Годовой отчет по безопасности
2015

Краткий обзор

Какой бы изменичивой ни была современная среда угроз, мы можем с уверенностью говорить о нескольких константах.

Современные хакеры неустанно ищут возможности преодолеть механизмы обнаружения и скрыть вредоносные действия. А тем временем службы информационной безопасности должны постоянно улучшать методы защиты организации и ее сотрудников от все более изощренных атак.

Между ними находятся обычные пользователи. Оказывается, они не только являются целью, но и могут поневоле стать соучастниками атак.

В *годовом отчете Cisco по безопасности за 2015 год*, в котором собраны результаты исследований и мнения сотрудников Cisco® Security Research и других экспертов компании, рассматривается непрерывная гонка между злоумышленниками и защитниками, на фоне которой пользователи становятся все более слабым звеном в системе безопасности.

Информационная безопасность — это обширная и сложная проблема, которая оказывает огромное влияние на пользователей, организации и правительства по всему миру. В *годовом отчете Cisco по безопасности за 2015 год* выделены четыре темы для обсуждения. На первый взгляд кажется, что эти разделы и рассматриваемые в них вопросы не имеют ничего общего, но при ближайшем анализе становится очевидна их взаимосвязь.

Четыре темы для обсуждения в *годовом отчете Cisco по безопасности за 2015 год*

1. **Аналитика угроз.**
2. **Сравнительное исследование возможностей систем безопасности, проведенное Cisco.**
3. **Геополитические и отраслевые тенденции.**
4. **Изменение взгляда на информационную безопасность — от пользователей до совета директоров.**

1. Аналитика угроз
В этом разделе представлен обзор исследования, проведенного компанией Cisco. Из него вы узнаете об эксплойтах, спаме, угрозах, уязвимостях и вредоносной рекламе. Также в отчете изучается роль пользователей в организации атак. В основе анализа тенденций 2014 года, проведенного Cisco Security Research, лежат телеметрические данные со всего мира. Сведения об угрозах, представленные в отчете, отражают результаты работы ведущих экспертов Cisco.

2. Сравнительное исследование возможностей систем безопасности, проведенное Cisco
Чтобы изучить восприятие состояния защиты в различных организациях, компания Cisco задала вопросы руководителям и специалистам по информационной безопасности в организациях разных масштабов из девяти стран относительно их ресурсов и процедур. Эти результаты вы можете прочитать только в *годовом отчете Cisco по безопасности за 2015 год*.

3. Геополитические и отраслевые тенденции
В этом разделе специалисты Cisco по безопасности и геополитике характеризуют текущие и новые геополитические тенденции, на которые организациям, особенно международным корпорациям, следует обратить пристальное внимание. В центре внимания – рост киберпреступности в зонах слабого контроля со стороны государства. Также здесь будут рассмотрены общемировые проблемы суверенитета, локализации, шифрования и совместимости данных.

4. Изменение взгляда на информационную безопасность – от пользователей до совета директоров
Специалисты Cisco по безопасности полагают, что организациям, которые хотят построить по-настоящему надежную систему безопасности в современных условиях, пора иначе взглянуть на вопросы информационной защиты. Во-первых, нужны более сложные инструменты управления безопасностью, чтобы защититься от угроз до, во время и после атаки. Во-вторых, необходимо поднять проблему информационной безопасности на уровень совета директоров. В-третьих, необходимо взять на вооружение манифест информационной безопасности Cisco – принципы, которые позволят реализовать более динамичный подход к защите, опережая на шаг злоумышленников.

Взаимосвязь тем, рассматриваемых в *годовом отчете Cisco по безопасности за 2015 год*, заключается в следующем. Злоумышленники становятся на удивление изобретательными, они научились использовать бреши в системе безопасности для маскировки вредоносной активности. Ответственность за защиту данных несут как специалисты по информационной безопасности, так и сами пользователи. Хотя многие защитники считают свои методы прекрасно оптимизированными, а инструменты безопасности эффективными, на самом деле их готовность противостоять угрозам наверняка оставляет желать лучшего. События в сфере геополитики – от изменения законов до появления новых угроз – могут напрямую влиять на бизнес и отношение организации к безопасности. Таким образом, организациям любого размера жизненно важно осознать, что безопасность касается непосредственно пользователей, что атак невозможно избежать и что пришло время найти новый подход к вопросам безопасности.

Основные выводы

Ниже приводятся основные выводы годового отчета Cisco по безопасности за 2015 год.

Злоумышленники стали изощреннее использовать недостатки систем безопасности, чтобы скрыть свои вредоносные действия.

- В 2014 году злоумышленники активно использовали 1 % критических общих уязвимостей и незащищенных мест (CVE). Это означает, что организации должны быстро устранить этот 1 % уязвимостей. Однако даже при использовании ведущих технологий безопасности требуется высокая эффективность процессов для устранения уязвимостей.
- С момента устранения угрозы эксплойт-кита Blackhole в 2013 году ни одному эксплойту не удалось добиться подобного успеха. Однако следует иметь в виду, что высшая строчка в рейтинге, возможно, уже не так притягательна для авторов эксплойтов, как раньше.
- Количество эксплойтов, атакующих Java, уменьшилось на 34 % вместе с улучшением защиты Java и появлением новых векторов атак.
- Вредоносные программы Flash теперь могут взаимодействовать с JavaScript, чтобы скрывать вредоносные действия, а также значительно затруднять их обнаружение и анализ.
- В период с января по ноябрь 2014 года объем спама увеличился на 250 %.
- Среди возникающих угроз можно отметить «спам на снегоступах», который отправляет небольшой объем нежелательных сообщений с большого количества IP-адресов, чтобы избежать обнаружения.

Пользователи и ИТ-специалисты невольно стали частью проблем безопасности.

- Интернет-преступники рассчитывают, что пользователи будут устанавливать вредоносные программы или помогать им использовать бреши в системе защиты.
- Heartbleed – опасная уязвимость OpenSSL. При этом, 56 % всех используемых версий OpenSSL старше 50 месяцев и, следовательно, все еще уязвимы.
- Безответственное поведение пользователей при использовании Интернета в сочетании с целевыми кампаниями, которые реализуют злоумышленники, подвергают многие отраслевые вертикали повышенному риску воздействия вредоносного ПО, распространяемого через Интернет. В 2014 году, по данным специалистов Cisco Security Research, фармацевтическая и химическая отрасли оказались лидерами с наибольшим риском воздействия вредоносного ПО, распространяемого через Интернет.
- Создатели вредоносного ПО используют расширения веб-браузера в качестве средства для распространения таких программ и нежелательных приложений. Такой подход к распространению вредоносного ПО оказался успешным для злоумышленников, так как многие пользователи привыкли доверять расширениям или просто считают их безвредными.

***Сравнительное исследование возможностей систем безопасности, проведенное Cisco*, показывает расхождение в оценке готовности к защите.**

- 59 % руководителей по ИТ-безопасности считают, что их процедуры защиты оптимизированы, той же точки зрения придерживаются 46 % менеджеров по операциям обеспечения безопасности.
- 75 % руководителей по ИТ-безопасности отзываются о своих средствах безопасности как об очень или исключительно эффективных. При этом, четверть из них указывает, что их средства эффективны до некоторой степени.
- 91 % респондентов из компаний со сложными системами безопасности, безусловно, согласны с тем, что руководители их компаний считают обеспечение безопасности приоритетной задачей.
- Менее 50 % респондентов использует такие стандартные средства, как исправления и настройки для предотвращения нарушений безопасности.
- Более крупные организации и компании среднего размера с большей степенью вероятности используют исключительно сложный анализ состояния защищенности в сравнении с организациями других размеров, рассматриваемых в исследовании.

Содержание

Злоумышленники против разработчиков систем безопасности: продолжающаяся гонка

Специалисты по информационной безопасности и интернет-преступники продолжают свою гонку на опережение, пытаясь обхитрить друг друга.

С точки зрения безопасности, очевидно, что организации улучшили свои позиции, приняв на вооружение более сложные средства для предотвращения атак и уменьшения их последствий. Они достаточно серьезно воспринимают необходимость мощного анализа состояния защищенности и уверены в том, что их процедуры защиты оптимизированы. Поставщики технологий также более внимательно подходят к обнаружению и устранению уязвимостей в своих продуктах, в результате чего злоумышленники имеют меньше возможностей для запуска эксплойтов.

Однако злоумышленники становятся более изощренными не только в своем подходе к запуску атак, но также и в уклонении от обнаружения.

- Они постоянно изменяют свою тактику и средства, исчезая из сети до того, как будут остановлены, или быстро выбирая другой метод проникновения.
- Преступники разрабатывают спам-кампании с использованием сотен IP-адресов в попытках обойти зарекомендовавшие себя продукты защиты от спама на основе IP-адресов.
- Они создают вредоносные программы на базе инструментов, которым доверяют пользователи или которые выглядят безвредными, чтобы закрепить эти программы в компьютерах и спрятать их на самом виду.
- Злоумышленники отыскивают новые уязвимости, если поставщики устраняют слабые места в других продуктах.
- Они пытаются добиться скрытого присутствия или растворяются в целевой организации, иногда затрачивая недели или месяцы для создания многочисленных плацдармов в инфраструктуре и пользовательских базах данных. И только при полной готовности они приступают к выполнению своей основной миссии.

Согласно данным нового *сравнительного исследования возможностей систем безопасности, проведенного Cisco* (см. стр. 24), специалисты по безопасности отмечают свой оптимизм и хорошую подготовку для отражения интернет-атак злоумышленников. Тем не менее преступники продолжают красть информацию, зарабатывать деньги на мошенничестве или нарушать работу сетей для достижения политических целей. В конце концов, обеспечение безопасности — это игра с числами. Даже если организации удается блокировать 99,99 % из миллиарда спам-сообщений, некоторые из них все же проникнут в систему. Способов обеспечить 100-процентную эффективность не существует.

Когда такие сообщения или эксплойты добираются до пользователей, именно сами пользователи становятся слабым звеном сети. Так как организации накопили опыт применения решений, блокирующих проникновение в сеть, вредоносное ПО и спам, злоумышленники могут задействовать пользователей, отправляя им фальшивые запросы на сброс пароля.

Поскольку пользователи становятся все более слабым звеном в цепочке безопасности, организациям приходится внимательнее выбирать технологии и политики безопасности. Не открывают ли организации новые лазейки для киберпреступников, в то время как разработчики пытаются сделать приложения и программное обеспечение более простыми в использовании? Жертвуют ли организации интересами пользователей, которым, по их мнению, нельзя доверять или которых невозможно обучить, применяя строгие меры безопасности, препятствующие нормальной работе пользователей? Пытаются ли организации рассказать пользователям о необходимости элементов управления безопасностью и ясно объяснить им их роль в обеспечении динамической защиты организации, которая поддерживает бизнес?

Принципы манифеста информационной безопасности Cisco, изложенные на странице 45, дают положительный ответ на последний вопрос. Технологические решения редко задействуют пользователей для управления безопасностью в качестве активных участников. Вместо этого такие решения вынуждают пользователей обходить средства обеспечения безопасности, которые мешают им работать, что уменьшает безопасность организаций. Сегодня вопрос, можно ли взломать сеть, утратил свою актуальность. Каждая сеть *будет* рано или поздно взломана. А что же в таком случае делать организациям? Если персонал безопасности знает, что сеть будет взломана, не будет ли он по-другому подходить к вопросам безопасности?

В *годовом отчете Cisco по безопасности за 2015 год* содержатся данные последних исследований специалистов группы Cisco Security Research. Группа анализирует достижения в области информационной безопасности, помогающие организациям и пользователям защититься от атак, а также рассматривает методы и стратегии, применяемые злоумышленниками для преодоления этой защиты. В отчете также содержатся основные выводы по результатам *Сравнительного исследования возможностей систем безопасности, проведенного Cisco,* в котором рассматривается анализ состояния защищенности организаций и их мнение о готовности к защите от атак. Кроме этого, в отчете обсуждаются следующие темы: геополитические тенденции, глобальные процессы, связанные с локализацией данных, польза более сложных элементов управления безопасным доступом, сегментация на основе ролевого доступа, а также важность переноса рассмотрения вопросов информационной безопасности на уровень совета директоров компаний.

1. Аналитика угроз

В этом отчете группа Cisco Security Research собрала и проанализировала информацию о безопасности на основе телеметрических данных со всего мира. Эксперты по безопасности Cisco регулярно изучают и анализируют вредоносный трафик и другие обнаруженные угрозы, что позволяет собрать сведения о возможном поведении преступников в будущем и помочь в выявлении угроз.

Веб-эксплойты: создатели эксплойт-китов считают, что высшая строчка в рейтинге не обязательно означает ваше превосходство

В деловом мире компании стремятся стать признанными лидерами. Но по данным специалистов Cisco Security Research, для авторов эксплойт-китов, действующих в так называемой теневой экономике, удержание четвертой или пятой позиции среди ведущих эксплойтов может стать еще более явным признаком успеха.

Как отмечается в *отчете Cisco по безопасности за первую половину 2014 года,* с конца 2013 года не наблюдается явный лидер среди эксплойт-китов[1]. Это произошло после того, как власти обезопасили широко используемый, хорошо поддерживаемый и высокоэффективный эксплойт-кит Blackhole после ареста его предполагаемого создателя и распространителя, известного как Paunch. Специалисты Cisco Security Research полагают, что основная причина отсутствия доминирующего эксплойт-кита в настоящее время состоит в том, что просто не появился другой, который бы стал бесспорным технологическим лидером среди конкурентов. Еще одна выявленная тенденция: с момента ареста хакера Paunch и обезвреживания Blackhole похоже, что больше пользователей эксплойт-китов стали инвестировать в технически сложные эксплойты с точки зрения их способности избегать обнаружения.

Согласно данным экспертов Cisco по вопросам информационной безопасности, в течение 2014 года наиболее часто наблюдалось использование следующих эксплойт-китов: Angler, Sweet Orange и Goon. В 2014 году чаще других обнаруживалось использование эксплойт-кита Angler. По неизвестным причинам эта тенденция особенно ярко проявила себя в августе. Специалисты Cisco Security Research объясняют популярность Angler решением его автора(-ов) отказаться от требования загружать исполняемый файл Windows для доставки вредоносной программы.

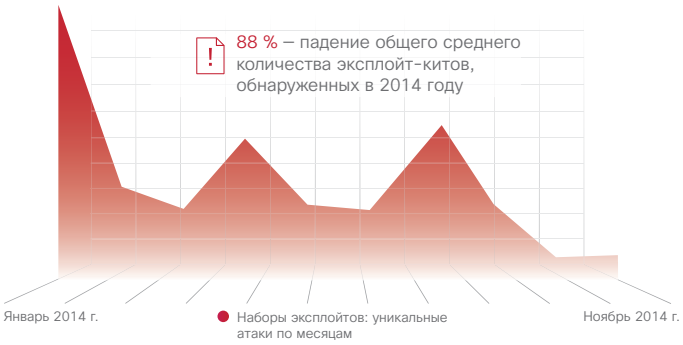
Исследователи Cisco считают, что способность эксплойт-кита Angler использовать уязвимости Flash, Java, Microsoft Internet Explorer (IE) и даже Silverlight требует к себе внимания. После запуска эксплойта содержимое вредоносного ПО записывается не на диск, а прямо в память с помощью такого процесса, как, например, iexplore.exe. Доставляемое Angler содержимое выглядит как BLOB-объект зашифрованных данных, что затрудняет его идентификацию и блокирование.

