КТО ВООРУЖЕН, ТОТ НЕ ЗАРАЖЕН

Николай АЛЕКСЕЕВ
n.alekseev@souzveche.ru

Правоохранители России и Беларуси отмечают взрывной рост преступлений в информационной среде. Каков размах угроз в 2017-м и как с ними бороться?


Владимир ТРЕФИЛОВ/РИА Новости

У них нет имени, нет лица, но проблем могут доставить, как целая армия.

ОБЩАЯ ТРЕВОГА

- С 2013-го по 2016 год число киберпреступлений увеличилось в шесть раз - с 11 тысяч до 66 тысяч. Значительный рост наблюдается и в этом году - плюс 26 процентов, - заявил недавно **Генпрокурор РФ Юрий Чайка.** - Все большую распространенность получают мошенничество в Сети, информационные блокады, компьютерный шпионаж. В прошлом году две трети преступлений экстремистской направленности совершалось с использованием интернета.

Ежегодный ущерб от хакеров экономике РФ составляет по разным оценкам от двухсот до четырехсот миллиардов рублей. По данным компании SecureWorks, популярными «услугами» теневого интернета стали взломы кредиток и сетевых аккаунтов, DDoS-атаки и продажа досье на любую компанию.

В марте **Президент России Владимир Путин** сообщил, что количество атак на государственные информресурсы за год выросло в три раза. Он поручил усовершенствовать системы защиты секретных сведений, учитывая массовый переход ведомств на электронный документооборот.

В белорусском Следственном комитете сообщили, что в республике активизировался киберкриминал. В первом полугодии возбуждено почти на девять процентов дел больше, чем за аналогичный период 2016 года.

УКРАЛИ ПРОЦЕНТ ВВП

По оценкам международных экспертов, общие потери от вредоносных программ уже достигают одного триллиона долларов, что больше одного процента от мирового ВВП. И цифры продолжают расти.

В компании Microsoft отмечают, что Беларусь и Россия стали благодатной почвой для киберугроз из-за повсеместного использования пиратского программного обеспечения. В нем, как правило, есть «потайные двери».

- В 65 процентах случаев на ПК сотрудников устанавливается нелицензионное ПО, а каждый четвертый сотрудник самостоятельно скачивает нелегальные программы, - рассказали «СВ» в Microsoft. - 97,5 процента компаний минимум раз в год подвергались киберугрозам.

Сейчас у Управлений «К» министерств внутренних дел России и Беларуси горячая пора - жалобы сыплются как из рога изобилия. Обе структуры сформированы в 2001 году и с тех пор активно сотрудничают.

В МВД обеих стран отмечают: на смену хакерам-одиночкам и небольшим бандгруппам пришли крупные высокоорганизованные преступные сообщества. Один из способов обуздать их - ужесточать наказание. В этом году приговоры интернет-бандитам стали строже.

ПЛЕЧОМ К ПЛЕЧУ

Информационной безопасностью должно заниматься не только МВД, а буквально все ведомства. Об этом шла речь на недавней коллегии министерств связи России и Беларуси.

- Летом мы встречались с российскими коллегами и подписали соглашение о развитии интеграционных проектов, - рассказал «СВ» **министр связи и информатизации Беларуси Сергей Попков**. - Вы видите, что сейчас делается - кибербезопасность выходит на первое место. Нужно принимать решения совместно, чтобы обеспечить нашу защиту. К сожалению, это борьба долгая, трудная и не всегда мы можем предотвратить тот или иной инцидент, который может повлиять как на экономику, так и в целом на безопасность страны. В Беларуси есть специалисты, которые занимаются защитой предприятий от кибернападений, и здесь мы должны держать связь с российскими коллегами.

Министр связи и массовых коммуникаций России Николай Никифоров подтвердил, что с белорусами установлены хорошие контакты:

- Нужно усилить взаимодействие в сфере IT-безопасности, создания системы мониторинга и совместного реагирования на возникающие угрозы.

Готово оказать содействие и Парламентское Собрание Союза Беларуси и России.

- На заседаниях комиссий мы также поднимаем вопросы информационной безопасности. У нас есть площадка межпарламентского сотрудничества, мы можем помочь в решении проблемы на законодательном уровне, - сказал глава **Комиссии ПС по вопросам внешней политики, сенатор РБ Сергей Рахманов.**

Будут осуществляться мероприятия и за счет Союзного государства. Например, в этом году бюджет СГ профинансирует конференцию «Комплексная защита информации».

МНЕНИЕ ЭКСПЕРТА

Злой Petya остановил конвейер на заводах

Илья САЧКОВ, президент компании Group-IB, самый известный частный кибердетектив России:


Владимир ТРЕФИЛОВ/РИА Новости

- Мы создаем технологии раннего предупреждения кибератак, которые экспортируем в 60 стран мира. Даже в США в прошлом году увеличили выручку на 150 процентов. Атаки хакеров в основном ориентированы на получение финансовой выгоды, но есть, к сожалению, новый тренд - кибертерроризм. Большое число предприятий абсолютно к этому не готовы. В первую очередь из-за того, что разработчики средств защиты информации зачастую не понимают, что такое компьютерная преступность. Их решения выглядят как накачанный боксер, который ни разу не выходил на ринг.

Пример начала лета: из-за вируса Petya в России 150 предприятий остановили работу. А ведь они проинвестировали в информационную безопасность двести миллионов долларов! Замерло производство, автозаправки перестали принимать карты, встал даже выпуск алкоголя.

Мы видим, что у специалистов просто не хватает знаний. Необходимо налаживать работу между университетами, в том числе и белорусскими. Я сейчас преподаю в МГТУ им. Баумана, мы сотрудничаем с Кембриджем. И я вижу даже в этих уникальных вузах отсутствие знаний, от чего ребята должны защищать бизнес и государство. Но ведь цифровая экономика не может развиваться без информационной безопасности.

Мы также готовы предоставлять белорусским компаниям современные знания по предотвращению кибератак. Например, наши клиенты были защищены от этого «Пети» даже притом, что в базе еще не было информации о нем. Помогли серьезные наработки в области машинного обучения. Система автоматически его остановила.

ПОРВАЛИ СЕТИ

ВИРУСЫ-РАЗРУШИТЕЛИ

В 2010 году вирус Stuxnet успешно атаковал и частично вывел из строя ядерную систему Ирана. Он заблокировал работу двадцати процентов иранских центрифуг для обогащения урана. При этом скопировал запись систем видеонаблюдения и прокрутил ее во время операции, чтобы служба безопасности ничего не заподозрила.

Эксперты «Лаборатории Касперского» увидели в Stuxnet прототип кибер-оружия, создание которого повлечет за собой новую гонку вооружений. И, к сожалению, оказались правы.

В начале лета специалисты компании ESET сообщили об обнаружении нового вируса-разрушителя - Industroyer. Его назвали крупнейшей угрозой инфраструктуре после Stuxnet. Он способен приводить как к простому отключению электроэнергии, так и к повреждению оборудования. Industroyer уже опробовали в 2016 году для атаки на электросети Украины.

- Ситуация с киберзащищенностью промышленных систем по всему миру хуже некуда, целевые атаки на них - вопрос ближайшего будущего, - считает **глава компании «Монитор безопасности» Дмитрий Гвоздев.**

Но наши АЭС полностью автономны, все системы, включая компьютерные, изолированы от внешних угроз. Так что сетевые атаки не страшны.