ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

Тенденции и иновации в информационната сигурност

доц. д-р инж. Делян Генков, консултант мрежи и сигурност

27.09.2018 г.

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

Сдружение Клъстер Айтос (ITOS) е създадено през 2013 година.

Членове на сдружението: водещи компании в областта на информационните технологии, утвърдени строителни фирми, научни организации към БАН, НПО, читалище и общини

Сдружението работи за стимулиране развитието на информационните технологии , инфраструктурата за предоставянето на ИТ услуги; Аутсорсинга на ИТ услуги от България , облачни услуги, поддръжка на ИТ инфраструктурата, информационни системи.

Цели: Повишаване на квалификацията на български ИТ специалисти и подпомагане на международното сътрудничество в областта на информационните технологии.

ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

Сдружение Клъстер АЙТОС изпълнява проект № BG16RFOP002-2.009-0043 „Развитие на капацитета и интернационализацията на продуктите на Клъстер Айтос /ITOS/“ с финансовата подкрепа на ЕС чрез Европейския фонд за регионално развитие.

ОПЕРАТИВНА ПРОГРАМА ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

- **Общата цел на проекта е да насърчи устойчивото развитие на "Клъстер АЙТОС" чрез осигуряване на подкрепа за интернационализация на новите и съществуващите продукти на клъстера, както и изграждане на споделена инфраструктура за общите клъстерни дейности.**
- Специфичните цели на проекта са:

1. Повишаване степента на интеграция и сътрудничество на компаниите, работещи в сектора на информационните технологии в посока максимално използване на техния капацитет за разработка на конкуренти бизнес продукти и услуги и насърчаване активното присъствие на регионалния, националния и външните пазари. В рамките на проекта се извършва диверсификация на продуктите на Клъстер Айтос като с общи усилия на членовете на организацията се създава нов, конкурентен и търсен на регионалния пазар продукт – Платформа за облачно автоматизирано тестване на уеб и мобилни приложения.
2. Осигуряване на подкрепа за развитието на споделена клъстерна инфраструктура чрез създаване и оборудване на Симулационен център и развойна лаборатория към него за разработване и тестване на нови услуги и продукти на Клъстер Айтос, които да допринесат за интернационализацията на организацията. Новосъздадения център се разполага в град Габрово.
3. Насърчаване на клъстерния марктинг чрез осигуряване на необходимия експертен персонал за създаване на сътрудничества и интенрационализация на клъстерните продукти: наемане на експерт по интернационализация, ангажиране на консултантска компания, която да подпомогне навлизането на продуктите на пазара във Великобритания, както и разработване на Стратегия за интернационализация на Клъстера.
4. Подпомагане развитието на "Клъстер АЙТОС" и привличането на нови членове чрез организиране и участие в събития за представяне на клъстера и неговите продукти в страната и чужбина: пазари за ново-разработената услуга са Сърбия, Босна, Франция, Белгия, Германия, Великобритания и Македония.
5. Повишаване капацитета на Клъстера за създаване на сътрудничества и интернационализация чрез специализирани обучения, в които да вземат участие служители на членовете на Клъстера.