Подробнее об Angler, а также об использовании вредоносной рекламы в качестве основного способа доставки эксплойт-китов пользователям см. в публикации блога Cisco Security Angling for Silverlight Exploits (Ловим эксплойты Silverlight).

Эксплойт-кит Sweet Orange также отличается исключительной динамичностью. Его компоненты, порты и URL-адреса содержимого постоянно меняются, что позволяет Sweet Orange сохранять свою эффективность, избегая обнаружения. По мнению специалистов Cisco Security Research, эта особенность дает основание считать, что при сравнении с другими эксплойтами Sweet Orange с наибольшей степенью вероятности добьется успеха. Эксплойт-кит Sweet Orange внедряет ряд вредоносных программ в системы конечных пользователей, к которым не применены исправления, а также содержит эксплойты для уязвимостей в Adobe Flash Player, IE и Java. Злоумышленники, использующие Sweet Orange, часто рассчитывают на вредоносную рекламу, которая перенаправляет пользователей на веб-сайты, в том числе легитимные, с размещенными эксплойт-китами. Как правило, в ходе этого процесса пользователи перенаправляются не менее двух раз. Скомпрометированные веб-сайты с устаревшими версиями таких систем управления контентом, как WordPress и Joomla, часто становятся удобным местоположением для размещения эксплойт-кита Sweet Orange[2].

Что касается эксплойт-кита Goon, то, по мнению Cisco Security Research, вероятной причиной его скромной, но устойчивой популярности в 2014 году можно считать его надежность. Этот эксплойт также отличается наибольшей организованностью по сравнению с другими эксплойт-китами. Впервые открытый в 2013 году специалистами по информационной безопасности, эксплойт Goon, известный также как эксплойт-кит Goon/Infinity, представляет собой среду распространения вредоносного ПО, которая создает эксплойты для уязвимостей браузеров, имеющих отношение к компонентам Flash, Java или Silverlight на платформах Windows и Mac[3].

Рис. 1. Тенденции применения эксплойт-китов: количество уникальных атак, обнаруженных в период с января по ноябрь 2014 г.



Источник: Cisco Security Research

Прочитайте публикацию в блоге Cisco Security Fiesta Exploit Pack Is No Party for Drive-By Victims (Эксплойт-пакет Fiesta не доставляет радости случайно пострадавшим жертвам) и узнайте, как компании могут защититься от эксплойт-кита Fiesta. Этот набор доставляет вредоносное ПО через такие объекты, как Silverlight, и использует динамические DNS-домены (DDNS) в качестве целевых страниц эксплойта.

Подробнее об эксплойт-ките Nuclear и его возможностях получать доступ в систему пользователя для определения уязвимостей и доставки подходящих типов вредоносного ПО см. в публикации блога Cisco Security Evolution of the Nuclear Exploit Kit (Эволюция эксплойт-кита Nuclear).

Хотя общее количество обнаруженных эксплойт-китов упало на 87 % в месяцы после устранения Blackhole, летом 2014 года число эксплойтов, обнаруженных специалистами Cisco Security Research, увеличилось (см. рис. 1). В последние две недели августа они отметили значительное увеличение количества обнаружений, связанных с эксплойт-китом Angler. Однако к ноябрю общее количество обнаружений известных эксплойт-китов снова уменьшилось, причем Angler и Goon/Infinity по-прежнему проявляли себя чаще других. Общее среднее снижение количества эксплойт-китов, обнаруженных в период с мая по ноябрь 2014 года, составило 88 %.

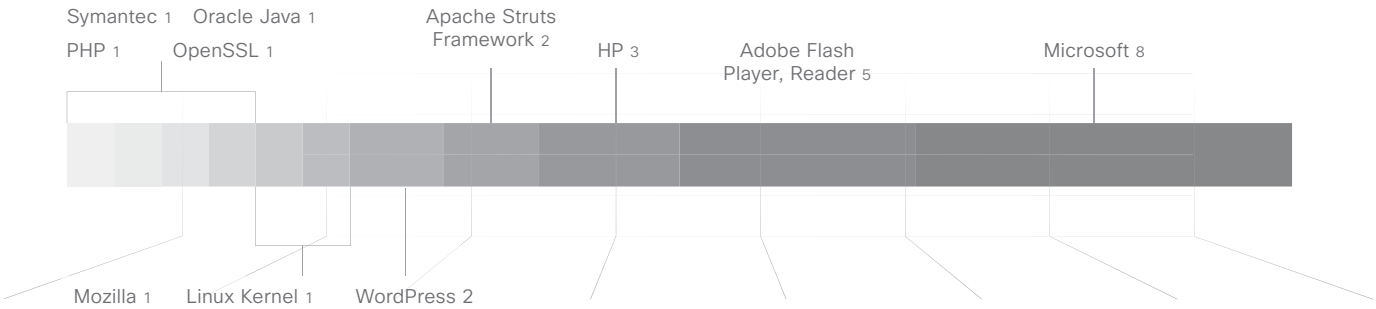
Угрозы и уязвимости: Java теряет свою привлекательность как вектор атак

В последние годы Java занимала незавидное ведущее место в списках наиболее распространенных и опасных уязвимостей. Однако согласно данным группы Cisco Security Research, похоже, что Java теряет популярность среди злоумышленников, которые стремятся найти максимально быстрый и простой, а также наименее обнаруживаемый способ для запуска эксплойтов.

Среди 25 оповещений о критических уязвимостях, имеющих отношение к поставщикам и продуктам, в период с 1 января по 30 ноября 2014 года только одно оповещение было связано с Java (см. «Общую систему оценки уязвимостей [CVSS]» в таблице 1 на стр. 10). В 2013 году группа Cisco Security Research зарегистрировала 54 новых критических уязвимостей Java. В 2014 году количество обнаруженных уязвимостей Java упало до 19. Однако это не должно уменьшить популярность и эффективность атак на эти более старые уязвимости, которые остаются и сегодня.

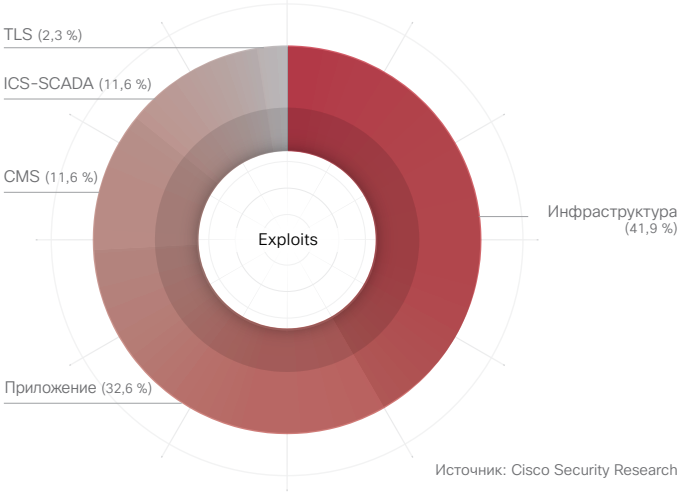
Данные из Национальной базы данных уязвимостей (NVD) также подтверждают аналогичное уменьшение. Согласно информации NVD в 2013 году было обнаружено 309 уязвимостей Java, а в 2014 году – 253 новые уязвимости Java. (Cisco Security Research отслеживает значительные уязвимости, которые получают высокую оценку по шкале CVSS. Этим объясняется меньшее количество, тогда как NVD помещает в отчет все обнаруженные уязвимости.) На рис. 2 указаны ведущие эксплойты уязвимостей по поставщикам и продуктам за 2014 год.

Рис. 2. Ведущие поставщики и эксплойты уязвимостей их продуктов



Источник: Cisco Security Research

Рис. 3. Ведущие категории продуктов, подвергшихся атакам эксплойтов



Источник: Cisco Security Research

Эксплойты с использованием уязвимостей на стороне клиента в Adobe Flash Player и Microsoft IE отобрали ведущее место у Java вместе с эксплойтами, нацеленными на серверы (например, эксплойты, использующие уязвимости в Apache Struts Framework, среде с открытым исходным кодом). Растущее количество эксплойтов Apache Struts Framework можно считать примером тенденции, когда преступники компрометируют онлайн-инфраструктуру для увеличения охвата и возможностей во время атак. Благодаря своей популярности Apache Struts Framework представляет собой логическую начальную точку для эксплойтов.

На рис. 3 показаны наиболее популярные категории продуктов, которые были атакованы эксплойтами в 2014 году.

По данным группы Cisco Security Research, в 2014 году наиболее часто подвергались атакам эксплойтов приложения и инфраструктура.

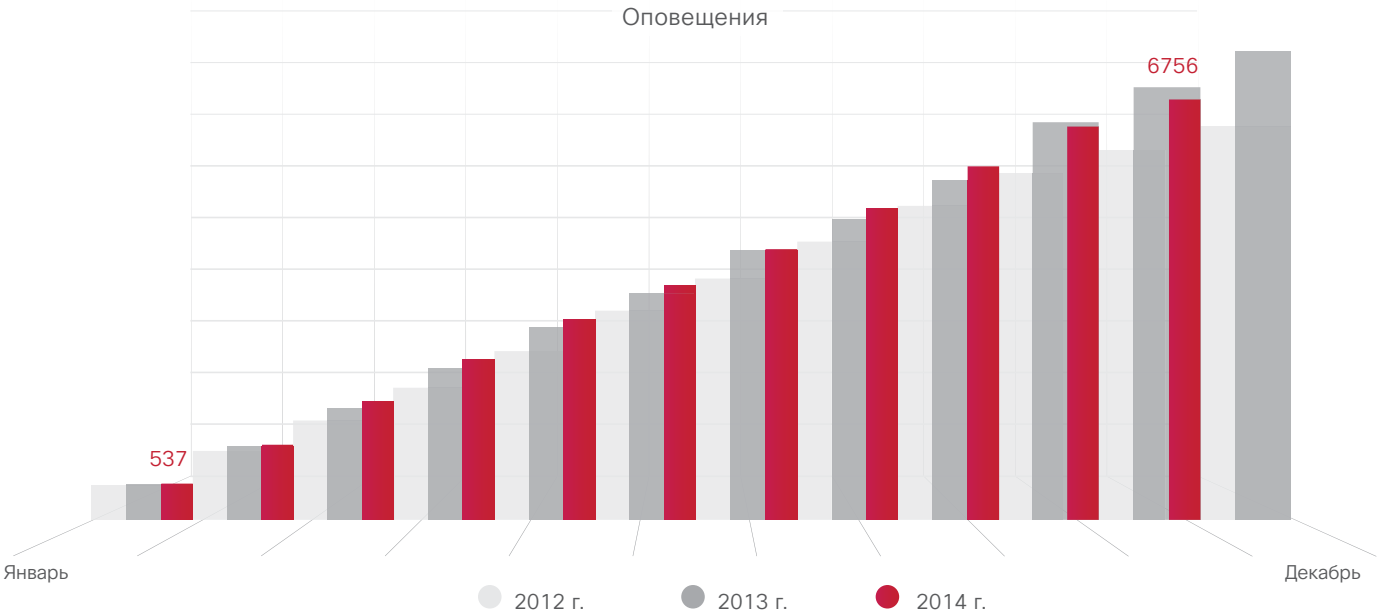
Системы управления контентом (CMS) также представляют собой предпочтительные цели. Злоумышленники рассчитывают на веб-сайты со старыми версиями CMS для упрощения доставки эксплойтов.

Совокупное количество оповещений уменьшилось

Общее количество оповещений за год, в число которых входят новые и обновленные уязвимости продуктов, обнаруженные в 2014 году и собранные Cisco Security Research, уменьшилось (рис. 4). По состоянию на ноябрь 2014 года общее количество оповещений снизилось на 1,8 % по сравнению с 2013 годом. Процент может показаться небольшим, однако впервые за последние несколько лет отмечается снижение количества оповещений по сравнению с предыдущим годом.

Наиболее вероятной причиной уменьшения считается растущее внимание к тестированию программного обеспечения и разработке со стороны поставщиков. Улучшенные жизненные циклы разработки, по всей вероятности, оказывают влияние на уменьшение количества уязвимостей, которые могут быть легко использованы преступниками.

Рис. 4. Совокупные показатели оповещений



Источник: Cisco Security Research

Поделиться отчетом

Таблица 1. Наиболее часто используемые уязвимости

Общая система оценки уязвимостей (CVSS)

IntelliShield ID	Заголовок	Срочность	Доверие	Степень важности	Базовое значение	Временное значение
33695	Уязвимость OpenSSL TLS/DTLS Heartbeat, утечка информации				5,0	5,0
35880	Уязвимость GNU Bash, обработка содержимого переменной окружения выполнение произвольного кода				10,0	7,4
35879	Уязвимость GNU Bash, обработка определений переменной окружения выполнение произвольного кода				10,0	7,4
36121	Уязвимость Drupal Core, внедрение SQL				7,5	6,2
32718	Уязвимость Adobe Flash Player, удаленное выполнение кода				9,3	7,7
33961	Уязвимость Microsoft Internet Explorer, выполнение кода удаленного объекта памяти				9,3	7,7
28462	Уязвимость Oracle Java SE, выполнение произвольного кода				9,3	7,7
30128	Уязвимость продуктов нескольких производителей, Struts 2 Action: внедрение команды обработки параметра				10,0	8,3

Источник: Cisco Security Research

Новые оповещения в сравнении с обновленными оповещениями

Количество новых оповещений в 2013 и 2014 годах показывает продолжающееся увеличение новых уязвимостей в отчетах в сравнении с предыдущими годами. Это означает, что поставщики, разработчики и исследователи проблем информационной безопасности находят, устраняют и заносят в отчеты больше новых уязвимостей в своих продуктах. Как видно на рис. 5, общее количество новых оповещений и общее количество за год в 2014 году равно уровню 2013 года или даже немного меньше его.

В таблице 1 показаны некоторых из наиболее часто используемых уязвимостей в соответствии с «Общей системой оценки уязвимостей (CVSS)». Национальная база уязвимостей (NVD), созданная Национальным институтом США по стандартам и технологиям (NIST), обеспечивает среду для распространения информации о характеристиках и воздействии уязвимостей в области ИТ, а также поддерживает CVSS. Показатель «срочности» в таблице CVSS указывает на активное использование этих уязвимостей, что соответствует показателю «временные» – индикатору активных эксплойтов. Помимо этого, предприятия путем сканирования списка продуктов, используемых злоумышленниками, могут определять, какие именно из этих продуктов используются злоумышленниками и, следовательно, подлежат мониторингу и исправлению.

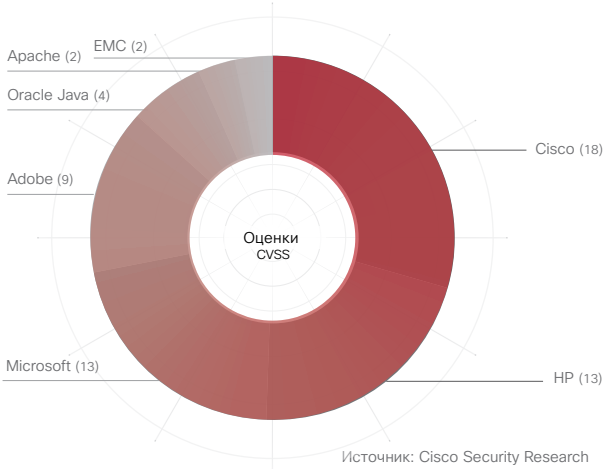
На рис. 6 указаны поставщики и продукты с наивысшими оценками CVSS. Cisco, используя оценки CVSS, указывает на существование кода эксплойта, подтверждающего концепцию. Однако при этом неизвестно, что код стал общедоступным.

