с данни
Банкови и финансови системи	Кражби на лични данни; Подправяне на банкови данни	Финансови загуби
Многократно увеличаване на информационните потоци	Интелектуални престъпления	Загуба на интелектуална собственост
Разработване на зловреден и измамен софтуер	Вируси, червеи, троянски коне, запущване и разрушаване на комуникациите	Кражба на информацията, промяната ѝ, подмяната ѝ или унищожаването ѝ
Развитие на социалните мрежи и чатове Facebook, Twitter, Skype, ICQ	Отворен достъп до ресурсите на личното РС	Кражба на лични данни, шантажи, угрози, заплахи, сексуално насилие, педофилство
Въвеждане на електронно обслужвано гражданство (електронно правителство), електронно гласуване	Изискване за свободен достъп до информация и осигуряване на сигурността ѝ	Кражба на лични данни, манипулиране на личните данни; при електронно гласуване - манипулиране на вота, грешки при въвеждането от незнание, грешки при обработката на вота от промени в софтуера и др.

На разпространението на заплахите помага и липсата на ефективно национално законодателство и правна рамка за контрол на операторите и развитието на социалното ползване на киберпространството.

За системите, работещи по **сигурността на страната**: заплахите са от запущване на комуникациите, разрушаването им, пробиви в защитата или неосъзнаване и неспазване на изискванията при прилагане на изискванията за сигурност на мрежите.

Не е извършено хармонизиране на националната регулаторна рамка с тази на НАТО и ЕС, разработена в последните години, които изискват всяка страна членка да има Център за реагиране на кибер атаки и Група за реагиране, отблъскване, преодоляване и възстановяване на пораженията от кибератаки.

От направените обсъждания се открие заключението, че е нужно на правителствено ниво да има отговорност, да се оцени важността на кибер проблемите и заплахите, за да се реализира държавното управление с разработването на Стратегия и Политики, създаването на необходимата организация и изграждането на работеща структура, с подходящо оборудване, съвременно обучение и всичко необходимо за постигане на национална кибернетична сигурност.

С изчерпване на дневния ред кръглата маса бе закрыта от инж. Кьосев.

Изготвил: Д-р инж. Чавдар Пенков

София, 03.10.2010 г.