Управление на риска при компютърната обработка на резултатите от изборите

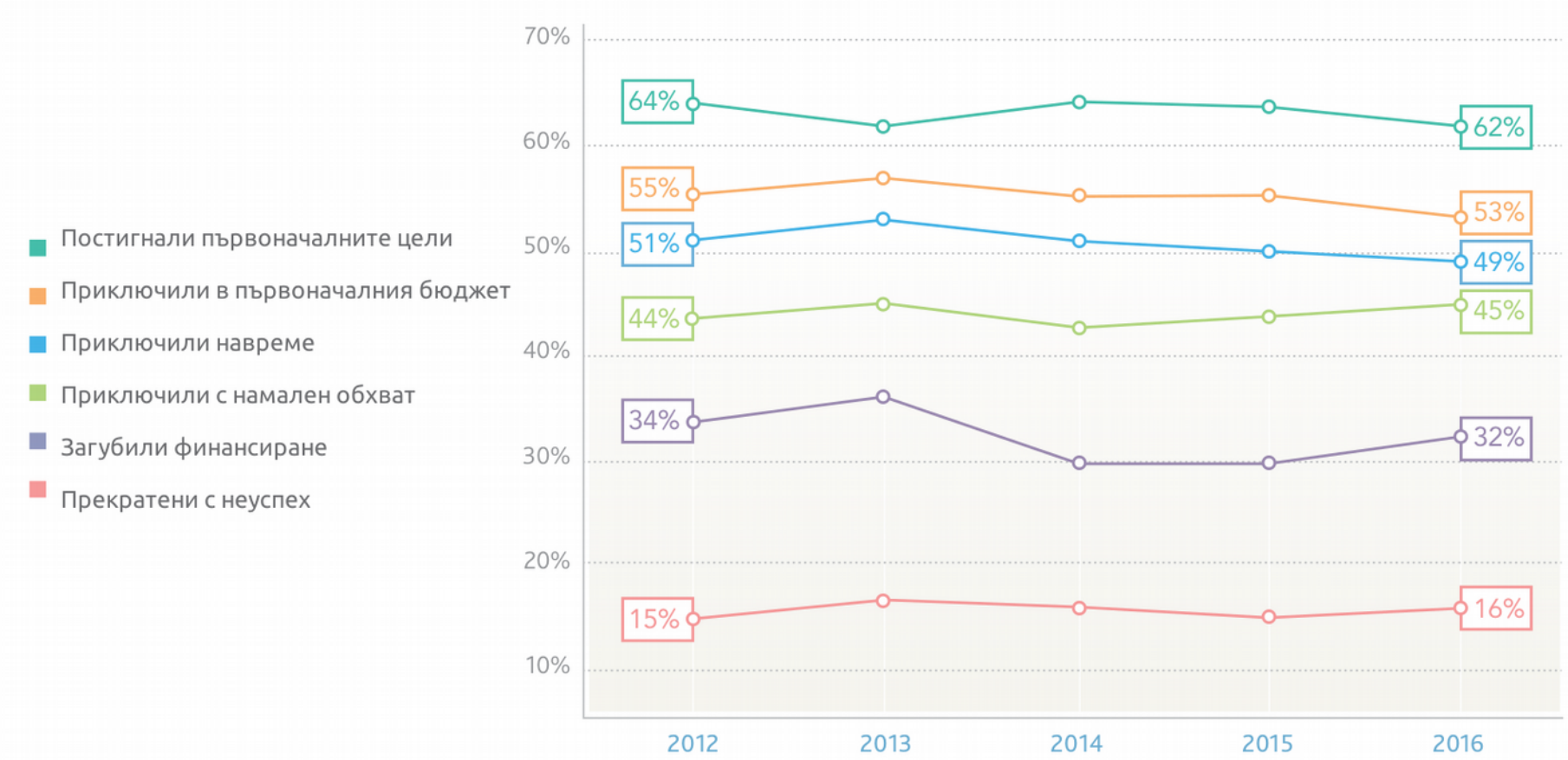
Александър СТАНЕВ
Илия ГОРАНОВ

БАИС, V НКИС
1-2 ноември 2016

Компютърната обработка като ИТ проект

- Класически пример за аутсорсинг на несвойствени (ИТ) дейности
- Изпълнителят на компютърната обработка е работен орган на избирателните комисии
- Управлението на промените е сложен, многостепенен процес
- Изпълнява се в изключително напрегнат времеви график
- Множество организационни дейности и съгласуване с външни фактори