Примечание: в таблице 1 указаны уязвимости, показавшие первоначальные признаки активности эксплойтов в период наблюдения. Большинство таких уязвимостей еще не вышли «на поток», то есть не были включены в число эксплойтов, предназначенных для продажи.

Рис. 5. Сравнение новых и обновленных оповещений

Источник: Cisco Security Research

Рис. 6. Поставщики и продукты с наивысшими оценками CVSS



Источник: Cisco Security Research

Поделиться отчетом

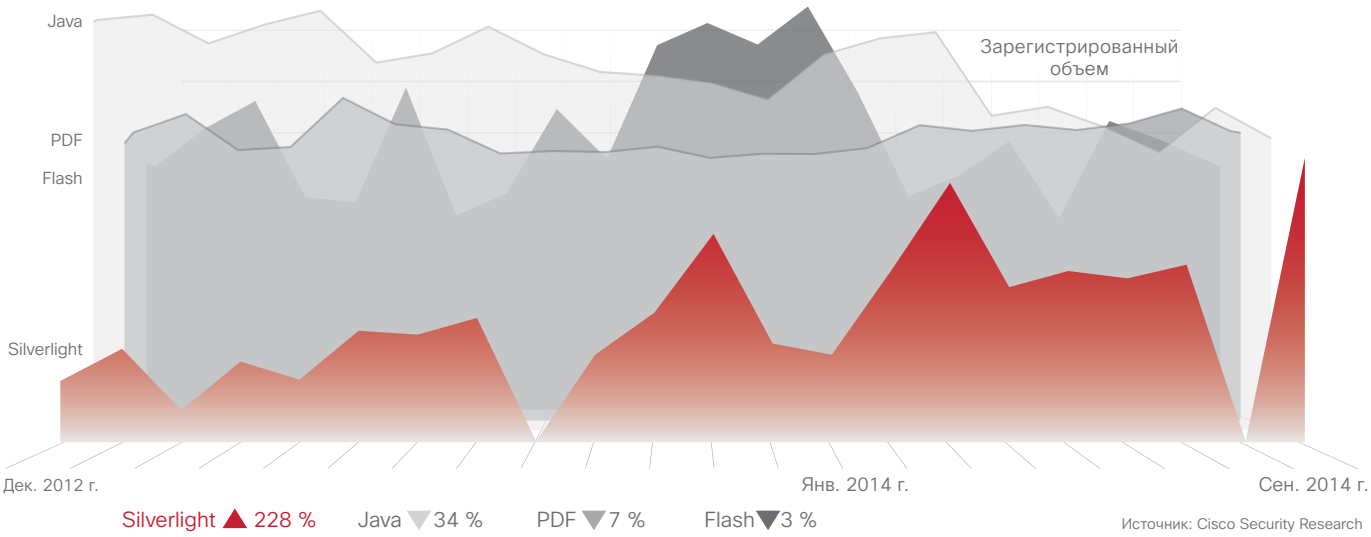
Анализ: вероятные факторы, подтверждающие потерю интереса к эксплойтам Java среди злоумышленников

Специалисты Cisco Security Research предполагают, что уменьшение количества эксплойтов Java может частично быть связано с отсутствием новых эксплойтов «нулевого дня», которые были бы раскрыты и доступны для использования злоумышленниками в 2014 году. Современные версии Java исправляются автоматически, а старые, более уязвимые версии Java Runtime Environment по умолчанию блокируются поставщиками браузеров. Apple даже предпринимает дополнительные меры для блокирования старых и уязвимых версий Java, а также для их исправления с помощью автоматических обновлений. Помимо этого, начиная с января 2013 года, Группа быстрого реагирования на компьютерные инциденты (US-CERT) рекомендует пользователям компьютеров обезопасить, заблокировать или удалить Java.

Последняя версия Java (Java 8) имеет более развитые элементы управления, чем предыдущие выпуски. Эту версию также труднее использовать, так как теперь она требует действий пользователя, например для подписи кода и для включения Java. Интернет-преступники нашли более доступные цели и обратили свое внимание на не имеющие отношения к Java векторы атак, которые обеспечивают более высокую рентабельность инвестиций. Например, многие пользователи не обновляют регулярно Adobe Flash и средства чтения PDF-файлов или браузеры, что дает преступникам более широкие возможности для использования как старых, так и новых уязвимостей. Согласно данным *отчета Cisco по безопасности за первую половину 2014 года,* количество эксплойт-китов, с учетом эксплойтов Microsoft Silverlight, возрастает[4].

На рис. 7 показано, что лидирующее положение Java как вектора атак устойчиво снижается в рамках тенденции, которая наблюдается вот уже более года. Использование Flash для запуска эксплойтов было в некоторой степени хаотично с максимальным всплеском в январе 2014 года. Использование PDF оставалось на постоянном уровне, так как многие злоумышленники, по всей вероятности, уделяли основное внимание запуску узких целевых кампаний с помощью сообщений электронной почты с вложенными PDF-файлами. Количество атак на Silverlight, все еще незначительное в сравнении с более традиционными векторами, продолжает возрастать, особенно начиная с августа.

Рис. 7. Сравнение тенденций изменения объема по векторам атак



Flash и JavaScript: лучше вместе?

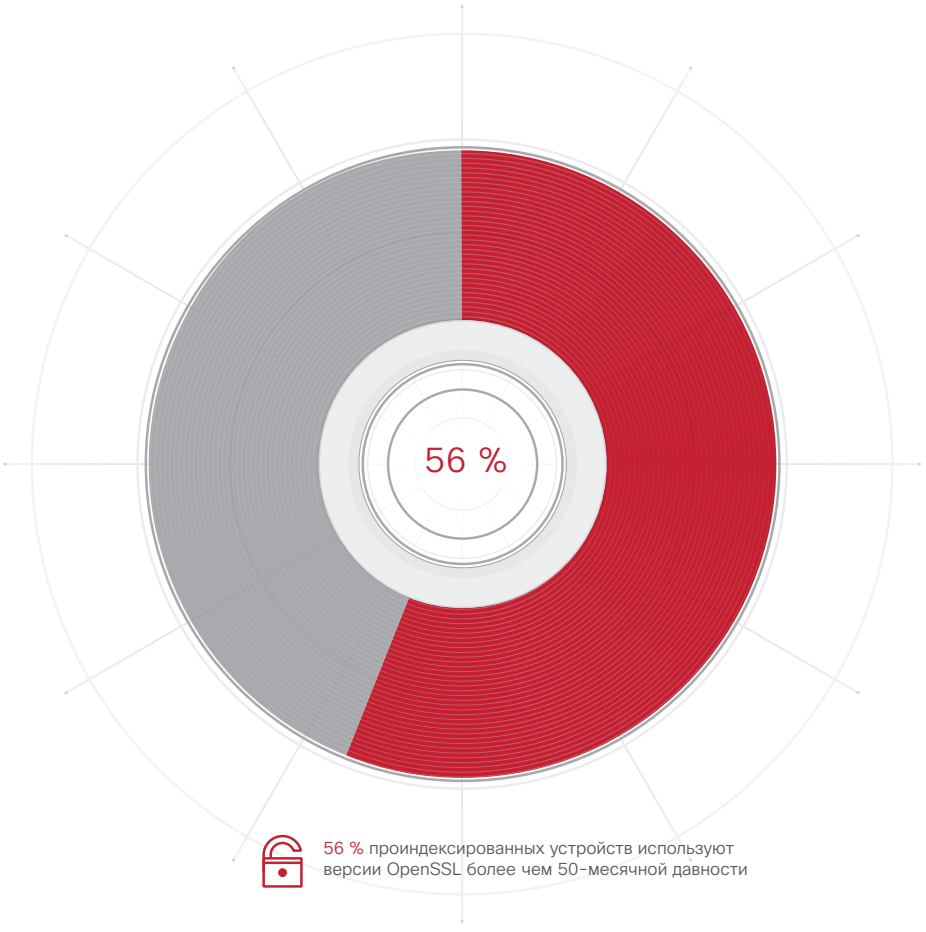
В 2014 году группа Cisco Security Research наблюдала рост использования вредоносных программ Flash, которые взаимодействовали с JavaScript. Эксплойт совместно используется двумя различными файлами – одним Flash и одним JavaScript. Совместное использование эксплойтов в двух различных файлах и форматах затрудняет устройствам обеспечения безопасности их обнаружение и блокирование, а также анализ с помощью средств реконструирования. Такой подход позволяет злоумышленникам совершать более эффективные и результативные атаки. Например, если первый этап атаки выполняется полностью в JavaScript, то второй этап, передача содержимого, не начнется до успешного завершения JavaScript. Таким образом, только пользователи, которые могут запустить вредоносный файл, получают содержимое.

Археология уязвимостей: опасности, связанные с устаревшим программным обеспечением, и причины, по которым исправления нельзя считать единственным решением

Как уже пояснялось при обсуждении уязвимостей (см. стр. 8), злоумышленники выбирают простейший доступный путь при определении, каким образом и где их эксплойты смогут добиться успеха. Они выбирают продукты, предлагающие больше возможностей с точки зрения поверхности атак. Такие возможности обыкновенно создаются при использовании неисправленного или старого программного обеспечения. Например, исправление устройств по-прежнему представляет собой серьезную проблему, так как многие системы все еще уязвимы для атак SSL Poodle[5]. Изучив тенденции, специалисты Cisco Security Research пришли к мнению, что распространение старых версий исполняемого программного обеспечения продолжит приводить к серьезным проблемам с информационной безопасностью.

Группа Cisco Security Research использовала модули проверки для анализа устройств, подключенных к Интернету и использующих OpenSSL. Группа обнаружила, что в 56 % проверенных устройств использовались версии OpenSSL старше 50 месяцев. Это означает, что, несмотря на широкую информацию об эксплойте Heartbleed[6], обнаруженные в 2014 году бреши в системе безопасности при обработке протокола Transport Layer Security (TLS) и срочную потребность выполнить обновление до последней версии программного обеспечения OpenSSL для устранения таких уязвимостей, организациям не удается обеспечить использование новейших версий. На рис. 8 показан возраст версий OpenSSL.

Рис. 8. Возраст версии OpenSSL



Источник: Cisco Security Research

Возможные решения: автоматические обновления и исправления

Более широкое применение автоматических обновлений может быть одним из решений проблем, связанных с устаревшим программным обеспечением. Группа Cisco Security Research проанализировала данные устройств, которые были подключены к Интернету и в которых использовался браузер Chrome или IE. Полученные данные показали, что 64 % запросов Chrome поступало от последней версии этого браузера. Что касается пользователей IE, то только 10 % запросов поступало от новейшей версии.

Специалисты Cisco Security Research считают, что система автоматических обновлений Chrome более успешно справляется с обеспечением максимально возможного количества пользователей самой последней версией программного обеспечения. (Кроме того, возможно, что пользователи Chrome имеют более глубокие технические знания, чем пользователи IE, и более склонны обновлять свои браузеры и устанавливать обновления.)

С учетом сокращения количества уязвимостей Java и их использования исследование ясно показывает, что программное обеспечение с автоматической установкой обновлений имеет преимущества при создании более защищенной среды безопасности. Чтобы исключить неизбежный риск в результате ручных процессов обновления, вероятно, организациям стоит смириться со случайными сбоями и несовместимостью, связанными с автоматическими обновлениями.

Отчет о рисках для отраслевых вертикалей: выбор цели злоумышленниками и безответственный подход пользователей – опасная комбинация для компаний в отраслях с высоким уровнем риска

В 2014 году фармацевтическая и химическая отрасли оказались лидерами с наибольшим риском встречи с вредоносным ПО, распространяемым через Интернет. В первой половине года это место принадлежало СМИ и издательской отрасли, но они переместились на второе место к ноябрю. Завершают лидирующую пятерку производство, транспорт, перевозки, а также авиация, занявшие соответствующие места. Все эти отрасли попали в ведущую пятерку в первой половине 2014 года.

Хотя можно было бы ожидать более высокое место от розничной торговли в этом списке с учетом недавних, широко известных атак, которые охватили отрасль, следует иметь в виду, что при создании рейтинга принимается в расчет показатель встречаемости вредоносного ПО, а не фактические нарушения безопасности.

Чтобы определить показатели встречаемости вредоносного ПО по секторам, исследователи Cisco Security Research сравнили усредненные показатели по всем организациям и по компаниям определенного сектора. При этом учитывались только предприятия, которые используют сервис Cisco Cloud Web Security (рис. 9). Показатели встречаемости в отрасли, превышающие 1 %, отражают повышенный риск встречи вредоносного ПО в сети, в то время как показатели ниже 1 % говорят о сниженном риске. Например, риск компании с показателем встречаемости 1,7 на 70 % выше среднего. Напротив, риск компании с показателем встречаемости 0,7 на 30 % ниже среднего.

Встречи в сравнении со взломом

Под встречей понимается случай блокирования вредоносного ПО. В отличие от взлома, оборудование в случае встречи не заражается, поскольку двоичный код не загружается.

Рис. 9. Риск встречи с вредоносными веб-приложениями в отраслевых вертикалях, все регионы, период с 1 января по 15 ноября 2014 г.

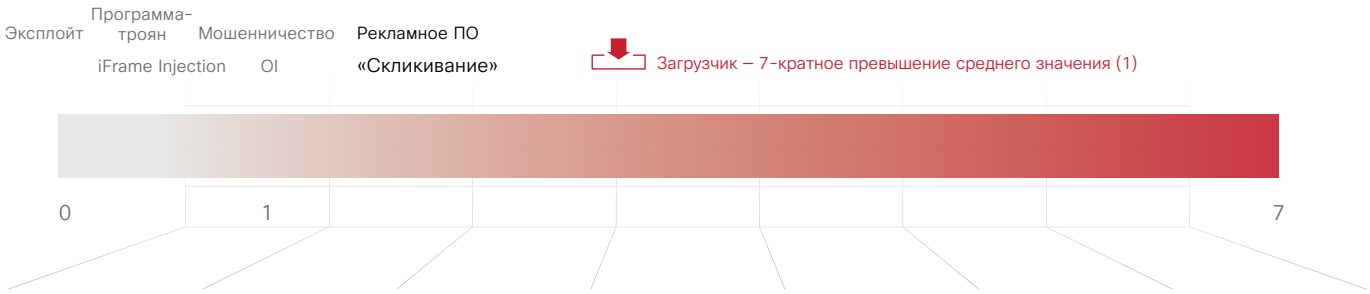
Источник: Cisco Security Research

Специалисты Cisco Security Research проанализировали восемь методов атак (рис. 10) с целью выяснить, что в наибольшей мере способствует увеличению риска встречи с вредоносным ПО в отраслевой вертикали: выбор цели злоумышленниками или способы использования Интернета пользователями. Они увидели идеальный шторм. Комбинация методов целевых атак и безответственного поведения пользователей в Интернете влияла на уровень риска.

Чтобы определить наличие фактической разницы между поведением пользователей в вертикали с высоким и низким уровнем риска, специалисты Cisco Security Research проанализировали четыре метода ненаправленных, нецелевых атак, с которыми пользователи часто встречаются во время работы в Интернете: рекламное ПО, ложные клики, мошенничество и внедрение iFrame. Специалисты также рассмотрели четыре типа более сложных атак, которые злоумышленники часто используют в целевых кампаниях: эксплойт, троян, OI (обнаружение вредоносного ПО) и загрузчик.

