ул. "Дякон Игнатий" № 9, София 1000
Република България
тел: (+359 2) 940 9771;
факс (+359 2) 988 5094

Киберзима 2011

Компютърно подпомагано учение по информационна сигурност

Накратко за ученето

На 7-ми декември 2011 година Министерството на транспорта, информационните технологии и съобщенията, подпомагано от Българската асоциация по моделиране и симулации "БУЛСИМ" се проведе първото в България компютърно подпомагано учение за държавната администрация с тематична област "информационна сигурност".

Компютърно подпомаганото учение "КИБЕРЗИМА 2011" беше открито и ръководено от Заместник министъра на транспорта, информационните технологии и съобщенията г-н Валери Борисов, и.д. Директор дирекция "Електронно управление" г-жа Цветанка Кирилова и Председателя на Управителния съвет на Българската асоциация по моделиране и симулации "БУЛСИМ" г-н Николай Томов.

Откриване на КПУ "Киберзима 2011" от Заместник-министър Валери Борисов

Основни участници в проекта за провеждане на компютърно подпомагано учение (КПУ)

"Киберзима 2011″ бяха:

» Министерство на транспорта, информационните технологии и съобщенията (МТИТС)

» ИА "Електронни съобщителни мрежи и информационни системи"

» ИА "Автомобилна администрация"

» ИА "Железопътна администрация"

» ГД "Гражданска въздухоплавателна администрация"

» ИА "Морска администрация"

» ИА "Проучване и поддържане на река Дунав"

» Национален център за действие при инциденти в информационната сигурност (CERT)

Българската асоциация по моделиране и симулации "БУЛСИМ" е организацията, която подпомогна МТИТС в планирането, подготовката, провеждането и анализа на учението. В допълнение, асоциацията даде своя принос и в следните дейности:

» Изготвяне на сценария за учението

» Консултиране при изграждане на физическата, хардуерната и комуникационната архитектура

» Изграждане на среда за моделиране и симулации на мрежата и инфраструктурата, нейния мониторинг, както и на настъпили инциденти в информационната сигурност

» Разработване на уеб-базирана информационна система за следене на общата оперативна картина

» Консултиране при анализа, оценката и извличането на поуки от учението.

Участници от I-во функционално ниво (лица взимащи решения) в действие

Основни цели на ученето

Проведеното компютърно подпомагано учение имаше за цел да тества някои специфични мерки, които трябва да бъдат предприети или процеси, които трябва да бъдат следвани при настъпване на инцидент в информационната сигурност. Тези мерки включваха сътрудничество и координация между звената на организацията, както и откриване на някои важни взаимозависимости, които не могат да бъдат доловени при стандартно провеждане на обучения. Основните цели за постигане в проекта бяха следните:

» Повишаване способностите на отговорните лица в МТИТС, изпълнителните агенции към него и на Националния център за действие при инциденти в информационната сигурност (CERT), за защита на националната критична информационна инфраструктура срещу киберзаплахи и настъпване на пробиви в информационната сигурност.

» Идентифициране на организационни и технически уязвимости в системата за управление на информационната сигурност, в процедурите и политиките за реагиране при настъпване на киберинциденти.

» Анализиране и прогнозиране на съвременните заплахи за информационната инфраструктура на министерството и изпълнителните агенции.

Участници от II-ро функционално ниво (технически експерти)

Общ сценарий

Сценарият на учението е разработен на базата на развитието на международна криза, възникнала поради рязко увеличаване на кибер-атаките срещу правителствени сайтове, системи на държавната администрация, както и срещу корпоративни организации от Европа и света.

В последните месеци се наблюдава активизиране в интернет на нова хакерска групировка The Cyberwolves (Кибервълците), които имат идея да обединят усилията си с други две хакерски групи – Anonymous и LulzSec, които са доста политически мотивирани. Последните двете групи обявиха, че ще си сътрудничат, за да осъществят най-масовата акция срещу световните правителства, като операцията е наречена Anti-Security ("Антисигурност"). Целта й е кражбата на всякаква класифицирана информация от различни правителствени органи по света и публикуването й в социалните мрежи.

В миркоблогинга Twitter е публикувано съобщение, че Anonymous и LulzSec ще допуснат сътрудничество с "Кибервълците" при условие, че последните докажат своите умения да крадат и да публикуват правителствена информация и документация, както и да "сриват" работата на правителствени системи в информационната инфраструктура на дадена държава. За да демонстрират нагледно своите способности, принадлежащите към групировката на "Кибервълците" хакери обявяват в няколко IRC канала и форуми, че в следващите няколко дни ще блокират работата на няколко правителствени сайта и ще откраднат информация от ключови информационни системи на определена държава от Югоизточна Европа, разбивайки компютърната сигурност на информационната инфраструктура.