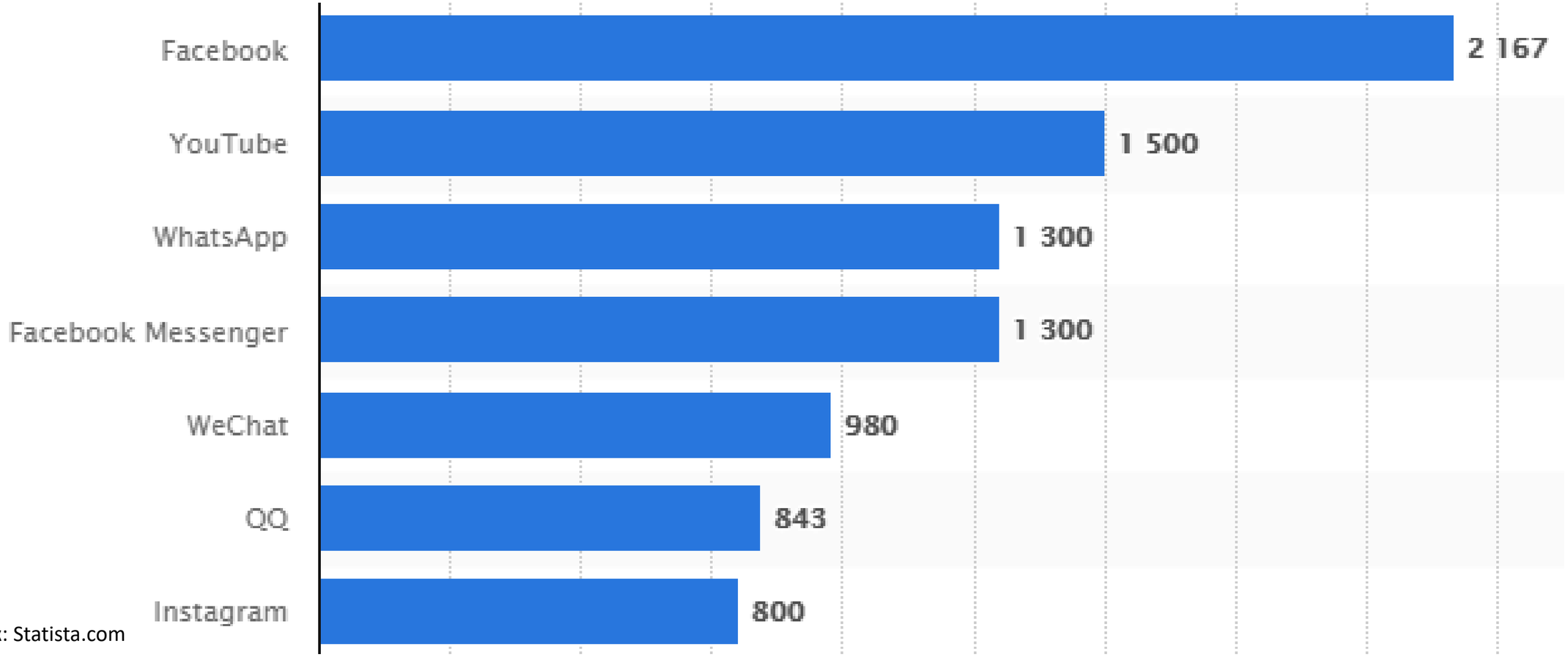
ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