Примечание. Специалисты Cisco Security Research распределили восемь методов атак по эвристическим корзинам.

Рис. 10. Методы атак с использованием вредоносного ПО, распространяемого через Интернет: сравнение первых четырех и последних четырех вертикалей с высоким уровнем риска



Источник: Cisco Security Research

Используя первые четыре и последние четыре вертикали с наибольшим риском воздействия вредоносного ПО согласно данным Cisco Cloud Web Security, специалисты Cisco Security Research определили процент для каждого метода атаки и вывели средние показатели для первых четырех и последних четырех вертикалей. Сравнительные данные на рис. 10 были получены путем деления среднего значения для первых четырех на среднее значение для последних четырех. Соотношение, равное единице, показывает, что наблюдаются одни и те же шаблоны действия для групп объектов, наиболее и наименее предпочтительных в качестве цели атаки.

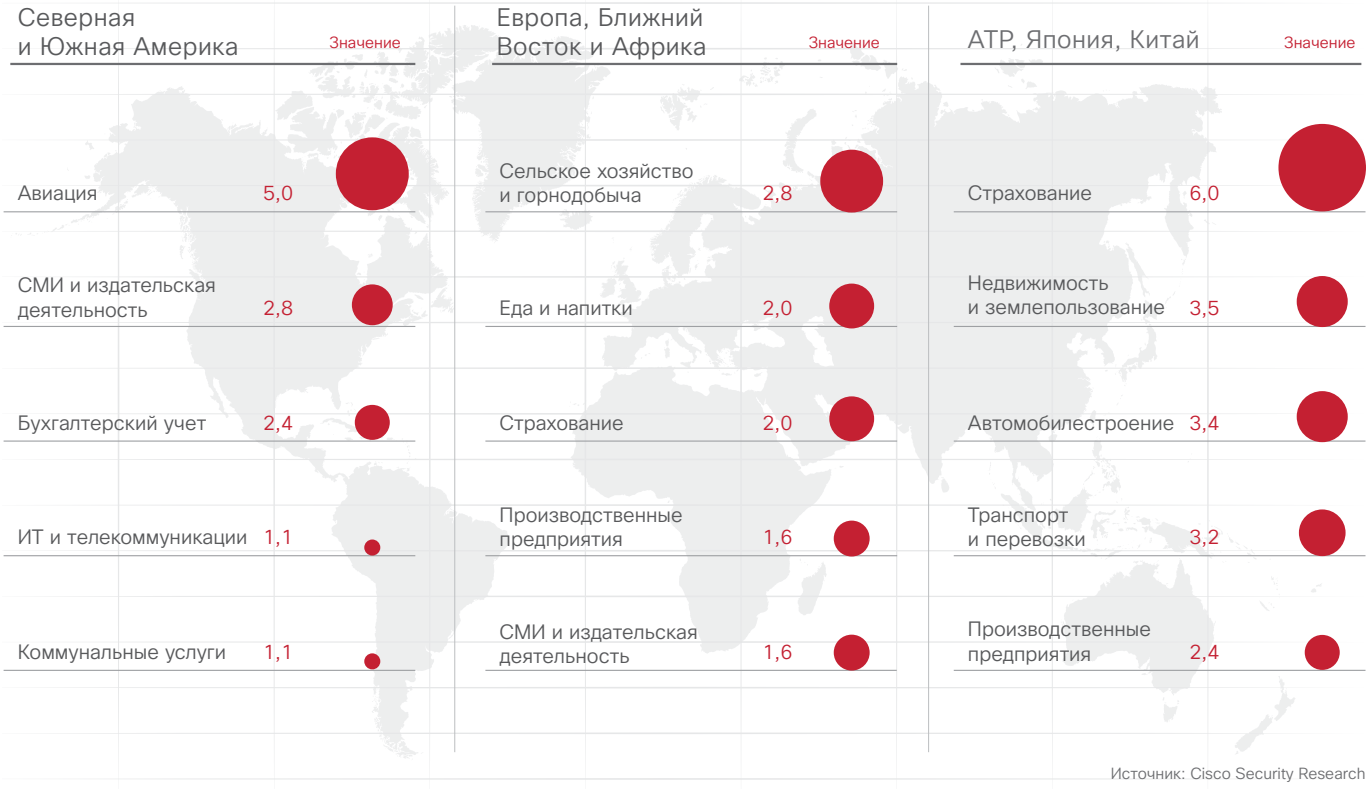
Данные указывают, что отраслевые вертикали с наиболее высоким риском встречаются со сложными методами атак, при которых используются загрузчики. При этом, частота встречи с такими методами атак в семь раз выше, чем у последних четырех отраслевых вертикалей с высоким уровнем риска. Этот результат соответствует тому, что можно было бы ожидать при реальных целевых методах атаки на вертикали с высоким уровнем риска.

Частота встреч с ложными кликами и рекламным ПО в целевых отраслевых вертикалях с высоким уровнем риска также выше в сравнении с вертикалями с более низким уровнем риска. Отсюда следует вывод, что различия могут объясняться более сложными причинами, чем просто выбор цели злоумышленниками. Поведение пользователей также может повышать риск встречи с вредоносным ПО. Возможно, это объясняется различиями во взаимодействии пользователей с Интернетом, а также их привычками при просмотре веб-сайтов. В результате пользователи вносят свой вклад в увеличение частоты встреч с атаками, в которых используется распространение вредоносного ПО через Интернет, в отраслевых вертикалях с высоким риском. Кроме того, пользователи в отраслях, где для обеспечения конкурентоспособности и инноваций поощряется быстрая адаптация к новым мультимедийным средствам, чаще встречаются с атаками на основе распространения вредоносного ПО через Интернет. В то же время пользователи в других отраслях, например в государственных органах, где использование Интернета ограничено или строго контролируется, реже встречаются с такими методами атак.

Например, специалисты Cisco Security Research считают, что из-за более интенсивного использования Интернета в СМИ и издательствах они подвергаются риску встречи с веб-эксплойтами чаще, чем пользователи в других отраслевых вертикалях.

Примечание. В 2014 году СМИ и издательства подвергались значительно более высокому, чем обычно, риску встречи с вредоносным ПО, распространяемым через Интернет. Группа Cisco Security Research, которая собирает подобные данные с 2008 года, ранее не сталкивалась с такими результатами. Одним из факторов этого явления можно считать более широкое воздействие вредоносного ПО на пользователей при посещении легитимных веб-сайтов.

Рис. 11. Вертикали с самым высоким уровнем риска воздействия вредоносного ПО в регионах: AMER, APJC и EMEA



Источник: Cisco Security Research

Встречаемость вредоносного ПО по регионам

Ниже приводятся данные, имеющие отношение к риску встречи с вредоносным ПО, распространяемым через Интернет, для отраслевых вертикалей с высоким уровнем риска в зависимости от региона. Выделяются следующие три региона:

- Северная, Центральная и Латинская Америки (AMER).
- Азиатско-Тихоокеанский регион, Китай, Япония (APJC).
- Африка, Европа и Ближний Восток (EMEA).

Специалисты Cisco Security Research определили локализованные отраслевые вертикали с наивысшим уровнем риска (см. перечисленные отрасли на рис. 11) в разных регионах мира и установили следующее.

- Пользователи в отрасли страхования из региона APJC с большей в шесть раз вероятностью подвержены риску воздействия вредоносного ПО в сравнении с 12 вертикалями, которые были проанализированы во всех трех регионах. (Средний базовый уровень: 1,5.)
- Пользователи в авиационной отрасли из региона AMER с большей в пять раз вероятностью подвержены риску воздействия вредоносного ПО.
- Пользователи в отрасли недвижимости и управления землей из региона APJC, а также пользователи в автомобильной отрасли из этого региона с большей в 3,5 раза вероятностью подвержены риску воздействия вредоносного ПО.
- Пользователи в отрасли транспорта и перевозок из региона APJC с большей в 3,25 раза вероятностью подвержены риску воздействия вредоносного ПО.

Cisco Security Research отмечает резкий рост цен на землю и жилье, недавние стихийные бедствия, а также высокую экспортную и производственную активность в регионе APJC как факторы, влияющие на целевые атаки злоумышленников в этом регионе. При этом, речь в первую очередь идет о пользователях, которые работают или ведут бизнес в следующих отраслях: автомобилестроение, страхование, недвижимость и управление землей, транспорт и перевозки. Кражи клиентских данных, интеллектуальной собственности (в том числе выбор в качестве цели определенных государств), а также данные по грузовым авиаперевозкам, вероятно, можно считать основными факторами выбора в качестве цели пользователей в авиационной отрасли из региона AMER.

Методы атак с целью распространения вредоносных программ (по регионам)

На рис. 12a–12c показаны методы распространения вредоносных программ, которые наиболее часто используются злоумышленниками (по регионам). Данные на этих диаграммах представлены в основном с учетом местоположения обнаруженных блоков вредоносного ПО (т. е. встречаемости) в соответствии с данными, предоставленными Cisco Cloud Web Security, в сравнении с типами угроз в сети Интернет.

В течение 2014 года пользователи в регионе AMER (Северная и Южная Америка) были атакованы преимущественно вредоносными скриптами; внедрение плавающего фрейма (iframe) оказалось на втором месте с существенным отставанием. В регионе APJC (АТР, Япония, Китай) злоумышленники в прошлом году особенно часто использовали мошенничество, вредоносные скрипты и эксплойты на основе веб-интерфейса для взлома во всех вертикалях. А в регионе EMEA (Европа, Ближний Восток и Африка) преобладали эксплойты на основе веб-интерфейса.

Прочитайте публикацию в блоге Cisco Security Threat Spotlight: Group 72, чтобы узнать о роли подразделения Cisco Security Research в выявлении и пресечении действий группы злоумышленников, направленных на широко известные организации, которые владеют ценной интеллектуальной собственностью в производственной, промышленной, аэрокосмической, оборонной сферах и СМИ.

Подробнее об инструменте Remote Administration Tool (RAT), который «Группа 72» использовала для кибершпионажа, см. в публикации "Threat Spotlight: Group 72, Opening the ZxShell".

Рис. 12a. Распределение методов атак, AMER

Метод атаки	Всего, %
Скрипт	24,93
iFrame Injection	17,43
Эксплойт	13,63
OI (обнаруживающее вредоносное ПО)	10,35
Троян	10,06

Источник: Cisco Security Research

Рис. 12b. Распределение методов атак, APJC

Метод атаки	Всего, %
Мошенничество	25,26
Скрипт	25,04
iFrame Injection	18,68
OI (обнаруживающее вредоносное ПО)	9,93
Эксплойт	6,72

Источник: Cisco Security Research

Рис. 12c. Распределение методов атак, EMEA

Метод атаки	Всего, %
Внедрение iFrame	51,48
Скрипт	15,17
Эксплойт	8,64
Мошенничество	7,31
OI (обнаруживающее вредоносное ПО)	4,16

Источник: Cisco Security Research

Рис. 13. Объем «спама на снегоступах» растет

Источник: Cisco Security Research

Новые способы рассылки спама: спамеры применяют стратегию «спама на снегоступах»

Фишинг часто используется злоумышленниками как инструмент доставки вредоносных программ и кражи учетных данных, поскольку пользователи по-прежнему часто становятся жертвой известных тактик спамеров. Злоумышленники осознали, что зачастую проще добираться до пользователей через браузер и по электронной почте, а не взламывать серверы. Это означает, что спамеры продолжают внедрять инновации.

Нет ничего необычного в том, что система защиты от спама перехватывает более 99 % проходящего через нее спама. А большинство самых лучших систем защиты от спама отфильтровывает свыше 99,9 % нежелательных писем. В такой среде спамеры просто стараются каким-либо способом обойти фильтры нежелательной почты. Чтобы спам гарантированно достигал своей целевой аудитории, спамеры все шире используют такие методы, чтобы избежать обнаружения системами защиты от спама, проверяющими репутацию на основе IP-адреса.

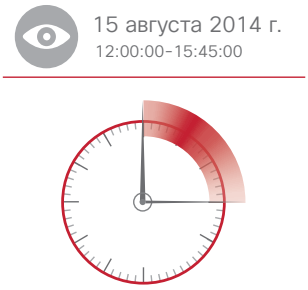
О «спаме на снегоступах». Это очень выразительное сравнение, ведь снегоступы позволяют идти по глубокому снегу, не проваливаясь в него, поскольку вес человека равномерно распределяется по большой площади. «Спам на снегоступах» — это массовая рассылка нежелательной электронной почты с большого количества IP-адресов при низком объеме сообщений, отправленных с одного IP-адреса. Это позволяет исключить обнаружение со стороны некоторых систем защиты от спама. Рис. 13 демонстрирует рост объема «спама на снегоступах» с 2013 по 2014 г.

В недавней кампании по рассылке «спама на снегоступах», которую исследовали сотрудники Cisco Security Research, была применена тактика блиц-крига. Это означает, что вся кампания по рассылке спама проходила в течение всего трех часов, но в некоторый момент ее объем составлял до 10 % глобального трафика спама (рис. 14).

Чтобы узнать подробнее о «спаме на снегоступах», читайте публикацию в блоге Cisco Security "Snowshoe Spam Attack Comes and Goes in a Flurry" .

Исследователи Cisco проверили сообщения из этой рассылки «спама на снегоступах» и выявили некоторые стандартные признаки спама. Например, в них были строки темы с опечатками, например inovice 2921411.pdf, и они содержали номера, сгенерированные случайным образом. В качестве приложений использовались обычно PDF-файлы, содержащие трояны, которые эксплуатируют уязвимости в Adobe Reader.

Рис. 14. Кампания по рассылке «спама на снегоступах»



Источник Cisco Security Research

Чтобы снизить воздействие «спама на снегоступах», специалисты по безопасности не могут полагаться на решения на основе репутации, поскольку одни и те же сообщения в кампании могут отправляться с сотен и даже тысяч адресов (в случае кампаний, которые проводятся с помощью ботнетов). Исследование других признаков спама, таких как гигиена почтового сервера, может обеспечить более точное распознавание. Например, в кампаниях, которые исследовали сотрудники Cisco Security Research, для некоторых IP-адресов отсутствует соответствие прямой и обратной зоны в системе доменных имен (DNS). Это обычно рассматривается как очевидный индикатор того, что почтовый сервер не является проверенным и безопасным.

У некоторых таких IP-адресов отсутствовали записи об отправке сообщений электронной почты перед началом кампании по рассылке «спама на снегоступах». Это еще раз доказывает, что интернет-преступники используют взломанные компьютеры, чтобы создать инфраструктуру для «спама на снегоступах».

Рис. 15. Объемы спама по странам

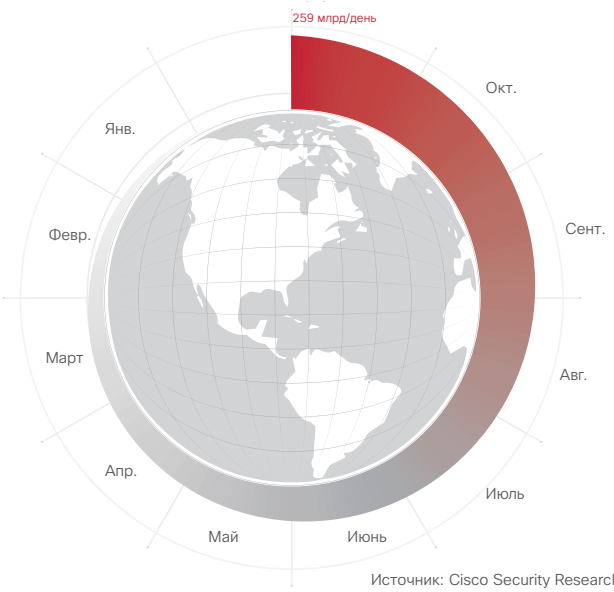
Источник: Cisco Security Research

Спамеры расширяют свою тактику, чтобы обмануть потребителей

Объемы спама в мире неуклонно растут. Это значит, что этот способ атаки киберпреступники по-прежнему считают перспективным (рис. 16). Злоумышленники постоянно меняют свои сообщения, чтобы убедить получателей пройти по опасной ссылке, зачастую используя приемы социальной инженерии.