ИТ проектите на практика



По данни на PMI,
Pulse of the profession 2016

Подход за управление на риска

Управлението на риска е постоянен процес, който протича по време на целия проект.

- Приемане на методика за управление на риска
- Идентифициране на възможните заплахи
- Анализ на риска
- Оценка на риска
- Прилагане на подходи за ограничаване на риска
- Контрол на изпълнението
- Мерки за ограничаване на последствията
- Превантивни действия

Групиране на рисковете

Категория	Описание
Управленски	Свързани с цялостната организация по управление на проекта
Финансови	Свързани с финансирането на дейностите
Ресурсни	Свързани с подбора на експерти
Външни	Свързани с трети страни, имащи отношение към дейностите по проекта
При клиента	Свързани с дейностите и особеностите на клиента
Технически	Свързани с техническата среда – хардуер, софтуер, комуникации

Степен на критичност на риска

- Определяне нивото на въздействие [1-4]
- Определяне на вероятността [1-3]
- Степента на критичност се получава като [въздействие х вероятност]

		Вероятност за реализиране		
		1-ниска	**2-средна**	**3-висока**
Въздействие на риска	**1-ниско**	Нисък риск	Нисък риск	Среден риск
	2-средно	Нисък риск	Среден риск	Висок риск
	3-високо	Среден риск	Висок риск	Критичен риск
	4-критично	Висок риск	Критичен риск	Критичен риск

Идентифицирани рискове - извадка - I

Управленски рискове

Неподходящо разпределение или припокриване на ролите и отговорностите в управленския екип

Въздействие	Вероятност	Оценка
3	1	Среден риск

Детайлно планиране на дейностите със срокове и водещ процеса служител. Провеждане на регулярни работни срещи. Онлайн координация.

Финансови рискове

Надхвърляне на планирания бюджет по пера

Въздействие	Вероятност	Оценка
2	2	Среден риск

Прехвърляне на средства между бюджетни пера. Наем срещу закупуване. Оптимизиране на бюджета.

Идентифицирани рискове - извадка - II

Ресурсни рискове

Участие на експерти в изборния процес под друга форма

Въздействие	Вероятност	Оценка
1	2	Нисък риск

Административни мерки – декларации. Проверка в регистрите на ЦИК/РИК/ОИК.

Отпадане на експерти поради извънредни събития

Въздействие	Вероятност	Оценка
1	2	Нисък риск

Поддържане на актуален списък с резерви.

Недостатъчно ниво на обучение и осъзнатост

Въздействие	Вероятност	Оценка
3	2	Висок риск

Работни срещи. Прилагане на онлайн обучения. Подготовка на видеоматериали. Обратна връзка.

Идентифицирани рискове - извадка - III

Външни рискове

Промяна на Изборния кодекс или други подзаконови нормативни актове

Въздействие	Вероятност	Оценка
3	3	Критичен риск

Проследяване на draft версиите на законопроектите. Ранна реализация и тестване на софтуерната система. Предварителна подготовка на персонала.

Невъзможност на доставчиците на външни услуги да изпълнят ангажиментите си

Въздействие	Вероятност	Оценка
3	1	Среден риск

Ранно информиране на всички доставчици на външни услуги за ролята им в процеса. Обновяване на контактните точки за спешни случаи. Оценка на представянето на доставчиците и замяна при необходимост.

Проблеми при интеграцията със системи на външни организации

Въздействие	Вероятност	Оценка
3	1	Среден риск

Приет риск. Ранно комуникиране с външните организации. Обновяване на контактните точки за спешни случаи.

