Кибербезопасность

Международная конференция, посвященная 25-летию кыргызского сома, Бишкек, 11 Мая 2018 г.

Dr. Stephan Murer, Murer Consulting GmbH

stephan.murer@ggaweb.ch

Кибербезопасность – это больше, чем конфиденциальность

Конфиденциальность

Целостность

Доступность

Хакеры продают данные пользователей карт и др. за 1 доллар
Американское бюро кредитной истории «Equifax» сообщает, что кибератака могла повлиять на, как минимум, 143 млн человек в США.

101 млн долл. США похищены из Центрального банка Бангладеша через SWIFT
Кейс-стади : Ограбление Банка Бангладеш

криминальное

Неполадки в «облачных» сервисах интернет-магазина «Амазон» приводят к сбоям работы различных веб-сайтов
Это пример одного из различных сбоев, риск концентрации

и снова в 2017 год
Самолеты авиакомпании «United Airlines» вынуждены совершать аварийные посадки из-за компьютерных проблем

случайное

https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery , 9.4.2018
https://bits.blogs.nytimes.com/2011/04/21/amazon-cloud-failure-takes-down-web-sites/, 9.4.2018
https://www.nytimes.com/2015/07/09/business/united-airlines-grounds-flights-citing-computer-glitch.html, 9.4.2018
https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html, 9.4.2018

Угрозы

	Мотивация	Игроки	Цель
Кибервойна	Военная / политическая	Национальные государства	Критическая инфраструктура
Терроризм	Политические изменения	Террористические группы	Инфраструктура, государственные активы
Шпионаж	Разведка, выгода от интеллектуальной собственности	Национальные государства, предприятия	Правительства, компании, индивидуумы
Организованная преступность	Финансовая выгода	Преступники	Компании, индивидуумы
Хакеры	Эго, любопытство, изменение	Группы, индивидуумы	Правительства, компании, индивидуумы

…но имейте в виду, что в 30-70% случаев это является случайными инцидентами

https://www.slideshare.net/MarketingArrowECS_CZ/modern-malware-and-threats, 9.4.2018

Экономический ущерб от киберпреступности

Регион (Всемирный банк)	Регион ВВП (трлн долл. США)	Потери от киберпреступности (млрд долл. США)	Потери от киберпреступности (в % от ВВП)
Северная Америка	20,2	от 140 до 175	от 0,69 до 0,87
Европа и Центральная Азия	20,3	от 160 до 180	от 0,79 до 0,89
Восточная Азия и Тихий океан	22,5	от 120 до 200	от 0,53 до 0,89
Южная Азия	2,9	от 7 до 15	от 0,24 до 0,52
Латинская Америка и Карибский бассейн	5,3	от 15 до 30	от 0,28 до 0,57
Субсахарная Африка	1,5	от 1 до 3	от 0,07 до 0,20
Ближний Восток и Северная Африка	3,1	от 2 до 5	от 0,06 до 0,16
Мир	**75,8**	**от 445 до 608**	**от 0,59 до 0,80**

Киберпреступность	Оцененная ежедневная активность, долл. США
Злонамеренное сканирование	80 млрд
Новые вредоносные программы	300 тыс.
Фишинг	33 тыс.
Вымогательство	4 тыс.
Потеря данных вследствие взлома	780 тыс.

- Сопоставимо с глобальной торговлей наркотиков
- ~15% всех транснациональных преступлений
- Только объемы Internet экономики стран G-20 составляют 4,2 трлн долл. США

https://www.csis.org/analysis/economic-impact-cybercrime, 9.4.2018
https://www.bcg.com/documents/file100409.pdf, 9.4.2018

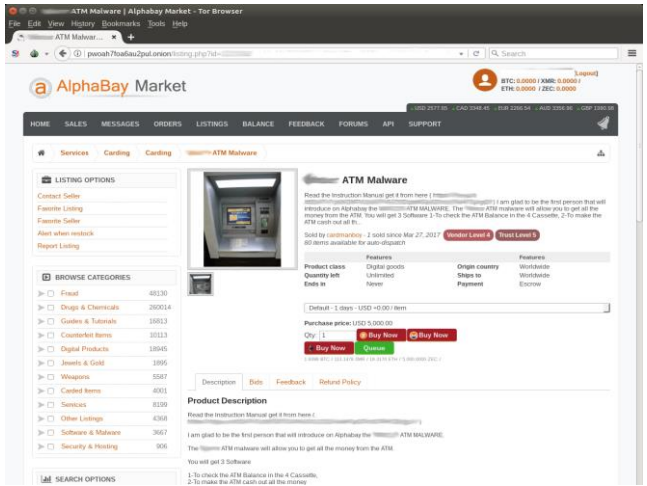
Экосистема киберпреступности

Обнаружение / использование уязвимостей
Хакеры / Создатели вредоносных кодов

Заражение / распределение
Непрофессиональные хакеры / Распространители вредоносных программ / Спамеры