В то время как в 2014 году объем спама в США в целом снизился, в других странах в тот же период эти показатели росли (рис. 15). Исследователи Cisco Security Research полагают, что причиной тому стало смещение зоны интересов злоумышленников. Рост объемов спама в некоторых странах может указывать на то, что злоумышленники в других регионах переняли приемы распространения спама у своих «коллег» из США, ведь именно Штаты ранее были основным источником спама. Однако США завершили этот год с более высокими показателями.

Рис. 16. Рост объемов спама по всему миру в 2014 г.



Источник: Cisco Security Research

Фишинговые сообщения, которые долгие годы кормили интернет-преступников, развились до такого уровня, когда даже опытные конечные пользователи с трудом выявляют фейковые письма среди настоящих. Эти искусно составленные сообщения, адресованные конкретным лицам, приходят якобы от широко известных поставщиков услуг или провайдеров, от которых пользователи обычно получают сообщения. Это могут быть службы доставки, сайты интернет-торговли, поставщики музыки и других развлечений. Электронные письма с хорошо известными названиями и логотипами, даже если они подделаны, приобретают большее значение, чем обычный спам с рекламой лекарств или часов. А если в сообщении есть интерактивный элемент, знакомый получателям, такой как уведомление о недавнем заказе или номер отслеживания в системе доставки, пользователи будут еще больше склоняться к тому, чтобы нажимать ссылки в электронном письме.

Специалисты Cisco Security Research недавно исследовали небольшую подборку нацеленных на конкретного пользователя фишинговых сообщений, которые якобы исходили от корпорации Apple и утверждали, что получатели загрузили популярную игру для мобильных устройств iOS. Строка темы электронной почты содержала случайный номер квитанции и другие кажущиеся подлинными детали. Ссылка в сообщении электронной почты предлагала получателям войти в систему и поменять пароль, если они еще не инициализировали загрузку игры. И эта ссылка перенаправляла пользователя на известный фишинговый веб-сайт.

Спамеры видоизменяют сообщения, чтобы избежать обнаружения

Когда спамеры находят формулу успеха (под этим подразумевается, что они могут убедить пользователей нажимать ссылки в спам-сообщениях или приобретать несуществующие продукты), они будут видоизменять сообщения, не затрагивая их основной структуры. Но эти сообщения имеют достаточную степень различия, чтобы обходить спам-фильтры, по крайней мере, на короткое время. В таблице 2 показано, сколько раз в течение исследуемого периода времени спамеры пытались изменять содержимое сообщения, чтобы избежать текущих мер по устранению угроз. В этой таблице перечислены угрозы, которые потребовали изменения правил для Cisco Email Security Appliance (ESA).

Таблица 2. Оповещения об угрозах: самые устойчвые угрозы спама и фишинга

IntelliShield ID	Заголовок	Version	Urgency	Credibility	Severity
24986	Оповещение об угрозе: фальшивое уведомление об отправке FedEx	95			
31819	Оповещение об угрозе: фальшивое сообщение о доставке факса	88			
30527	Оповещение об угрозе: вредоносное вложение в виде личных изображений	81			
36121	Оповещение об угрозе: фальшивое сообщение об отмене электронного платежа	80			
23517	Оповещение об угрозе: фальшивое сообщение о заказе продукта	79			
23517	Оповещение об угрозе: фальшивое вложение в виде счета	78			
27077	Оповещение об угрозе: фальшивое уведомление о денежном переводе	78			
26690	Оповещение об угрозе: фальшивое уведомление о платеже банка	78			

Источник: Cisco Security Research

Вредоносная реклама через расширения браузера: небольшой ущерб из расчета на пользователя с идеей получения большой прибыли

Недавно сотрудники Cisco Security Research провели глубокий анализ вредоносной рекламы, которая использует браузерные расширения для распространения вредоносных программ и нежелательных приложений. Они выяснили, что эта угроза имела характеристики, напоминающие поведение ботнетов. Проведя исследование, которое включало проверку действий более 800 000 пользователей из 70 компаний в период с 1 января по 30 ноября 2014 года, специалисты Cisco Security Research измерили общий объем угроз и выявили их назначение и структуру.

Анализ показал, что число зараженных браузерных расширений гораздо выше предполагаемого и что создатели вредоносных программ используют сочетание очень сложного, профессионального кода и отточенных бизнес-моделей, чтобы длительное время поддерживать доходность своих операций. Другими словами, полное управление целевым хостом не обязательно для успешной монетизации. Это приводит к увеличению случаев поражения вредоносными программами, разработанными специально для снижения воздействия на затрагиваемый хост и оптимизации с целью долговременной монетизации, охватывающей широкую популяцию затронутых компьютеров.

Пользователи заражаются такими вредоносными браузерными расширениями, устанавливая комплекты ПО (то есть ПО, распространяемого вместе с другим программным пакетом или продуктом) и обычно без явного согласия пользователя. Такие приложения, как инструменты PDF или видеопроигрыватели, пользователи загружают из непроверенных источников и устанавливают осознанно. Они верят в то, что эти программы исходят из законных источников.

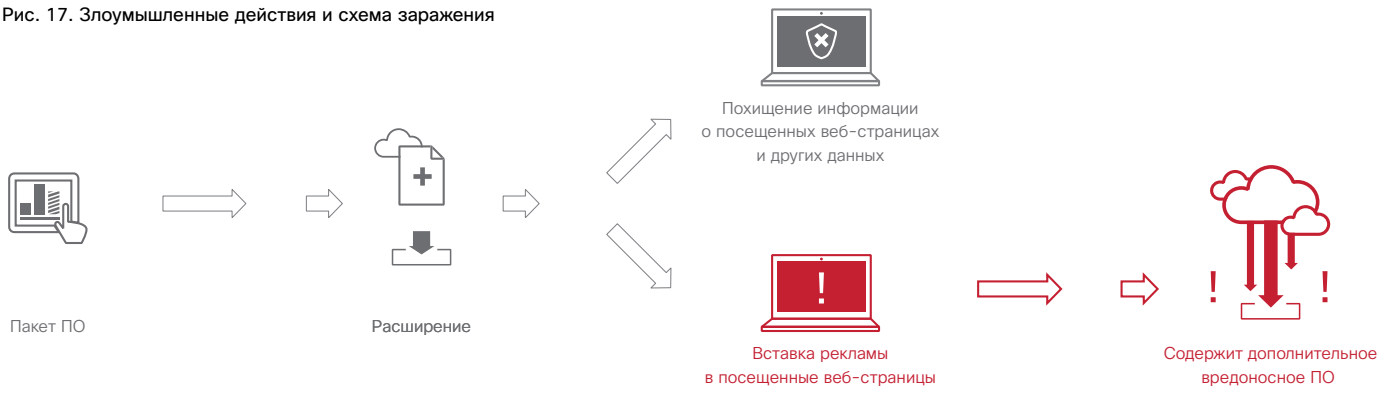
Такие приложения могут оказаться в одном комплекте с нежелательными или вредоносными программами. Этот подход к распространению вредоносных программ использует схему монетизации с оплатой за установку (PPI), при которой издатель получает плату за каждую установку программного обеспечения в комплекте с фирменным приложением.

Многие пользователи доверяют расширениям так же, как и браузерам, или просто считают их безвредными, поэтому такой подход к распространению вредоносных программ приносит успех их создателям. Этот метод распространения вредоносных программ позволяет злоумышленникам снизить зависимость от других технологий, таких как наборы эксплойтов, которые могут быть обнаружены с большей вероятностью. (См. «Веб-эксплойты: создатели эксплойт-китов считают, что лидирующая позиция не обязательно означает ваше превосходство», стр. 7.)

Сотрудники Cisco Security Research выяснили, что веб-трафик, генерируемый этим семейством браузерных расширений, имеет особые характеристики и может быть обнаружен с помощью двух четко определенных шаблонов. Строка запроса обычно содержит данные в зашифрованном виде, в котором такая информация, как имя расширения и посещенный URL-адрес (включая ссылки Интранет), преодолевает фильтры.

Во время анализа специалисты Cisco Security Research выявили свыше 4000 различных имен расширений, включая PassShow, Bettersurf, Bettermarkit и связанные алгоритмы SHA (bee4b83970ffa8346f0e791be92555702154348c14bd8 a1048abaf5b3ca049e35167317272539fa0dece3ac1a60 10c7a936be8cbf70c09e547e0973ef21718e5). Поскольку в одной установке может использоваться несколько имен расширений, отслеживание таких вредоносных программ затруднено (рис. 17).

Рис. 17. Злоумышленные действия и схема заражения



Источник: Cisco Security Research

Вредоносные программы распознают типы ОС, помогая внедрять подходящие эксплойты

Исследователи Cisco Security Research выяснили, что вредоносные расширения отображают определенные типы рекламы в зависимости от браузера пользователя. Внедренные объявления для пользователей Linux обычно были связаны с сайтами онлайн-игр. Пользователи с установленным Microsoft IE перенаправлялись на объявления, которые вели на загрузку якобы фирменного программного обеспечения, но оно оказывалось вредоносным.

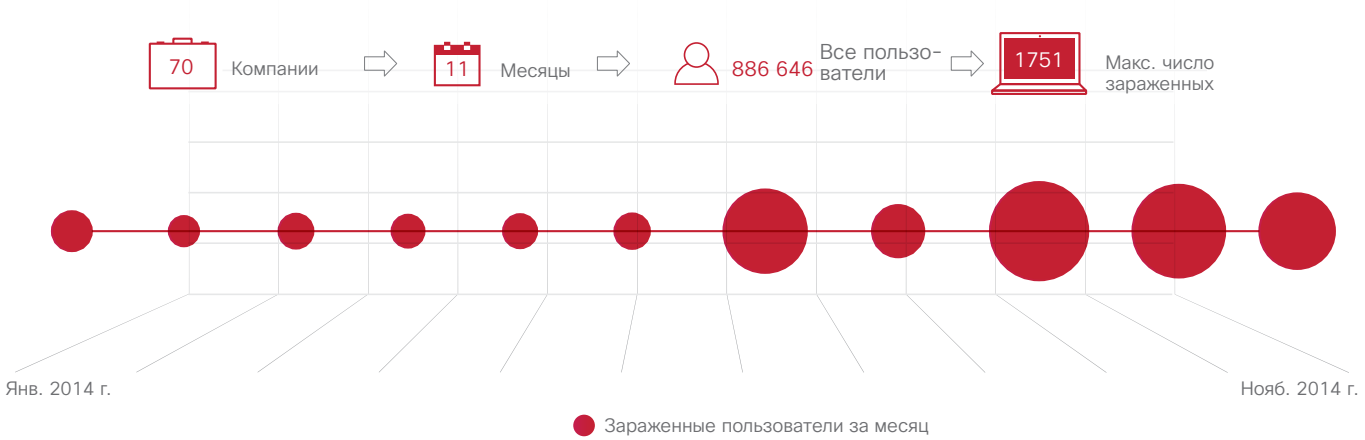
Linux

Microsoft IE

Согласно анализу активности пользователей из 70 компаний в течение 11 месяцев, количество пользователей, затронутых этой угрозой, росло. В январе было затронуто 711 пользователей, а во второй половине года количество затронутых пользователей превысило 1000. Пиковое значение 1751 пришлось на сентябрь (рис. 18). Одной из причин значительного всплеска в сентябре и октябре мог быть рост интернет-активности в период, когда пользователи приступили к работе после летних отпусков.

В рамках этого исследования эксперты по безопасности Cisco выяснили, что для проведения кампании по распространению вредоносных программ злоумышленники задействуют несколько разных серверов. Вероятно, это означает, что либо одна организация киберпреступников, действующая в нескольких сегментах, распространяет эту угрозу, либо один «поставщик технологий» продает свой продукт различным группам. Но кто бы ни распространял эти вредоносные программы, они пытаются создать ботнеты большого размера.

Рис. 18. Количество затронутых пользователей по месяцам, январь – ноябрь 2014 г.



Источник: Cisco Security Research

Поделиться отчетом

Сотрудники Cisco Security Research также выявили более 500 уникальных доменов, связанных с этой угрозой. 24 из них имеют рейтинг на Alexa ниже миллиона наиболее популярных доменов. Некоторые из них имеют относительно высокий рейтинг (рис. 19). Значит, это популярные домены, хотя и очень опасные для посетителей из-за риска нарушения безопасности.

Некоторые домены были активны более года, но большинство имело гораздо более короткий жизненный цикл — во многих случаях всего несколько недель (рис. 19). Все эти домены имеют одну общую характеристику: они очень быстро набирали популярность.

Советы по предотвращению и выявлению проблем безопасности

Чтобы избежать нарушения безопасности по схеме браузерных расширений или справляться с существующими вирусами, пользователям следует воспользоваться следующими советами.

- Загружайте приложения из доверенных источников.
- Отменяйте выбор нежелательных приложений в комплектных установках.
- Используйте анализ угроз, технологии изолированных сред и веб-безопасности, чтобы предотвратить и обнаружить угрозы этого типа.
- По возможности вручную удаляйте расширения; кроме того, используйте антишпионские инструменты для очистки нежелательных программ.

Рис. 19. Популярные домены, использованные для вредоносной рекламы по схеме браузерных расширений, с рейтингом на Alexa

Источник: Cisco Security Research

2. Сравнительное исследование возможностей систем безопасности, проведенное Cisco

Чтобы численно оценить мнение специалистов по безопасности о состоянии безопасности в их организациях, корпорация Cisco опросила руководителей по информационной безопасности (CISO) и менеджеров по безопасности операций (SecOp) в некоторых странах и организациях различного размера об их ресурсах и процедурах обеспечения безопасности. *Сравнительное исследование возможностей систем обеспечения безопасности,* проведенное Cisco в октябре 2014 года, содержит статистические данные о текущем уровне развития операций и практических мерах по безопасности.

Возможности систем безопасности: насколько компании удовлетворяют требованиям?

Как специалисты по безопасности оценивают готовность своих организаций устранять бреши в системе безопасности? Как отмечается в новом исследовании Cisco, их ответы могут зависеть от роли, которую они играют в организации, и от того, в какой отрасли они работают.

На рис. 20 показаны ответы специалистов по отраслям и размеру организации. Производители, не связанные с компьютерной отраслью, и респонденты из сферы коммунального обслуживания и энергетики сообщают о самых высоких уровнях заинтересованности и знаний в сфере безопасности.