Експерти от БАМиС "БУЛСИМ", извършващи контролирани хакерски атаки

На 7-ми декември масираната симулирана хакерска атака започна…

Събитията, които бяха проигравани на самото учение, се състояха от контролирани хакерски атаки върху следните симулирани елементи от информационната инфраструктура:

- » Уеб-базирани системи на МТИТС и изпълнителните агенции;
- » E-mail инфраструктурата;
- » Други системи и мрежови услуги.

Събитията бяха подбрани така, че да ангажират с отговорно действие всички йерархични звена в организациите – системни администратори, младши и старши експерти, ръководители на отдели, директори на дирекции, заместник министри и министър.

Всички те бяха запознати с основните моменти от сценария, но не и с разпределените във времето съобщения/инжекции за нарастване на обстановката, които постъпваха към тях. За да бъдат поставени участниците в по-близка до реалната среда на работа, бяха извършвани и контролирани промени по предварителния списък с инциденти.

Архитектура на ученето

Следвайки добрите практики, за целите на ефективното провеждане на компютърното учение всички участници бяха поставени в "изолирана" среда, ситуирани на една обща площ, разделена на съответните центрове, съгласно оперативната архитектура на ученето.

Всеки участник имаше определена роля и спрямо тази роля – достъп до съответната информация. Основните моменти от сценария бяха визуализирани с помощта на софтуерни продукти за моделирани и симулации на мрежи, хардуер и основни софтуерни приложения, като по този начин се подпомагаше взимането на решения от отговорните за това лица. Всяко действие и предприета стъпка от участниците, беше записвана и съхранявана за последващ анализ.

Цялата информация за протичане на ученето беше достъпна посредством система за представяне на общата оперативна картина. Тази информация беше архивирана за целите за анализи и извличане на поуки.

Резултати от ученето

Общоприето е мнението, че всяко едно проведено учение е само по себе си успех, защото всички участници научават по нещо ново и откриват възможности, както за своето развитие, така и за усъвършенстване на своята организацията в областта на информационната сигурност.

Допълнителни цели и дейности, проверени по време на учението бяха:

» Скорост на отговор и време за възстановяване;

» Процеси при взимане на решение;

» Споделяне на информация (вътре и извън организацията);

» Сътрудничество (вътре и извън организацията) за адресиране на възникнал проблем;

» Координиране на ресурсите, логистиката и способностите за поддръжка;

» Идентифициране на потенциални заплахи;

» Мерки за ответна реакция;

» Капацитета за сътрудничество, нивата на сътрудничество между различните звена, оперативността и използваемостта на комуникационните средства и информационните системи в случай на инциденти, способностите за обхващане на общата картина, оперативната готовност, нивото на достатъчност на властта, с която разполагат длъжностните лица, най-добри практики;

Чрез средствата на проведеното КПУ, участващите звена от различни сектори извлякоха следните ползи:

» Идентифицираха взаимозависимости, за които не са предполагали, че съществуват;

» Добиха опит, работейки заедно със служители на техните позиции, но от други звена;

» Споделиха добри процедурни практики;

» Провериха дали собствените им процедури работят добре на практика;

» Провериха информацията за контакт и каналите за комуникация в различните звена;

» Демонстрираха степен на подготвеност пред ръководители и наблюдаващи органи.

КИБЕРЗИМА 2011 донесе и ползи за висшите длъжностни лица, отговорни за реагиране при настъпване на инцидент. Обикновено тези лица нямат цялостно и детайлно виждане как индивидуалните отговорни служители и инфраструктурата на организацията ще се справят в случай на инцидент. Конкретно:

» Да наблюдават действията за преодоляване на инциденти на практика;

» Определяне степента на информационна сигурност;

» Идентифициране на слабостите в процедурите за отговор при инцидент;

» Поставяне като задача изготвянето на планове за действие за подобряване на процедурите;

» Оценка на подобренията.

Извършването на пробиви в информационната сигурност целеше да бъде проверена

готовността на експертния и ръководен персонал да извършват следните дейности:

» Да установяват наличието на инцидент

» Да извършват първично отработване на инцидента в най-кратки срокове, с цел да се предотврати последваща загуба на данни, или други необратими повреди в информационната система, както и за да се затвори пробив в системата, ако инцидентът е резултат от такъв

» Да извършат damage assesment, и да установят всички детайли на инцидента

» Да съставят план за възстановяване на поразената система към работещо състояние

» Да възстановят поразената система.

В настоящото КПУ, следвайки добрите практики, бяха включени повечето важни елементи за провеждане на компютърно подпомагани учения по информационна сигурност.