Эксплуатация (выкачивание средств)
Кассиры / Преступные сообщества / «Прачечные» по отмыванию денег

- Номер кредитной карты, учетные записи электронной почты – 0,50-20$ за 1000 единиц
- Аккаунт облака – 7-8$
- Информация о средствах по страхованию здоровья – 50$
- Пользовательские вредоносные программы – 3500$
- DDoS-атака – 1000$ в день



http://www.siemworks.com/Solutions-Security.asp, 9.4.2018
https://www.cybersecobservatory.com/2017/10/17/atm-malware-sold-darknet-market/, 9.4.2018

Финансовая индустрия – ключевая задача

Финансовые услуги		2016 ранг	Тренд
1) Развитие рынка (волатильность, интенсивная конкуренция / новые участники, M&A, стагнация рынка, колебания рынка)	41%	1 (44%)	-
2) Кибер-инциденты (кибер-преступления, ИТ-сбои, утечка данных и т.д.)	40%	2 (44%)	-
3) Изменения в законодательстве и регулировании (смена правительства, экономические санкции, протекционизм и т.д.)	36%	3 (37%)	-
4) Макроэкономические достижения (программы по сдерживанию расходов, рост цен на товары, дефляция, инфляция)	33%	4 (29%)	-
5) Политические риски и насилие (война, терроризм и т.д.)	23%	Новый	▲

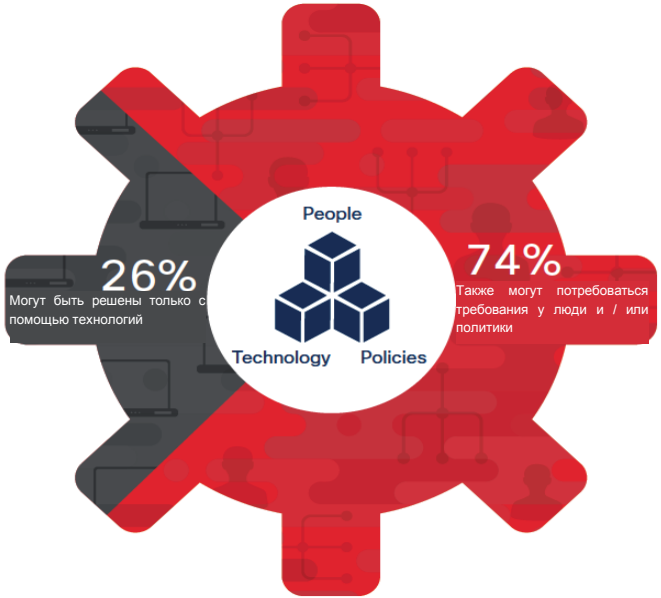
252 responses
Source: Allianz Global Corporate & Specialty. Figures represent the number of responses as a percentage of all responses. More than one risk selected.

Топ-5 наиболее часто атакуемых секторов

… и мы знаем это!

IBM X-Force Threat Intelligence Index 2017, IBM Security, March 2018
Allianz Risk Barometer, Business Risk 2017