N (количество респондентов) = 1738

Рис. 20. Профили респондентов и готовность к отражению угроз

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Исследование проведено по результатам опроса руководителей по информационной безопасности и менеджеров по безопасности операций для того, чтобы выяснить, какие ресурсы их компании выделяют на обеспечение информационной безопасности, какие применяются политики и процедуры, насколько развиты системы защиты. Хорошие новости, полученные в результате опроса, заключаются в том, что большинство специалистов по безопасности считают, что они располагают средствами и инструментами по эффективному поддержанию безопасности. Тем не менее руководители по информационной безопасности заметно более оптимистичны, чем их коллеги по безопасности операций, в отношении состояния безопасности. Например, 62 % руководителей по информационной безопасности отметили, что они в значительной мере согласны с тем, что процессы обеспечения безопасности прозрачны и понятны, по сравнению с 48 % менеджеров по безопасности операций. Руководители по информационной безопасности видят процессы по обеспечению безопасности также в более благоприятном свете. 59 % опрошенных руководителей считают, что их процедуры защиты оптимизированы, той же точки зрения придерживаются 46 % менеджеров по операциям обеспечения безопасности.

С чем связан этот разрыв в степени уверенности? Вероятно, это связано с тем, что руководители по информационной безопасности не принимают участие в повседневных действиях по обеспечению безопасности, в то время как менеджеры по безопасности операций непосредственно работают над разрешением как крупных, так и незначительных инцидентов безопасности. Руководители по информационной безопасности из очень крупных организаций могут не знать о том, что в течение обычного рабочего дня вредоносными программами заражаются тысячи компьютеров, в то время как менеджеры по безопасности операций обычно посвящают гораздо больше времени устранению последствий заражения. Поэтому их мнение менее оптимистично.

Кроме того, руководители по информационной безопасности могут устанавливать такие политики, как блокировка доступа к социальным сетям, что дает им иллюзию более непроницаемой системы защиты. Тем не менее, полностью отключив такие каналы, отделы безопасности могут лишиться информации об угрозах, которые по-прежнему наблюдаются вне их сетей.

Другой разрыв в степени уверенности можно наблюдать по вопросу о том, доверяют ли респонденты политикам безопасности своих организаций. Как руководители по информационной безопасности, так и менеджеры по безопасности операций демонстрируют высокую степень доверия к политикам (см. рис. 21), хотя они менее уверены в своей способности оценить риски и противостоять нарушениям безопасности (см. рис. 28).

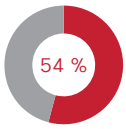
Подобный разрыв наблюдался, когда респондентов просили оценить их средства контроля безопасности. Практически все респонденты сообщали о том, что располагают хорошими средствами контроля безопасности, но почти четверть считает, что их инструменты безопасности только лишь «в некоторой степени», а не «очень» или «в высшей степени» эффективны (см. рис. 29).

Уверенность в процессах и процедурах обеспечения безопасности также зависит от отрасли. Руководители по информационной безопасности и менеджеры по безопасности операций из организаций в сфере телекоммуникаций, коммунального обслуживания и энергетики выражают большую степень уверенности по сравнению с государственными учреждениями, финансовыми службами, фармацевтическими организациями и учреждениями здравоохранения. Например, 62 % руководителей организаций в сфере телекоммуникаций, коммунального обслуживания и энергетики в значительной степени согласны с тем, что их процессы обеспечения безопасности оптимизированы, по сравнению с 50 % тех, кто работает в финансовых службах и 52 % представителей государственных учреждений.

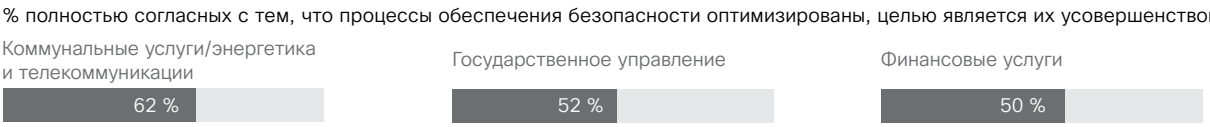
Специалисты по безопасности из организаций в сфере телекоммуникаций, коммунального обслуживания и энергетики демонстрируют высокий уровень развития своих практических действий по обеспечению безопасности, в то время как государственные учреждения и финансовые службы представляются менее развитыми в этом отношении. Организации в сфере коммунального обслуживания и энергетики обычно имеют хорошо документированные процедуры для отслеживания инцидентов. Но это не означает, что они лучше защищены, чем организации в других отраслях.

Рис. 21. Основные результаты исследования по отраслям и должностям

90 % компаний уверены в надежности своих политик и процедур безопасности



Однако 54 % компаний пришлось провести расследование нарушения безопасности

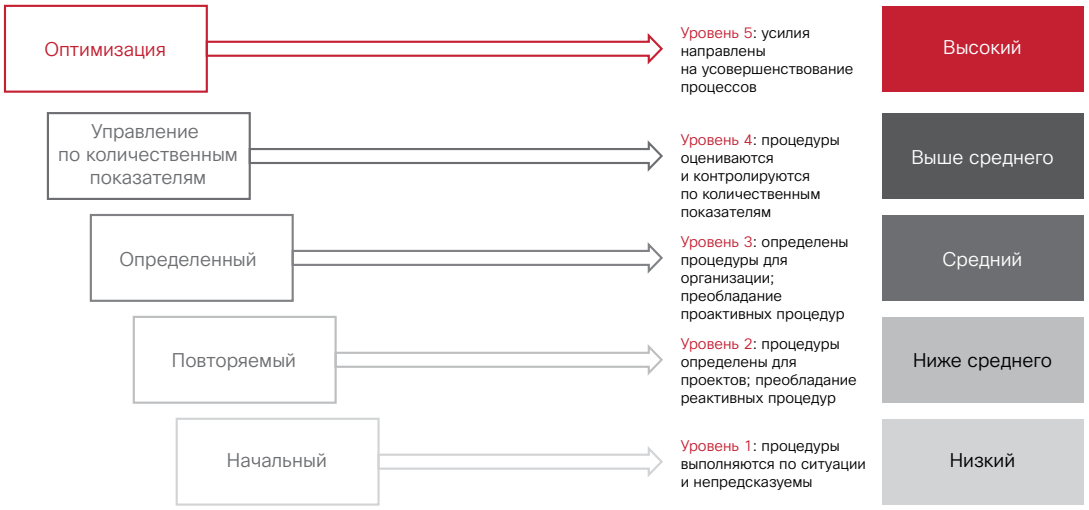


Различия между крупными и средними предприятиями невелики, что указывает на то, что число сотрудников само по себе слабо влияет на сложность системы безопасности.

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Рис. 22. Сопоставление уровней развития систем защиты с текущей выборкой

Компания Cisco изучила несколько вариантов сегментации выборки, прежде чем остановиться на 5-сегментном отображении, составленном на основе серии вопросов о состоянии процедур защиты. Это 5-сегментное решение довольно близко соответствует набору моделей CMMI.



Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Признаки развития средств обеспечения безопасности

В сравнительном исследовании Cisco также приведены признаки организации с более высоким уровнем развития систем защиты. К таким признакам относятся следующие.

- Руководство ставит безопасность во главу угла.
- Четкие, задокументированные политики и процедуры.
- Интегрированные инструменты, применяемые вместе.

91 % респондентов из высокотехнологических компаний в значительной степени согласны с тем, что руководство компаний считает безопасность приоритетной задачей, в то время как только 22 % респондентов из менее технологичных компаний согласны с этим утверждением. Кроме того, 88 % респондентов высокотехнологических компаний в значительной степени согласны с тем, что процессы обеспечения безопасности прозрачны и понятны, по сравнению с 0 % респондентов из менее технологичных компаний.

Рис. 23. Основные результаты исследования в отношении руководящих сотрудников по вопросам безопасности в организациях

В сравнении со специалистами по информационной безопасности, руководители подразделений (или их эквиваленты) более оптимистичны в оценках состояния безопасности своих компаний – возможно, потому, что они находятся дальше от повседневных реалий.

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

На рис. 23. показано, что 91 % респондентов сообщают о том, что в их организации есть руководящие сотрудники с непосредственными обязанностями в сфере безопасности. Чаще всего это руководитель по информационной безопасности (CISO) или руководитель службы безопасности (CSO). Высокие показатели организаций с назначенным ответственным лицом по вопросам безопасности вдохновляют. Без таких руководителей рабочие процессы обеспечения безопасности медленнее определяются, меньше обсуждаются и хуже внедряются. Вероятно, бреши в сфере безопасности, широко обсуждавшиеся недавно, подтолкнули организации к тому, чтобы в структуре руководства найти место и для менеджеров по безопасности.

78 % респондентов из наиболее высокотехнологичных компаний в значительной мере согласны с тем, что технологии обеспечения безопасности хорошо интегрированы и эффективно работают вместе, по сравнению с 17 % респондентов из менее технологичных компаний.

Хорошая новость для тех организаций, которые хотели бы повысить уровень развития своих систем защиты, заключается в том, что не обязательно заниматься подбором большой команды высококлассных специалистов, которых к тому же трудно найти. В менее технологичных компаниях в среднем работает 32 специалиста по безопасности. В компаниях с самым высоким уровнем развития технологий среднее число таких специалистов также равно 32. Поэтому привлечение дополнительных сотрудников не связано напрямую с повышением эффективности защиты. Более удачный подход к привлечению новых сотрудников по безопасности заключается в том, чтобы установить оптимальное отношение количества сотрудников по безопасности к общему количеству служащих компании.

Рис. 24. Основные результаты исследования в отношении приоритетности вопросов безопасности

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

На рис. 24 показано, что представители организаций с менее развитыми системами безопасности не верят в то, что их руководство считает безопасность приоритетной задачей. Также они не верят в то, что процессы обеспечения безопасности прозрачны и понятны.

При сравнении уровней развития средств безопасности по странам выявляются более обнадеживающие факты. Представители высокотехнологичных компаний составляют большинство в каждом сегменте. Но в некоторых странах респонденты придерживаются более позитивного взгляда на состояние безопасности в своей стране, чем в остальном мире. Чрезмерную уверенность респондентов в некоторых странах можно отчасти объяснить культурными особенностями, например стремлением представить себя и свою организацию в хорошем свете.

Остерегайтесь самонадеянности

Хотя руководители по информационной безопасности и менеджеры по безопасности операций доверяют мерам по обеспечению безопасности, они также отмечают, что они не используют стандартных средств, которые помогли бы устранить угрозы использования брешей в системе безопасности в своей организации. Менее 50 % респондентов используют следующие средства.

- Администрирование удостоверений или выделение ресурсов для пользователей.
- Установка исправлений и настройка.
- Тестирование на проникновение.
- Техническая проверка конечных устройств.
- Поиск уязвимостей.

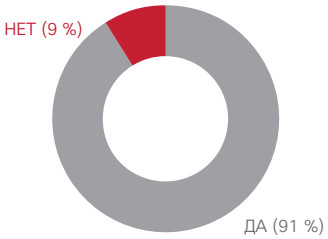
Ресурсы организаций в отношении безопасности

Рис. 25. Количество выделенных специалистов по безопасности в организации

В среднем в организациях насчитывается 123 специалиста по безопасности. Государственные учреждения с большей вероятностью привлекают сторонние организации для предоставления услуг по обеспечению безопасности.

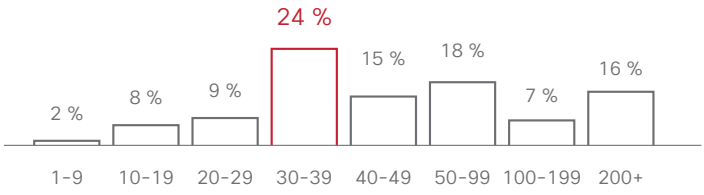
Состояние ресурсов защиты

Существует ли в организации группа реагирования на инциденты?



Среднее число специалистов по безопасности

Средний процент времени, затраченного на решение задач безопасности



Число выделенных специалистов по безопасности

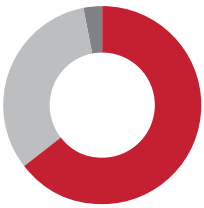
Правительственные организации используют больше сторонних услуг в сравнении с организациями из других отраслей.

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Рис. 26. Технологии обеспечения безопасности, которые используются в организациях

Около двух третей респондентов сообщают, что у них есть современные технологии обеспечения безопасности, которые часто обновляются.

Как бы вы описали состояние вашей инфраструктуры безопасности? Общее количество: n = 1738



64 % Наша инфраструктура безопасности актуальна и постоянно обновляется с применением самых совершенных технологий.

33 % Мы регулярно выполняем замену или обновление наших технологий безопасности, но не используем самые последние и совершенные инструменты.

3 % Мы выполняем замену или обновление наших технологий безопасности только в тех случаях, когда прежние уже не работают или устарели, либо при возникновении совершенно новых потребностей.

С заявлением об актуальности инфраструктуры своей организации согласилось гораздо больше руководителей подразделений (70 %) чем специалистов по безопасности (57 %).

Представители телекоммуникационных компаний чаще всего утверждают, что их инфраструктура безопасности поддерживается в актуальном состоянии.

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Рис. 27. Средства защиты от угроз, используемые организациями

В 2014 г. в организациях применялся целый ряд мер по защите от угроз.

	Средства защиты от угроз, используемые организацией		Средства защиты, управляемые с помощью облачных сервисов	
	Специалисты по безопасности (n = 797)	CISO (n = 941)	Специалисты по безопасности (n = 759)	CISO (n = 887)
Сетевая безопасность, межсетевые экраны/предотвращение вторжений	57 %	64 %	30 %	39 %
Защита веб-трафика	56 %	62 %	33 %	41 %
Защита электронной почты/мгновенных сообщений	53 %	58 %	33 %	41 %
Предотвращение потери данных	55 %	55 %	–	–
Шифрование/конфиденциальность/защита данных	52 %	55 %	–	–
Управление доступом/авторизация	55 %	52 %	24 %	24 %
Аутентификация	54 %	51 %	24 %	22 %
Безопасность мобильных систем	48 %	54 %	24 %	32 %
Защита беспроводной связи	47 %	52 %	22 %	30 %
Защита конечных устройств/нейтрализация вредоносного ПО	45 %	52 %	24 %	27 %
Поиск уязвимостей	44 %	51 %	24 %	26 %
VPN	49 %	46 %	25 %	27 %
Администрирование удостоверений или выделение ресурсов для пользователей	43 %	47 %	16 %	23 %
Управление событиями и информацией о безопасности	39 %	46 %	–	–
Техническая проверка сети	41 %	43 %	–	–
Установка исправлений и настройка	38 %	40 %	–	–
Тестирование на проникновение	39 %	37 %	20 %	19 %
Защита от DDoS-атак	35 %	37 %	–	–
Техническая проверка конечных устройств	29 %	33 %	–	–

Число респондентов, использующих средства защиты от угроз: n = 1646

13 % респондентов утверждают, что они не применяют облачные сервисы для администрирования средств защиты от угроз. Это утверждение особенно справедливо для таких отраслей, как здравоохранение, финансовые услуги и фармацевтика.

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Политики, процедуры и процессы обеспечения безопасности в организациях

Рис. 28. Уровни доверия в отношении политики безопасности и степень уверенности в способности противостоять нарушениям безопасности в организации

В то время как организации испытывают доверие в отношении политики безопасности, они демонстрируют значительно меньшую степень уверенности в своей способности оценить риски и противостоять нарушениям безопасности.

