

ИЗКАЗВАНЕ

На представител на Държавната комисия по сигурността на информацията - инж. Милена Христова по време на кръглата маса „Състояние и проблеми на сигурността в киберпространството на България” на 28.09.2010 г. в ЦВК, София.

Уважаеми дами и господа,

След навлизането и разпространението на информационните технологии в съвременното общество се налага да се предприемат все повече действия за предотвратяване на опитите за кибернетични атаки и да се ограничат възможностите за терористично влияние върху системите, свързани с националната сигурност на държавата. Както знаете, сигурността не е състояние, тя е процес и динамика.

Осигуряването на защитата на инфраструктурата на държавата, управлявана от компютърни системи като цяло е една от целите на киберзащитата в национален мащаб. Разрушителни биха били пораженията върху критични компоненти на инфраструктурата, като електроснабдяване, водоснабдяване, финансови пазари, компютърните системи на правителствени структури и структурите със стратегически производствени цели.

Известно е, какво се случи в Естония и Грузия вследствие на кибер атаките през 2007 и 2008 г. Анализът от тогава показва, че този род атаки са насочени главно към:

- „парализиране” на публичните и държавни информационни системи и мрежи;
- Блокиране на обществените дейности;
- „сриване” на комуникационно-информационните системи с цел блокиране дейностите на държавните институции и влияние върху общественото съзнание и психика.

Съвременната киберзащита е все още реактивна, търси се решение след възникване на заплахата, а съвременният анализ на заплахите и уязвимостите все още не е достатъчно автоматизиран.

Ето защо, националните дейности по киберсигурност следва да са насочени към формиране на единна политика за защита на компютърните мрежи и системи, важни за държавата. Защитата на компютърните мрежи и системи следва да е част от Стратегията за национална сигурност.

Противодействието на кибератаките се постига чрез прилагане на комплексни мерки по киберзащита и те трябва да се разглеждат в различен аспект-технически, правни и организационни, както и такива в областта на обучението и подготовката на специалисти в областта на киберсигурността.

В рамките на защитата на националната сигурност Република България изостава в тази област. Засега в нашата страна липсват изготвени и приети базисни документи, каквито има в НАТО и ЕС, няма ясно дефинирани и разписани отговорности на националните органи в областта на киберсигурността и защитата. Няма дори ясна дефиниция на понятието „киберсигурност”, а се разглежда като едно общо понятие.

Обхватът на държавната политика в областта на информационната сигурност е доста широк и съвместните усилия на различни държавни органи и структури, свързани с националната сигурност трябва да бъдат насочени в следните области:

1. Политики и доктрини за усъвършенстване на способностите на страната за защита от кибератаки;
2. Определяне и възлагане на задачи на различни държавни органи, правителствени и неправителствени организации в дейностите по киберсигурността;
3. Принципи и препоръки за формулиране на механизмите за обща координация и задълженията на организациите в областта на киберсигурността;
4. Създаване в Република България на Център за подготовка на специалисти в областта на киберсигурността и защитата.
5. Обучение и подготовка на специалисти в областта на киберсигурността, включващи:
 - предварителна оценка на риска от кибернетична атака и планиране на мерки за сигурност и защита;
 - възможности за откриване в реално време на действия за налични кибератаки.
 - възможности за действие срещу кибератаки;
 - процедури и мерки за надеждна защита;
 - възможности за намаляване последствията от кибератаките;
 - начини за предупреждение на ползвателите на компютърни системи за наличие на кибератаки;
 - управление на ситуацията;
 - общи стандарти и процедури за обучение
 - възстановяване на системата след кибератаки

6. Координация по органи и нива и определяне на водещи специалисти или звена в организациите;
7. Определяне на механизми за адекватни отговори на кибератаки
8. Установяване на сътрудничество с частния сектор;
9. Възможности на национални и международни органи, правителствени и неправителствени организации за помощ при кибернетични атаки и координация на общите усилия в тази област.

В редица европейски документи се посочва, че начинът на мислене в държавите-членки остава ограничен в рамките на интересите на националната сигурност и че по този начин се пренебрегва общата отговорност за защитата на обединените европейски интереси.

Ето защо, като пълноправен член на НАТО и ЕС Република България има своите ангажименти към общата политика за сигурност и защита, която включва елементи от съвместни действия в областта на киберсигурността и защитата.

ДКСИ със свое решение е определила точка за контакт за Република България към проекта на ЕС „Механизъм за известяване при инциденти в сигурността на мрежите.”

Експерти от ДКСИ участват в работата на междуведомствена работна група, сформирана с цел да подготви текста на документа „Меморандум за разбирателство относно сътрудничество в областта на киберсигурността между Органа за управление на киберзащита към НАТО (NATO CDMA) и Република България. Целта на този Меморандум за разбирателство е да формализира споделянето на информация за киберзащита, обмена на услуги за киберзащита и участието в свързани с тях дейности. Договарящите страни ще провеждат двустранни дейности и споделяне на информация, свързани с киберзащитата, с което да допринасят за общите цели за защита на техните съответни информационни мрежи.

Като приоритети в областта на киберзащитата следва да се посочат:

- Бърза реакция при кибератаки;
- Защита на идентичността;
- Тренировки и упражнение;
- Осигуряване на резервираност;
- Обмен на информация;
- Гъвкавост на мрежите и системите;
- Осигуряване на бюджет;
- Проучване и изследване на бъдещи заплахи;

- Международна сигурност.

Като средства за постигане на тези цели могат да бъдат посочени:

- Изграждане на подходяща инфраструктура;
- Тясно сътрудничество с индустрията;
- Провеждане на бързо разследване при инцидент;
- Намаляване времето за актуализация и обновяване.

Проведените днес тук, на тази кръгла маса дискусии и поставените множество въпроси дават индикация, че в областта на киберсигурността все повече се работи, но както всички отбелязаха се изискват още по-интензивни действия от страна на държавните институции, работещи в тази област от една страна, частния бизнес от друга и научните институти в БАН. Необходимо е изграждането на добро сътрудничество и координиране на усилията на всички в тази област.

Благодаря за вниманието!