Идентифицирани рискове - извадка - IV

Рискове при клиента

Забавено приемане на решения

Въздействие	Вероятност	Оценка
2	2	Среден риск

Приет риск.
Предварително изпълнение на част от дейностите.
Незабавно нотифициране за критичните дейности.
Инициране на работни срещи с ЦИК.

Недостатъчно ниво на ИТ компетентност в избирателните комисии

Въздействие	Вероятност	Оценка
2	3	Висок риск

Отделяне на допълнителен експертен ресурс в помощ на избирателните комисии.
Подобряване на потребителската документация.

Идентифицирани рискове - извадка - V

Технически рискове

Отпадане на технически средства

Въздействие	Вероятност	Оценка
2	2	Среден риск

Извършване на профилактика. Дублиране на критичните ресурси. Обновяване на техниката.

Пробив в информационната сигурност на публичните ресурси

Въздействие	Вероятност	Оценка
3	1	Среден риск

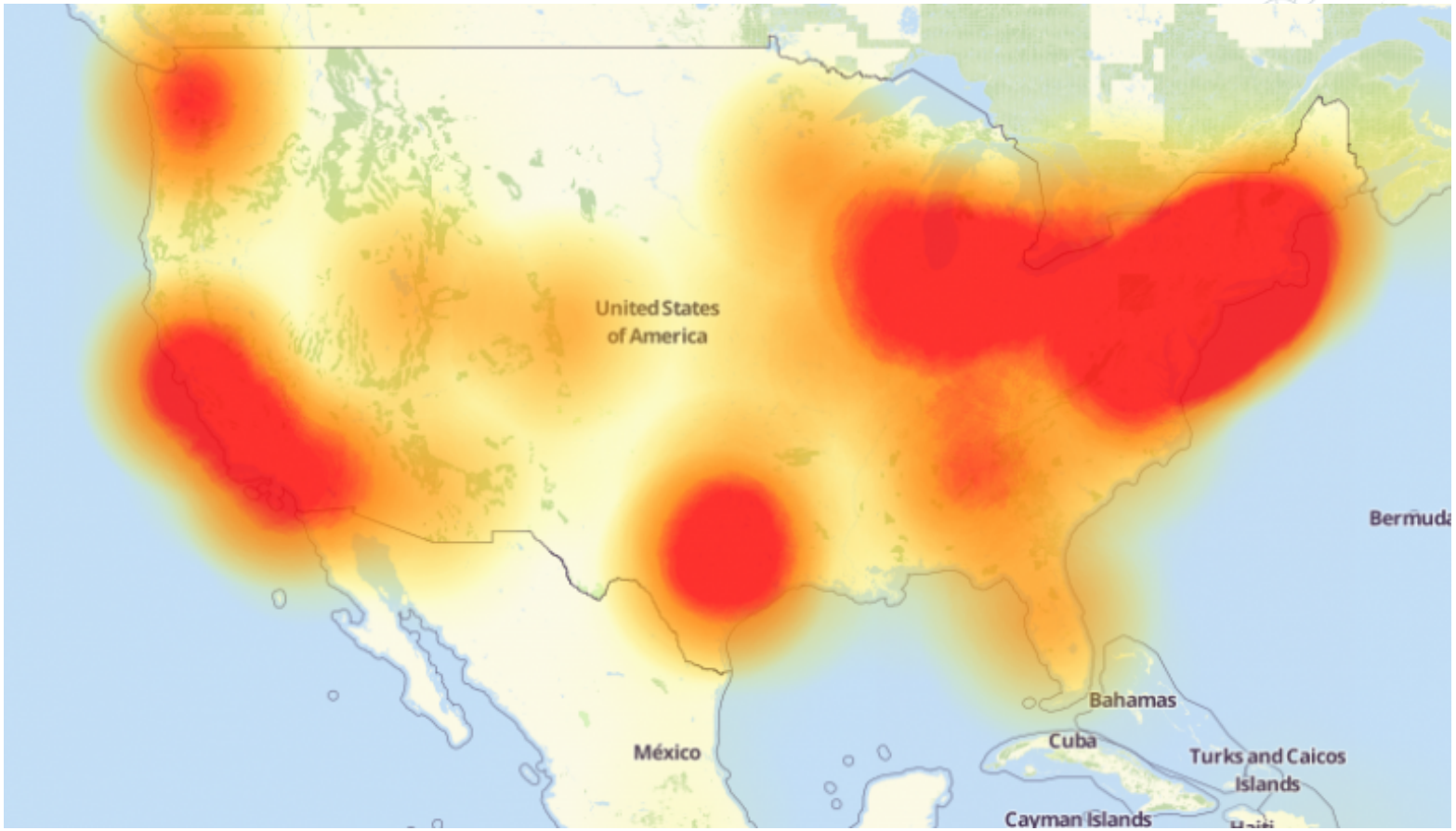
Извършване на вътрешни и външни одити на техническата уязвимост. Актуализиране на системните компоненти. Постоянно наблюдение на публичните ресурси.