Тенденции в информационния свят

ОПЕРАТИВНА ПРОГРАМА ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

Месечно активни потребители на Интернет приложения в милиони, януари 2018



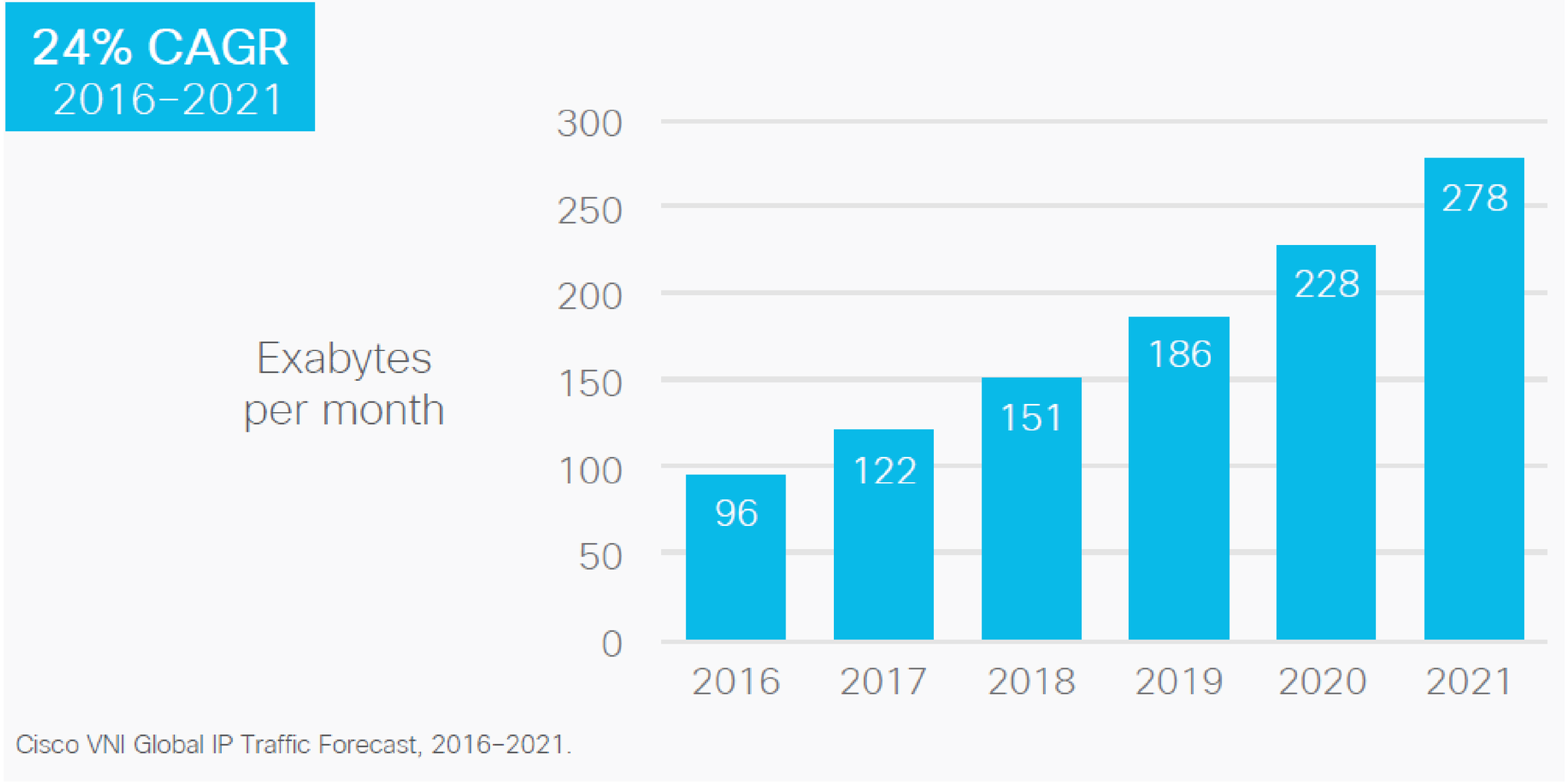
Източник: Statista.com

Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Годишно нарастване трафик

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ



Cisco VNI Global IP Traffic Forecast, 2016–2021.

ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

Глобален Интернет трафик

Year	Global Internet Traffic
1992	100 GB per day
1997	100 GB per hour
2002	100 GB per second
2007	2,000 GB per second
2016	26,600 GB per second
2021	105,800 GB per second

Източник: Cisco Systems

ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Съвременни технологии

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Облачни технологии (Cloud computing)
- Big Data
- Internet of Things (IoT)
- Artificial Intelligence (AI)
- Blockchain, криптовалута
- Електронно правителство
- Software Defined Networks (SDN)
- Bring Your Own Device (BYOD)
- IPv6

ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

Предизвикателства

- Cloud Security
  - Къде са моите данни?
  - Кой има достъп до тях?
  - Каква е сигурността на достъпа?
  - Какво ще стане, ако услугата спре?

- IoT
  - “S” in IoT stands for “Security”
  - 2016 – Mirai - 20000 IP камери и DVR с пароли по подразбиране спират достъпа до Twitter, Amazon, Tumblr, Reddit, Spotify и Netflix

ITCS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

Предизвикателства – продължение

- Artificial Intelligence (AI)
  - Много защитни механизми използват AI
  - Според IDG може и вече се използва в атаки
- Криптовалута
  - 01.2018 – над 500 милиона $ са откраднати
- Електронно правителство
  - Естония 2007, 2012
- Malware
  - WannaCry
  - Non Petya