Люди – самое слабое звено

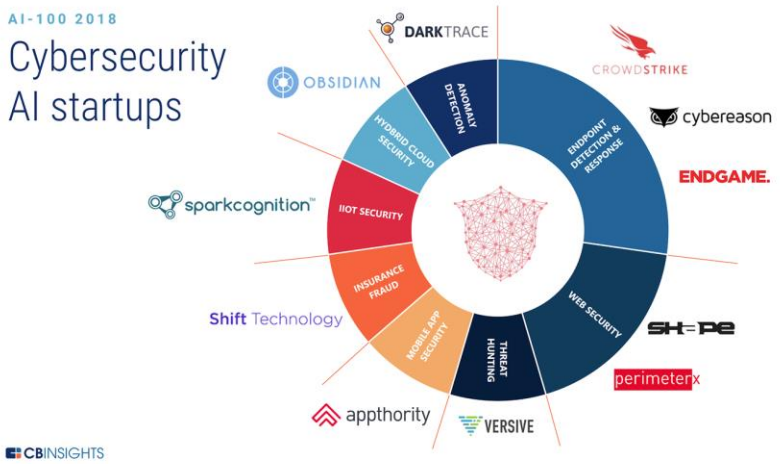


Source: Cisco Security Research

- 52% -95% инцидентов – это человеческий фактор в несоблюдение правил безопасности (случайно или умышленно, по халатности или саботаж)
- Использование социальной инженерии для проведения целенаправленных атак
- 10% (6% в финансовой отрасли) становятся жертвами организованных фишинг атак, количество жертв снижается вследствие информированности
- Чрезмерная нагрузка со стороны работодателей на сотрудников в финансовом секторе может привести к их недовольству. Такие сотрудники становятся сознательными проводниками кибер-атак
- Большинство человеческих ошибок являются результатом ошибок и халатности
- Технология порой беспомощна против человеческого фактора – нужен трехсторонний подход
- Личный опыт: большинство утечек данных были совершены недовольными сотрудниками (н-р, налоговой службе Германии были проданы CD с информацией о деятельности компании), крупнейшие махинации стали результатом халатности и слабых технологий со стороны пользователей

https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/, 10.4.2018
https://www.scmagazine.com/study-find-carelessness-among-top-human-errors-affecting-security/article/535928/, 10.4.2018
CISCO 2018 Annual Cybersecurity Report

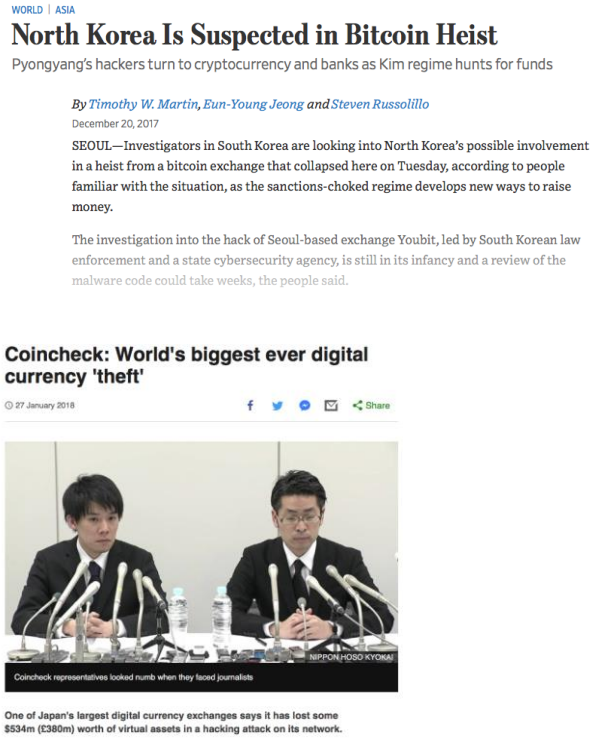
От защиты до обнаружения и быстрой реакции



- **Техническая защита имеет свои пределы**
  - Дороговизна
  - Не воспринимается пользователями (комфорт пользователей или же безопасность)
  - Ошибки в настройках средств защиты создают более высокий риск несанкционированного доступа к данным, что приводит к отклонению контроля риска безопасности (например, правила брандмауэра, сложные правила контроля доступа)
  - Невозможно защитить от разрешенных, но неосторожных или умышленных пользователей (человеческий фактор)
- **Мониторинг активности системы и пользователей и автоматизированное реагирование**
  - Машинное обучение для обнаружения отклонений (известные отклонения или неизвестные)
  - Схемы мошенничества при совершении сделок
  - Необычное поведение пользователей
  - Связанность между разными источниками событий (например, сетевой адрес, стиль ввода и характеристики транзакций для выявления атак с помощью электронного банкинга)
  - Автоматическое реагирование путем удаления доступа, прекращение осуществления операций или запрос дополнительной авторизации
  - Deep Instinct утверждает, что он может обнаружить > 98% новых угроз с ошибкой <0,01% (по сравнению с 63% и 2,5-5% со своими конкурентами)

https://www.cbinsights.com/research/artificial-intelligence-top-startups/, 11.4.2018
https://www.datanami.com/2018/01/25/deep-learning-approach-detecting-unknown-malware/, 13.4.2018

Криптовалюты не защищены



WORLD | ASIA

North Korea Is Suspected in Bitcoin Heist

Pyongyang's hackers turn to cryptocurrency and banks as Kim regime hunts for funds

By *Timothy W. Martin, Eun-Young Jeong* and *Steven Russolillo*

December 20, 2017

SEOUL—Investigators in South Korea are looking into North Korea's possible involvement in a heist from a bitcoin exchange that collapsed here on Tuesday, according to people familiar with the situation, as the sanctions-choked regime develops new ways to raise money.