Атаки от тип „отказ от услуга“ (DDoS)

Въздействие	Вероятност	Оценка
3	3	Критичен риск

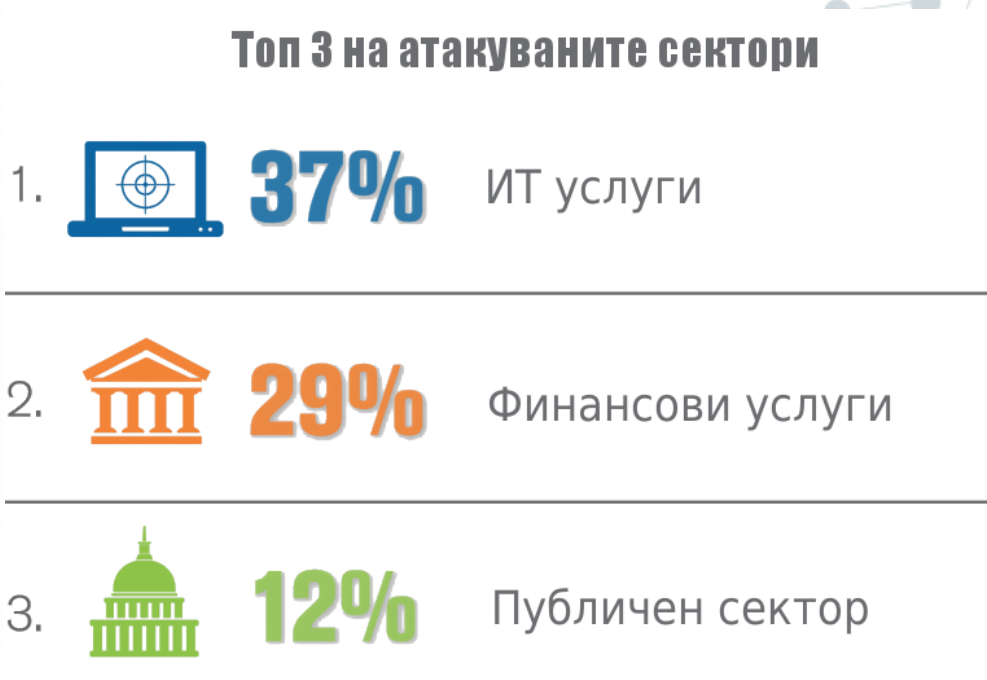
Специализирано мрежово оборудване. Постоянна връзка с доставчиците на Интернет, GovCERT и специализираните държавни органи. Постоянно наблюдение на публичните ресурси.