Сдружение Клъстер Айтос

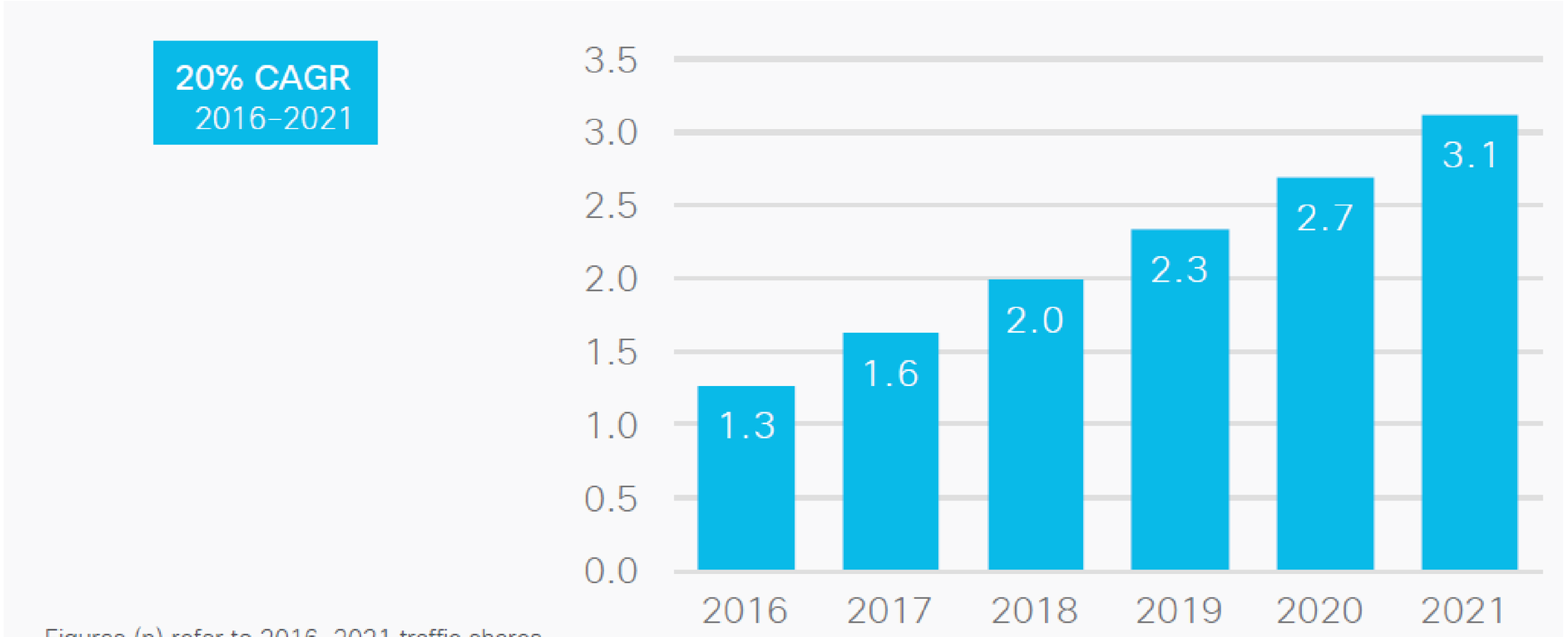
ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

Distributed Denial-Of-Services

DDoS атаки с трафик над 1 Gbit/s, в милиони

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

Global DDoS attacks forecast, 2016-2021



Figures (n) refer to 2016, 2021 traffic shares.
Source: Cisco VNI Global IP Traffic Forecast, 2016-2021.