The investigation into the hack of Seoul-based exchange Youbit, led by South Korean law enforcement and a state cybersecurity agency, is still in its infancy and a review of the malware code could take weeks, the people said.

Coincheck: World's biggest ever digital currency 'theft'

27 January 2018 Share

Coincheck representatives looked numb when they faced journalists

NIPPON HOSO KYOKAI

One of Japan's largest digital currency exchanges says it has lost some $534m (£380m) worth of virtual assets in a hacking attack on its network.

- Цифровые валюты – привлекательные цели для атак
- Основной недостаток – секретные ключи, которые:
  - являются единственным способом доступа к цифровым валютам
  - могут быть украдены, но не утеряны
  - не должны быть доступны
  - часто хранятся вместе с онлайн-кошельками
- Цифровые валюты подвержены потенциальному саботажу
- Используемые в настоящее время цифровые подписи могут потенциально быть взломаны будущим квантовыми компьютерами.

https://www.wsj.com/articles/north-korea-is-suspected-in-bitcoin-heist-1522303177, 11.4.2018
http://www.bbc.com/news/world-asia-42845505, 11.4.2018

Недостаток знаний в области кибербезопасности

- Дефицит в 2 млн специалистов по кибербезопасности к 2019 году
- 3-кратный рост рабочих мест по кибербезопасности по сравнению с другими ИТ-специальностям, в 2010-2014 годах
- У 53% организаций поиск специалистов по кибербезопасности занимает около 6 месяцев
- В Сингапуре (2015) 58% ИТ-специалистов в целом и 75% специалистов по безопасности были трудоустроены
- Среднее увеличение заработной платы специалистов в сфере ИТ-безопасности было почти в два раза больше общего роста зарплат ИТ-специалистов
- Недостаток кадров может увеличить риски компаний или задержать реализацию проектов
- Тяжело найти для правоохранительных органов компетентных специалистов области в киберпреступности

ISACA, 2016 cyber security skills gap, http://cybersecurity.isaca.org
https://www.computerworld.com.sg/print-article/79050/, 11.4.2018
https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf, 11.4.2018

Программа кибербезопасности для центрального банка

Использование возможностей центрального банка для защиты банковской системы от кибер угроз

- Создавать и поддерживать свою собственную систему реагирования в области кибер-рисков
- Определять современные стандарты управления кибер-рисками
- Настаивать на современном управлении кибер-рисками в поднадзорных учреждениях
- Регулярно проверять готовность учреждений к кибер-рискам и угрозам
- В случае слабой системы кибер-защиты у поднадзорных учреждений последние должны иметь достаточный капитал для покрытия операционных рисков

Соблюдение внутренних стандартов:

- Внедрять управление кибер-рисками в соответствии с самыми высокими стандартами
- Следить за кибер-рисками в новых проектах, особенно в цифровых валютных проектах

Как ключевое учреждение в малой экономике:

- Содействовать активному сотрудничеству между финансовыми институтами и государственными органами по вопросам кибер-рисков
- Усиливать обучение и навыки специалистов в области ИТ-безопасности
- Помогать информировать всех участников местных финансовых рынков о кибер-рисках

Спасибо

https://commons.wikimedia.org/wiki/File:Thank-you-word-cloud.jpg, 11.4.2018

Приложение: Атаки бывают разных форм

Инцидент

Атака(и)

Событие

Атакующие (нападающая сторона)	Инструменты	Уязвимости	Действия	Цель	Результаты неавторизированного доступа	Задачи
Хакеры	Физическая атака	Дизайн	Тестирование	Аккаунт	Повышенный доступ	Попытка взлома, удовлетворение
Шпионы	Обмен информацией	Имплементация	Сканирование	Процесс	Разглашение сведений / информации	Политическая выгода
Террористы	Команды для пользователей	Конфигурация	Флуд	Данные	Искажение информации	Финансовая выгода
Корпоративные рейдеры	Скрипты или программы		Аутентификация	Компоненты (программные объекты)	Отказ в доступе	Нанесение ущерба
Профессиональные преступники	Программные объекты (агенты)		Обход	Компьютер	Кража ресурсов	
Вандалы	Инструментальный пакет разработчика (прикладных программ)		Имитация	Сеть		
Вуаеристы	Дистрибутивный инструмент		Чтение	Сетевой комплекс		
	Запись данных (контроль потока данных)		Копирование			
			Воровство			