



radware

# GLOBAL APPLICATION & NETWORK SECURITY REPORT 2017-18

## ➔ КРАТКИЙ ОБЗОР

В течение 2017 года заголовки пестрили сообщениями о кибератаках и угрозах безопасности, в том числе о возможном вмешательстве в президентские выборы в США, эпидемиях заражения вредоносным ПО и взломе базы данных Equifax. Эти и другие громкие события вызвали рост инвестиций в киберзащиту, как со стороны государств и глобальных корпораций, так и со стороны частных лиц, приобретающих антивирусные решения для личных устройств. Однако с ростом инвестиций растет и число угроз, взломов и уязвимостей.

В стремлении понять эту сложную и проблематичную динамику Radware выпускает *Глобальный отчет о безопасности приложений и сетей*. В отчете обобщаются результаты опроса глобальной отрасли, собственные исследования Radware, фактические данные об атаках и истории клиентов для создания картины того, где именно мы находимся и что могут сделать специалисты по защите.

Этот отчет может быть полезным всему сообществу кибербезопасности, и он содержит исследования и выводы Radware по следующим вопросам:

- Панорама угроз – «кто, что и почему» агрессоров
- Возможное влияние на ваш бизнес, в том числе затраты, вызванные различными кибератаками
- Уровень готовности по отраслям
- Опыт организаций в вашей отрасли
- Возникающие угрозы и как от них защититься
- Прогнозы на 2018 год

## ➔ НА ПРЕДЕЛЕ ВОЗМОЖНОСТЕЙ

Сегодня основной мотив кибератак – киберпреступления. Атакующими движет стремление к финансовой наживе и благоприятные обстоятельства, которые им обеспечил бум криптовалют. В то же время атаки становятся все более адресными. Серьезно настроенный враг потратит время на изучение цели и инвестирует любые необходимые ресурсы в разведку, социальный инжиниринг и конкретные инструменты.



Вредоносное ПО и боты, а также угрозы, созданные с использованием социальной психологии, стали самыми распространенными векторами атак. Однако организациям не следует бояться только тех угроз, что уже находятся перед ними. Они должны опасаться того, что скрывается за углом, в том числе бот-сетей Интернета вещей, постоянного отказа в обслуживании (DDoS), SSL-атак и изолированного внедрения вредоносных программ. Организации могут подготовиться, познакомившись с новыми технологиями, такими как Интернет вещей (ИВ), блокчейн, функция как услуга (FaaS)/внесерверная обработка данных.

Нормативное регулирование продолжает играть важную роль в повышении уровня защиты, обеспечивая рекомендации и стандарты для отраслей или регионов. В то время как многие организации работают над обеспечением соответствия стандартам безопасности и конфиденциальности, создается впечатление, что соответствие при оценке решений по безопасности заботит их меньше. В итоге некоторые организации не знакомы со всеми типами сертификации, и почти одна треть никогда не спрашивает об этом своих поставщиков.

Массированные глобальные кибератаки в 2017 году стали успешными исключительно по причине незакрытых уязвимостей. Это пример небольшой и обычной человеческой ошибки с катастрофическими последствиями. Обучение машин и искусственный интеллект (AI) могут казаться логичным решением. Двадцать процентов организаций уже используют такие решения, и еще 28% планируют ввести их в 2018 году. Но и они не безупречны. Просто представьте себе риск заражения AI и хаос в автоматических системах, а также безумие, которое может охватить такие системы (например, Microsoft Tay и чат-боты Facebook).

Сложите все это вместе, и станет ясно, что мы ступаем на зыбкую почву. Люди приближаются к краю своей коллективной возможности удерживать контроль. Однако AI и обучение машин еще не достигли должного уровня и их легко обмануть.

## ➔ ДРУГИЕ ВЫВОДЫ И ФАКТЫ



### **Выкуп был мотивом каждой второй атаки**

На фоне стремительного взлета стоимости биткойна также увеличилось число атак для получения выкупа. Организации назвали выкуп мотивом половины атак, что делает его самой распространенной причиной – более частой, чем инсайдерские угрозы, хакерская активность и конкуренция. 42% организаций в мире стали объектом хакерских атак, что на 40% больше, чем в 2016 году.



### **Основная проблема: утечка данных**

Утечка данных/информации стала проблемой безопасности номер один – ее назвали 28% организаций во всем мире. Еще одна проблема – падение уровня/недоступность сервиса (23%).



### **Число DDoS-атак растет, и увеличивается их интенсивность на уровне приложений**

Распространенность DDoS-атак увеличилась на 10%, и им подвергались каждые две из пяти компаний. Одна из шести была объектом атаки бот-сети ИВ, и 68% атак привели к падению уровня или полной недоступности сервиса. И то, и другое означает потери. В 2017 году также выросло число атак на уровне приложений по сравнению с атаками на уровне сети.



### **80% не отслеживают затраты**

Восемьдесят процентов организаций не делают расчетов финансового ущерба от кибератак. У одной из трех по-прежнему отсутствует чрезвычайный план действий, даже несмотря на то, что кибератаки становятся обыденным делом. Обеспокоенность вызывает тот факт, что одна из четырех атак приводит к тому, что клиенты покидают подвергшуюся атаке организацию или подают на нее в суд.



### Безопасность по-прежнему «облачна»

Организации назвали неверную конфигурацию (26%) и уязвимости в приложениях (23%) как основные риски в облачной среде. Они также сообщили, что в 51% облачных приложений изменения вносятся еженедельно (увеличение на 16% по сравнению с 2016 годом). Частые изменения создают проблемы просматриваемости и контроля для специалистов по безопасности, особенно если четверть приложений – критические для бизнеса.

По мнению 46% организаций, наиболее распространенные проблемы безопасности при миграции приложений в облако – это контроль, управление и отсутствие просматриваемости. Далее идут отсутствие опыта и ноу-хау и дополнительная сложность управления политиками безопасности. Любопытно, что 51% пользователей облачных служб также надеются на системы защиты поставщиков облачных услуг и добавляют их в пакет, даже если эти поставщики не являются ориентированными на безопасность компаниями.



### Блокированный потенциал?

Блокчейн – горячая тема в сфере технологий, однако 36% респондентов признали, что не понимают его механизма. Только 10% считают, что блокчейн может повысить безопасность информации.



### Образование проваливает экзамены

Образование – вертикаль, наименее подготовленная к различным кибератакам. Уже второй год подряд этот сектор занимает последнее место.



### 72% не подготовлены к введению общих правил защиты данных

Почти три четверти организаций (72%) сообщают, что плохо готовы к введению общих правил защиты данных ЕС (GDPR). Шестнадцать процентов из этих респондентов вообще не знают, что такое GDPR.

Специалисты по безопасности могут использовать выводы и данные ежегодного *Глобального отчета о безопасности приложений и сетей* от Radware при анализе картины угроз и разработке стратегии безопасности для защиты своих предприятий. Поскольку киберагрессоры постоянно развиваются, ищут новые цели, методы и векторы атак, Radware также призывает организации быть на шаг впереди, воспользовавшись центром ресурсов по безопасности: [DDoSWarriors.com](http://DDoSWarriors.com).