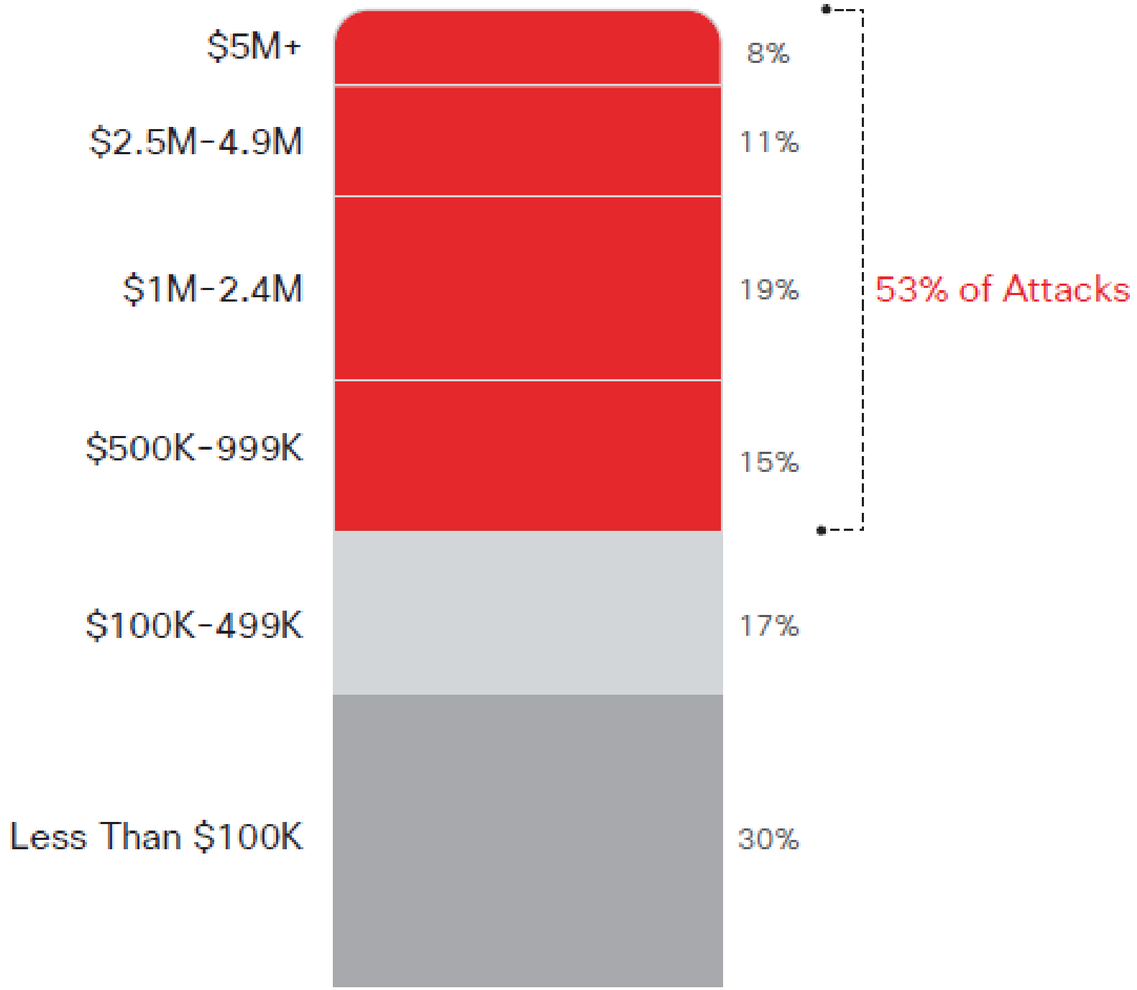
ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

Кражба на данни

Колко струва кражбата на данни и информация?



Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

Решения за сигурност

Част от решенията за сигурност

- Next Generation Firewall
- Next Generation intrusion prevention system
- Cloud Security
- Data Leak Protection
- Mobile Device Management
- Endpoint Security
- Web and E-mail security
- Advanced Malware protection
- Security Audits
- Vulnerability assessment и Penetration tests
- Outsourced Security

ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

NGFW

Защитни стени от ново поколение

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Притежават Advanced malware protection (AMP), адресиращо познати и непознати заплахи, интегриран sandbox
- Актуализират знанията си за атаки и зловреден код автоматично и централизирано
- Дават възможност за проследяване и ограничение на зарази
- Автоматично свързват събитията около дадена атака и намират уязвимостите
- Анализират слабостите в мрежата и препоръчват най-добрите политики за сигурност според ситуацията
- Интегрират се с много продукти за сигурност, като защитават предишните инвестиции и осигуряват по-добра степен на сигурност

ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

NGIPS

Системи за предотвратяване на прониквания от ново поколение

ОПЕРАТИВНА ПРОГРАМА ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

- Следят трафика в цялата мрежа и крайните системи, идентифицират и блокират познати и непознати атаки на базата на сигнатури, разлика в нормалното поведение и други фактори
- Позволяват наблюдение и контрол в реално време на потребители, приложения, устройства, заплахи и уязвимости в мрежата
- Светкавично откриват, блокират, ограничават и премахват заплахи, виртуално поправят уязвимостите преди наличието на нови версии или добавки на софтуера
- Автоматично свързват събитията и данните по даден пробив, за по-голяма сигурност и по-лесно разследване
- Получават автоматично над 35000 правила за атаки, заплахи и зловреден код от целия свят

Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Cloud Security

Сигурност на облачни приложения

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Защита от достъп до подозрителни места в Интернет по всяко време и на всяко място
- Защита на електронна поща от SPAM, вируси, Phishing
- Защита на потребители, данни и приложения в облачни инфраструктури срещу компрометирани акаунти, зловреден код и изтичане на данни

Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА РЕГИОНАЛНО РАЗВИТИЕ

Data Leak Protection

Системи за защита от изтичане на данни

ОПЕРАТИВНА ПРОГРАМА ИНОВАЦИИ И КОНКУРЕНТОСПОСОБНОСТ

- Следене на електронна поща за изпращане на чувствителна информация;
- Следене на достъп до външни облачни услуги;
- Използване на алгоритми, базирани на машинно обучение, което дава възможност на софтуера да различава нестандартни или нетипични дейности, свързани с обмяна на информация;
- Следене за неоторизиран достъп до ресурси, копиране или изпращане на чувствителни данни от персонала.
- Защитава: Data at-rest – архивирана информация, Data in-use – текущо използвани данни, Data in-motion – предавани по комуникационни канали

ITOS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Сигурност за крайните точки

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Антивирус, антиспам, защита от зловреден код;
- Криптиране на данните при предаване и съхранение;
- Автоматична актуализация на операционни системи и софтуер;
- Защита от достъп до подозрителни сайтове или места в Интернет;
- Резервираност на данните.

ITCS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Penetration тестове

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Извършат коректна оценка на способността да защитят своите мрежи, приложения, данни, системи и потребители от недоброжелателни хакери;
- Проверяват защитата на активите и репутацията на компанията за избягване на финансови загуби и негативна публичност, които могат да бъдат причинени от компрометиране на системите и данните на организацията;
- Предоставят подробна информация за действителни заплахи, които могат да бъдат експлоатирани;
- Идентифицират и дават оценка за това кои уязвимости са критични за организацията, кои са по-незначителни;
- Аргументират и оправдават нуждата от бюджет, свързан със сигурността;
- Предлагат по-ефективни методи за отстраняване на открити уязвимости и съответно повишаване сигурността на системите в организацията;

Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

Други услуги за сигурност

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

- Security Awareness обучения
- Анализ на трафика
- Анализ на безжичната мрежа
- Внедряване на стандарти, политики и процедури за сигурност
- Анализ и оценка на риска
- Изработване на стратегия
- Политика по информационна сигурност
- Изграждане, внедряване и изпълнение на процеси по управление на инциденти
- Анализи и сравнение с добрите практики
- Мониторинг и контрол

ITCS
Сдружение Клъстер Айтос

ЕВРОПЕЙСКИ СЪЮЗ
ЕВРОПЕЙСКИ ФОНД ЗА
РЕГИОНАЛНО РАЗВИТИЕ

ОПЕРАТИВНА ПРОГРАМА
ИНОВАЦИИ И
КОНКУРЕНТОСПОСОБНОСТ

Благодаря за вниманието

Въпроси?

- http://www.clusteritos.org/

- office@clusteritos.org
- dgenkov@tugab.bg

ITOS
Сдружение Клъстер Айтос