DDoS на практика



Прекъсване на достъпа до Интернет по време на атаката срещу Dyn (21 октомври 2016)

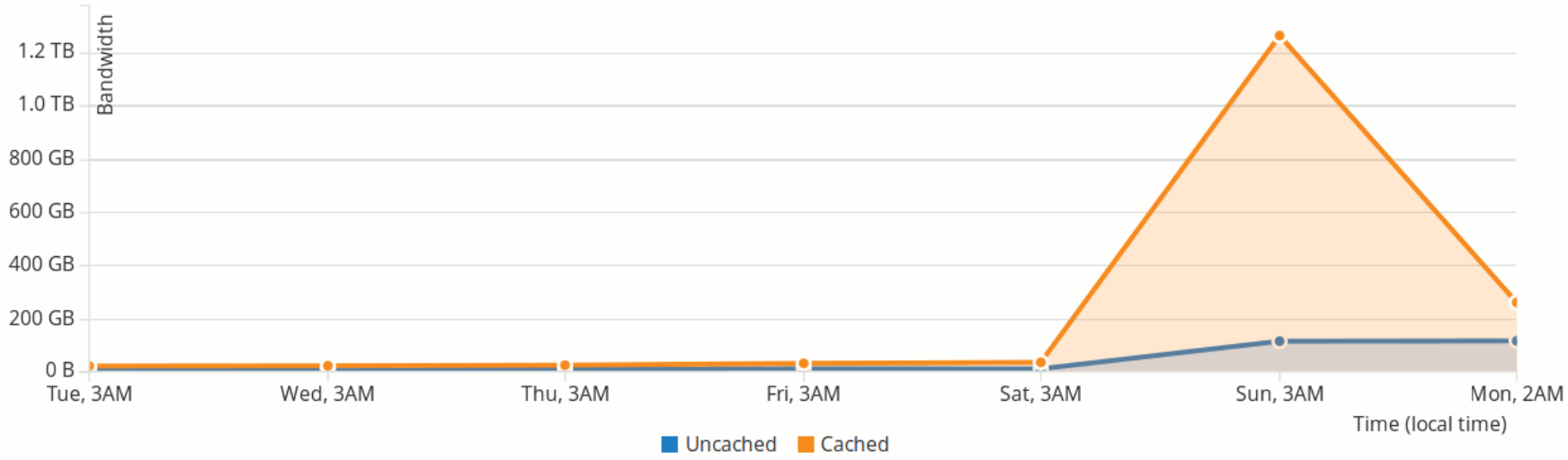
DDoS тенденции



Данни на Verisign,
Долкад за тенденциите при DDoS атаките, Q3 2016

DDoS срещу cik.bg през 2015

Total Bandwidth	Cached Bandwidth	Uncached Bandwidth
Last Week	Last Week	Last Week
2 TB	2 TB	276 GB

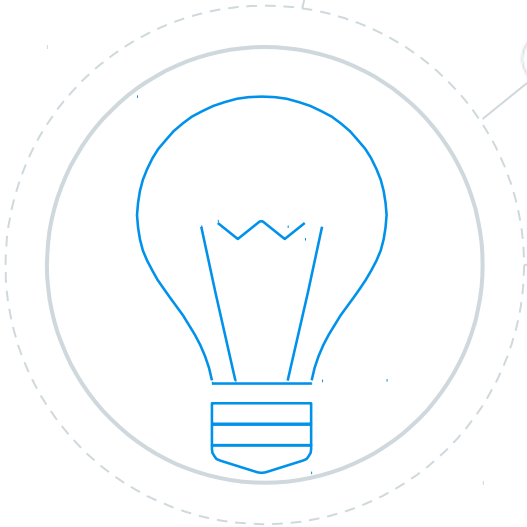


Атаката надвишаваше в пъти средните стойности за 2015

Обобщение

- ИО АД извървя дълъг път като организация и управление на дейностите по компютърната обработка през годините
- Създадени са условия за трансфер на добри практики между проектите
- Управлението на риска е постоянен процес, който не трябва да се подценява и извършва формално
- В същото време той не трябва и да затруднява и оскъпява дейностите излишно
- Потискането на съвременните заплахи изисква пълен синхрон и кооперация между всички участващи страни

Благодаря за вниманието!



Александър СТАНЕВ
alex@stanev.org

Илия ГОРАНОВ
i_goranov@bas.bg

БАИС, V НКИС
1-2 ноември 2016