Уровни доверия в отношении политики безопасности в организации

Политики безопасности (n = 1738)	Специалисты по безопасности (n = 797)			Руководители отделов информационной безопасности (n = 941)		
	Не согласен/согласен/ полностью согласен			Не согласен/согласен/ полностью согласен		
В организации проведена инвентаризация и классификация информационных активов.	11 %	40 %	49 %	4 %	38 %	58 %
Мы отлично управляем безопасностью кадровых подразделений.	9 %	45 %	46 %	4 %	36 %	60 %
Компьютерное оборудование моей организации надежно защищено.	10 %	39 %	51 %	4 %	34 %	62 %
В организации налажено эффективное управление техническими инструментами безопасности систем и сетей.	6 %	41 %	53 %	3 %	31 %	66 %
Права доступа к сетям, системам, приложениям, функциям и данным контролируются должным образом.	8 %	35 %	57 %	4 %	32 %	64 %
В организации ведется работа по созданию встроенных механизмов безопасности в системах и приложениях.	10 %	38 %	52 %	4 %	32 %	64 %
Проведена работа по внедрению элементов защиты в процедуры приобретения, разработки и сопровождения систем.	9 %	41 %	50 %	4 %	35 %	61 %

Степень уверенности в отношении способности противостоять нарушениям безопасности в организации

Практическое применение систем защиты (n = 1738)	Специалисты по безопасности (n = 797)			Руководители отделов информационной безопасности (n = 941)		
	Не согласен/согласен/ полностью согласен			Не согласен/согласен/ полностью согласен		
В течение долгого времени мы регулярно проверяем и совершенствуем методы защиты, соблюдая все формальные правила.	7 %	42%	51 %	3 %	36 %	61 %
У нас есть инструменты для проверки и предоставления отзывов о возможностях наших методов защиты.	10 %	41 %	49 %	4 %	39 %	57 %
Мы регулярно и систематически анализируем инциденты.	11 %	40 %	49 %	3 %	37 %	60 %
В случае необходимости мы можем усилить контроль безопасности ценных активов.	10 %	43 %	47 %	3 %	38 %	59 %
Мы регулярно проверяем активность подключений к сети, контролируя надлежащую работу механизмов защиты.	8 %	39 %	53 %	4 %	33 %	63 %
Наши средства обнаружения и нейтрализации угроз поддерживаются в актуальном состоянии.	9 %	38 %	53 %	3 %	36 %	61 %
Уровень интеграции наших технологий безопасности обеспечивает их эффективную совместную работу.	9 %	40 %	51 %	3 %	37 %	60 %
Технологии защиты согласуются с задачами и возможностями нашей организации.	10 %	39 %	51 %	2 %	34 %	64 %
Определение масштаба нарушения, его ограничение и устранение не вызывает трудностей.	15 %	44 %	41 %	8 %	42 %	50 %

Респонденты из организаций среднего размера однозначно согласились с утверждением «в течение долгого времени мы регулярно проверяем и совершенствуем методы защиты, соблюдая все формальные правила», чем специалисты из крупных компаний.

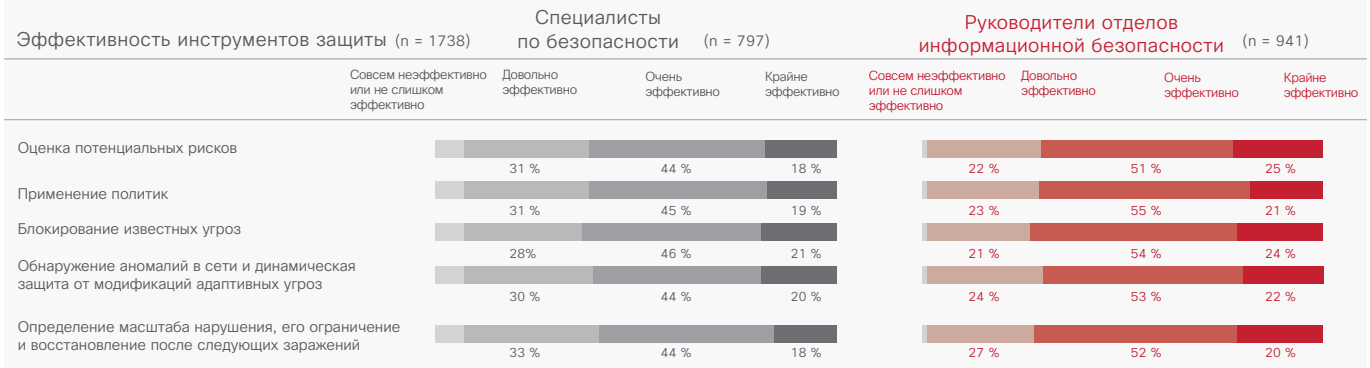
Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Рис. 29. Мнения респондентов об уровне контроля безопасности и о средствах обеспечения безопасности в организациях

Хотя специалисты по безопасности считают, что в их организациях поддерживается высокий уровень контроля безопасности, около четверти респондентов убеждено, что их средства по обеспечению безопасности не слишком эффективны.

Инструменты управления безопасностью (n = 1738)	Специалисты по безопасности (n = 797)			Руководители отделов информационной безопасности (n = 941)		
	Не согласен/**согласен**/ **полностью согласен**			Не согласен/**согласен**/ **полностью согласен**		
Мы применяем стандартные методики реагирования на события, например RFC2350, ISO/IEC 27035:2011 или метод, сертифицированный в США.	15 %	42 %	43 %	6 %	40 %	54 %
Мы используем эффективные процедуры интерпретации и определения приоритетов для поступающих отчетов по инцидентам и получения выводов на их основе.	11 %	46 %	43 %	4 %	39 %	57 %
Наши системы позволяют убедиться в возникновении нарушений безопасности.	11 %	41 %	48 %	4 %	36 %	60 %
Наша система позволяет классифицировать информацию об инцидентах.	10 %	43 %	47 %	4 %	37 %	59 %
Мы уведомляем акционеров об инцидентах и сотрудничаем с ними в этой области.	10 %	46 %	44 %	3 %	40 %	57 %
Мы ведем подробную документацию по процедурам отслеживания инцидентов и реагирования на них.	9 %	40 %	51 %	4 %	35 %	61 %
Оценки рисков безопасности регулярно проводятся в рамках общего процесса оценки рисков.	10 %	37 %	53 %	4 %	36 %	60 %

Значительно большее число респондентов из сферы коммунального хозяйства и энергетики полностью согласно с утверждением «мы ведем подробную документацию по процедурам отслеживания инцидентов и реагирования на них» в сравнении со специалистами из других отраслей.



Специалисты по информационной безопасности в сфере транспорта оказались менее уверенными в способностях своей организации обнаружить и нейтрализовать известные угрозы.

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Рис. 30. Процессы, используемые для анализа взломанных систем, и исключение причин инцидентов безопасности

Специалисты по безопасности с большей вероятностью используют журналы межсетевых экранов для анализа нарушений, хотя эти журналы обычно не содержат высококачественных данных или контекста для этой информации. Для более надежного анализа нарушений безопасности специалисты по безопасности должны регулярно просматривать журналы IDS и IPS, прокси, серверные системы предотвращения вторжений (HIPS), журналы приложений и NetFlow.

Также удивляет, что корреляционный анализ событий/журналов стал самым последним в списке средств, используемых для анализа нарушений. Это может означать, что респонденты не сопоставляют данные или связанные источники данных, а это могло бы помочь более глубоко проанализировать события.

Процедуры анализа взломанных систем	Специалисты по безопасности	Руководители отделов информационной безопасности
	(n = 797)	(n = 941)
Журнал межсетевого экрана	59 %	62 %
Анализ системного журнала	58 %	60 %
Анализ вредоносного ПО или сравнение файлов с исходным состоянием	51 %	58 %
Анализ сетевого потока	51 %	54 %
Анализ реестра	48 %	51 %
Полный анализ захвата пакетов	44 %	48 %
Анализ связанных событий или журналов	40 %	44 %
Проверка памяти	39 %	43 %
Проверка жестких дисков	38 %	41 %
Проверка на наличие признаков нарушения	38 %	38 %
Использование внешних (или сторонних) средств реагирования на инциденты или аналитических групп	36 %	38 %

Респонденты из правительственных организаций склонны использовать больше процедур для анализа взломанных систем по сравнению с респондентами из других отраслей.

Процедуры устранения причины инцидентов	Специалисты по безопасности	Руководители отделов информационной безопасности
	(n = 797)	(n = 941)
Помещение в карантин или удаление вредоносного приложения	55 %	60 %
Анализ основных причин	55 %	56 %
Блокирование коммуникаций вредоносного ПО	51 %	55 %
Дополнительный мониторинг	51 %	53 %
Обновление политик	50 %	51 %
Блокирование коммуникаций взломанного приложения	47 %	49 %
Разработка долгосрочного исправления	46 %	48 %
Восстановление предыдущего состояния системы из образа	43 %	47 %

Ответы руководителей и специалистов согласуются между собой, за исключением пункта «блокирование коммуникаций вредоносного ПО».

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Рис. 31. Ответы руководителей по информационной безопасности (CISO) и специалистов по безопасности операций о контроле после инцидента
Руководители по информационной безопасности чаще сообщают о внедрении дополнительных средств контроля после инцидента, чем специалисты по безопасности операций.

Процессы восстановления затронутых систем	Специалисты по безопасности	Руководители отделов информационной безопасности
	(n = 797)	(n = 941)
Реагирование на инцидент путем внедрения дополнительных или новых средств обнаружения и контроля на основе обнаруженных уязвимостей	55 %	65 %
Установка исправлений и обновлений для уязвимых приложений	59 %	60 %
Восстановление из резервной копии, созданной до инцидента	53 %	60 %
Дифференциальное восстановление	53 %	58 %
Восстановление из мастер-образа	33 %	36 %

Респонденты из организаций в сфере телекоммуникаций и коммунальных услуг/энергетики гиспользуют восстановление из мастер-образа чаще, чем представители других отраслей.

Рис. 32. Кто получает уведомления об инцидентах безопасности
Специалисты по операциям и партнеры по технологиям обычно получают уведомления об инцидентах безопасности посредством более формализованных процессов.

Группы, уведомляемые в случае инцидента	Специалисты по безопасности	Руководители отделов информационной безопасности
	(n = 797)	(n = 941)
Операции	44 %	48 %
Партнеры по разработке технологий	42 %	47 %
Инжиниринг	38 %	37 %
Отдел кадров	37 %	35 %
Юриспруденция	37 %	35 %
Все сотрудники	38 %	33 %
Производственные предприятия	31 %	36 %
Деловые партнеры	31 %	33 %
Маркетинг	30 %	31 %
Связь с общественностью	30 %	27 %
Внешние учреждения	25 %	20 %

Правительственные учреждения значительно чаще имеют четко определенные процедуры уведомления большего количества групп в сравнении с организациями из других отраслей.

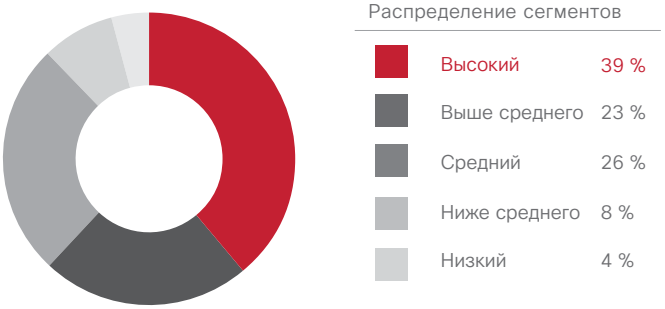
Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Уровень развития систем безопасности в организациях

Рис. 33. Уровень развития обеспечения безопасности

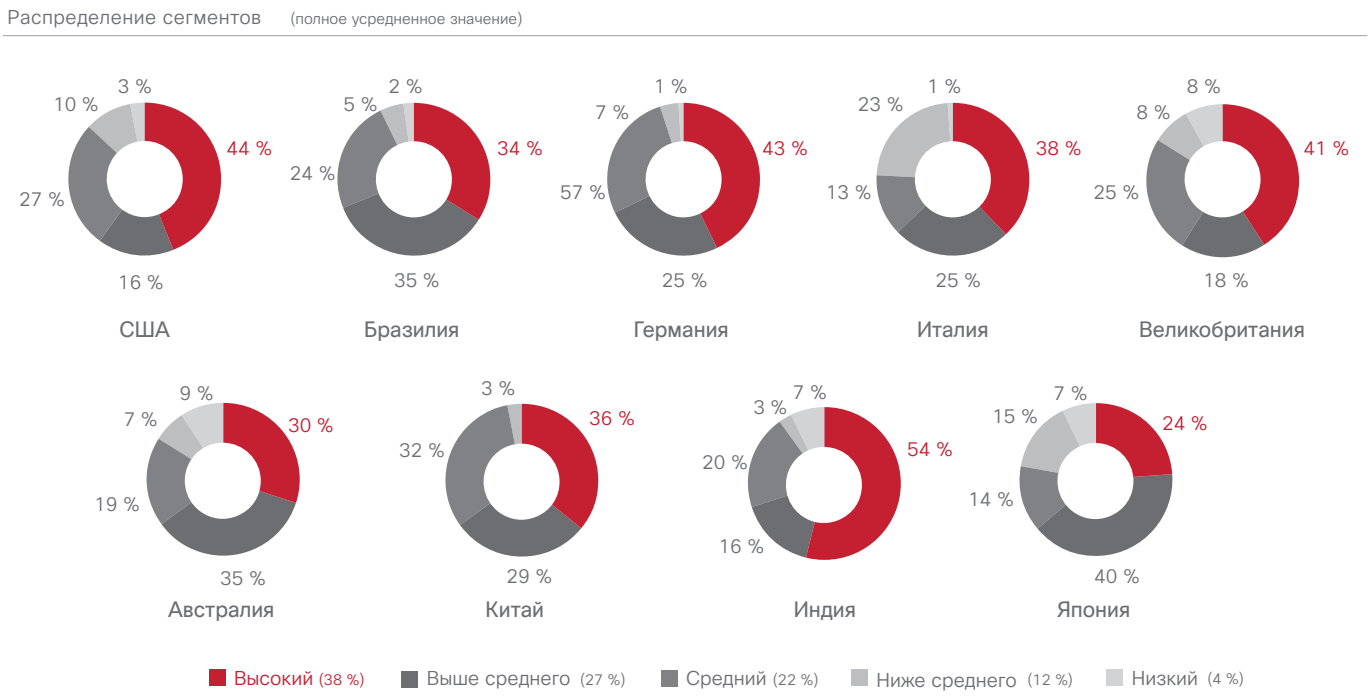
Большинство компаний соответствуют более развитым профилям безопасности. Это справедливо для всех стран (рис. 34) и всех отраслей (рис. 35).

Сегменты отражают рост уровней развития системы защиты и соответствующие изменения процедур.



Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

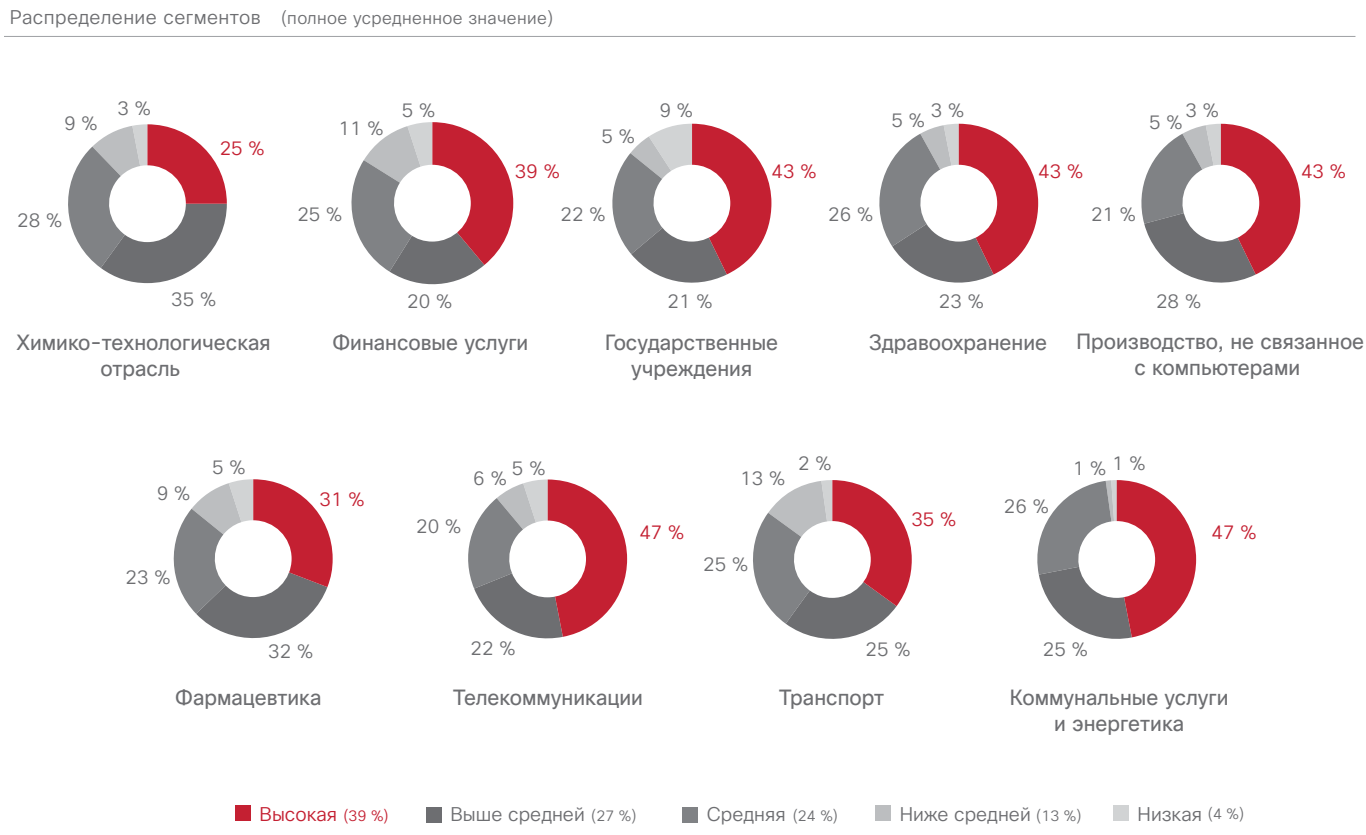
Рис. 34. Уровень развития обеспечения безопасности по странам



Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Рис. 35. Степень развития процессов обеспечения безопасности по отраслям

Почти половина организаций в сфере телекоммуникаций, коммунального обслуживания и энергетики относится к сегменту с высоким уровнем развития систем безопасности.



Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

Организации среднего размера имеют хорошие показатели готовности к защите от угроз

Предполагалось, что очень крупные организации могут успешно управлять безопасностью, поскольку у них есть нужные ресурсы: бюджеты на приобретение новейших технологий и обученный персонал для управления этими технологиями. Можно было предполагать, что большие организации среднего бизнеса (в этом исследовании к ним отнесены организации от 500 до 999 сотрудников) отстают от крупных предприятий (1000 и более сотрудников) с точки зрения готовности реагировать на инциденты безопасности. Тем не менее, согласно *сравнительному исследованию возможностей систем безопасности, проведенному Cisco,* большие предприятия среднего бизнеса не только соответствуют крупным предприятиям по готовности к защите от угроз во многих областях, но чаще имеют более высокие показатели, чем корпорации, возможно, за счет большей гибкости и оперативности.

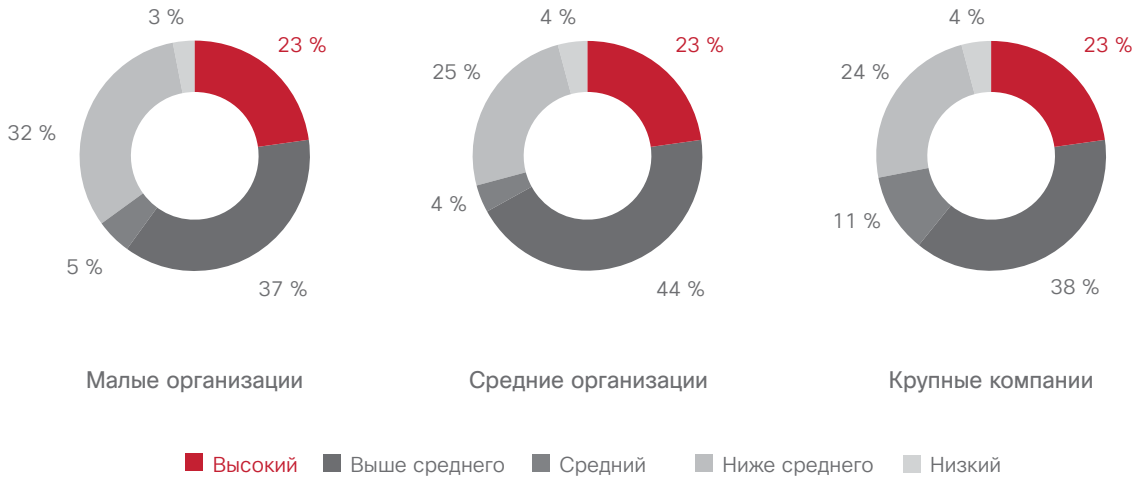
В действительности, согласно данным исследования, более крупные организации среднего бизнеса с большей вероятностью имеют высокоразвитые средства безопасности. Как показано на рис. 36, значительно больше организаций среднего бизнеса с числом сотрудников от 500 до 999 имеют уровень развития выше среднего или высокий, опережая менее крупные организации среднего бизнеса (от 250 до 499 сотрудников) и крупные предприятия (1000 и более сотрудников).

Предприятия среднего бизнеса могут надеяться на позитивную динамику по большинству важных показателей, так как компании среднего бизнеса являются локомотивом возрождающейся экономики.

Основные результаты сравнительного исследования предприятий среднего бизнеса и их готовности к защите от угроз.

- 92 % организаций среднего бизнеса имеют группы реагирования на внутренние инциденты (по сравнению с 93 % крупных предприятий).
- 94 % организаций среднего бизнеса имеют должности руководителей, напрямую отвечающие за безопасность (по сравнению с 92 % более крупных предприятий).

Рис. 36. Уровень развития средств безопасности больших организаций среднего бизнеса



Сегменты отражают рост уровней развития системы безопасности внутри организации и соответствующие изменения процессов и процедур.

Организации среднего размера имеют уровни развития системы безопасности «высокий» и «выше среднего» значительно чаще, чем малые организации и крупные предприятия.

Как минимум, 60 % организаций соответствуют профилям с более развитой системой безопасности.

Источник: *Сравнительное исследование возможностей систем безопасности, проведенное Cisco*

3. Геополитические и отраслевые тенденции

Эксперты Cisco по вопросам безопасности, геополитики и политики отмечают текущие и новые геополитические тенденции, которые организации, в особенности международные, должны учитывать. Эти эксперты также изучают изменение тенденций по всему миру, которые относятся к вопросам суверенитета в сфере данных, а также локализации, шифрования и совместимости данных.

Киберпреступность процветает в условиях слабого контроля со стороны государства

Руководители по информационной безопасности (CISO) и другие руководители в сфере безопасности не всегда уделяют достаточное внимание изменениям в геополитике, но они должны задумываться об этом, особенно если они работают в международной организации. То, что происходит в сфере геополитики, может иметь непосредственное влияние на глобальные цепочки поставок и на то, как предприятия управляют данными клиентов и сотрудников в разных странах. Это также может приводить к увеличению затрат на соблюдение законодательных и нормативных требований, рискам кражи коммерческой тайны, а также физическим и репутационным рискам.

Киберпреступность процветает по всему миру, особенно в условиях слабого контроля со стороны государства. Восточная Европа, которая долгое время была рассадником организованной преступности, – это один из примеров. В зонах со слабым контролем со стороны правоохранительных органов часто можно выявить доказательства связи между государственными разведывательными службами и организованными группами, связанными с киберпреступностью.

«Органы власти США сообщают, что некоторые резонансные атаки, направленные на объекты в США, вероятно, происходили из таких зон. Некоторые из этих атак не были направлены на извлечение дохода, но представляли собой политически мотивированные кампании, попытки собрать разведывательные данные или внедриться в инфраструктуру[7]. Это может свидетельствовать о том, что эти кампании были профинансированы государствами и выполнены высокотехнологичными организациями киберпреступников.

Некоторые государства предпринимают усиленные меры по внедрению стратегического управления в сфере киберпреступности в свои законодательные и нормативные требования. Например, Китай вынес тему «верховенства права» на четвертый пленум 18 съезда Коммунистической партии Китая[8]. Пекин предпринимает меры по искоренению коррупции и усилению законодательства в отношении бизнеса и государственных структур. Эти меры помогут усилить правоприменение и международную деятельность по выявлению киберпреступников и предотвратить их уход от ответственности.

Группы международных террористов, использующие Интернет

Опасность, исходящая от групп международных террористов, таких как Исламское государство (или ИГИЛ), – это другая требующая внимания геополитическая тенденция. Хотя такие группы, как ИГИЛ, не вовлечены в какую-либо значительную деятельность в сфере киберпреступности, они активно пользуются Интернетом, а именно социальными сетями, для привлечения новых членов. Сегодня основные группы международных террористов зарабатывают достаточно денежных средств с помощью традиционных методов финансирования, каких как грабеж, торговля людьми и нефть. Но по мере роста этих организаций они могут перейти к киберпреступлениям как к средству глобального финансирования своей деятельности. Также возможно, что начинающие террористические организации, которые не располагают такими ресурсами, как более развитые группы, могут прибегать к киберпреступлениям как к быстрому способу своего роста.

Читайте публикацию в блоге Cisco Cupcakes and Cyberespionage, чтобы узнать о новых методах защиты от кибершпионажа.

Поиск баланса между суверенитетом данных, локализацией и шифрованием

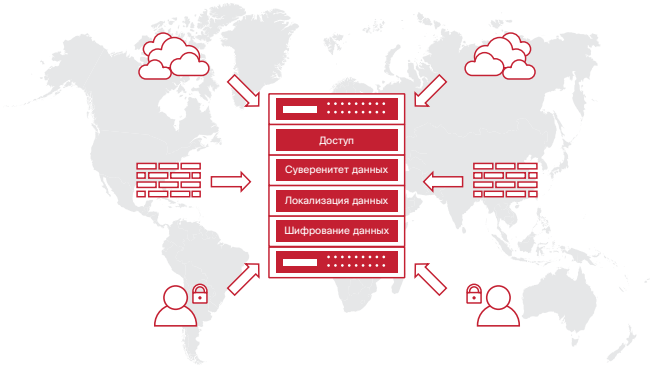
Большое внимание общественности привлекли заявления Эдварда Сноудена о перегибах в деятельности государственных разведывательных органов США, суверенитете в сфере данных (данные должны подпадать под юрисдикцию той страны, в которой они хранятся, а не иностранных правительств и судов, которые могли бы потребовать доступа к ним в одностороннем порядке), а также локализации данных (государство требует, чтобы данные хранились в определенном месте).

Некоторые страны начинают искать возможности локализации своих данных как способа предотвратить доступ иностранных государств к данным своих граждан. Они разрабатывают требования в отношении того, чтобы данные оставались внутри страны или передавались по определенным путям, а также чтобы компании использовали оборудование, изготовленные в пределах своей страны.

Например, Бразилия недавно приняла новый закон, который «содержит требования в отношении конфиденциальности, которые в существенной степени ограничивают [подпадающие под его действие] компании в части использования персональной информации пользователей, их переписки и некоторых интерактивных регистрационных данных»[9]. Тем временем Россия недавно внесла поправки в свое законодательство по защите данных и информации, согласно которым операторы, обрабатывающие персональные данные российских граждан, включая данные Интернета, должны хранить копии таких данных на серверах и в базах данных, расположенных на территории России. Этот закон должен вступить в силу в 2015 г[10].

Потенциально негативные последствия от того, что некоторые страны требуют локализации данных и принимают законы, препятствующие деятельности в глобальном масштабе, заключаются в том, что международные компании могли бы столкнуться с законодательными конфликтами. Обязанность удовлетворять требованиям одной страны в отношении производства, хранения и уничтожения данных могло бы нарушать законодательство другой страны.

Рис. 37. Поиск баланса между суверенитетом данных, локализацией и шифрованием



Кроме возможных конфликтов законодательства, требование локализации данных может также ограничить поток трансграничных данных. Это может вызывать недоразумения, а также серьезные трудности в администрировании сетей. Кроме того, есть аспекты, связанные с цепочкой поставки. Все большее число операторов глобальных цепочек поставок внедряют облачные технологии для связи между своими партнерами по всему миру. Локализация данных могла бы помешать или препятствовать обмену данными в таких бизнес-сетях, а также, возможно, препятствовать международным действиям по охране порядка в сфере киберпреступности.

Кроме того, так как некоторые страны предпочитают использовать свои собственные технологии или налагать серьезные ограничения в отношении того, кто имеет право обрабатывать данные их граждан, не исключено, что они тем самым будут отсекать себя от глобального пула специалистов и подвергаться возможному риску потери таких инноваций, которые возникают в результате обмена новыми идеями.

Некоторые ведущие технологические компании в США надеются, что сквозное шифрование позволит снять озабоченность своих клиентов в отношении защиты данных при их передаче по Интернету в другие страны. Правительство США выразило озабоченность, что такое шифрование не позволяет обеспечить защиту граждан. Новый директор Управления правительственной связи Великобритании, ведущей организации по радиоэлектронной разведке в Великобритании, аналогичной Управлению национальной безопасности в США, даже предположил, что крупнейшие социальные сети США помогают террористам, рассылая зашифрованные сообщения по всему миру[11].

Несмотря на эту критику, высокотехнологичные компании продолжают разрабатывать и внедрять технические средства, направленные на восстановление доверия клиентов, а правительства приняли политики, которые отражают важность свободы слова и безопасности коммерческой деятельности, а также обеспечивают общественную и национальную безопасность.

Доверие к технологическим продуктам и компаниям, которые их разрабатывают, должно пройти долгий путь, чтобы страны, их правительства и граждане поверили в то, что они и их данные защищены. Как отметил Марк Чэндлер (Mark Chandler), старший вице-президент, главный консультант и секретарь Cisco, в своем сообщении в блоге Cisco, опубликованном ранее в этом году, «доверие можно возвратить в результате очень серьезных усилий, которые, что очень важно, должны оправдать ожидания в отношении Интернета следующего поколения и построить мир, в котором связь между людьми и устройствами приносит свободу, процветание и новые возможности для людей во всем мире»[12].

Совместимость стандартов безопасности личных данных

Отношение личности или организации к безопасности личных данных может существенно различаться в зависимости от страны проживания или работы. Эти различные точки зрения влияют на требования правового регулирования безопасности личных данных и способы ведения бизнеса предприятиями в случае разногласий между этими требованиями. В отчете по исследованию индекса значимости вопросов в сфере защиты данных *(Data Protection Heat Index Survey Report)*, выполненному группой Cloud Security Alliance при поддержке компании Cisco, подробно описываются некоторые из проблем, с которыми сталкиваются предприятия, работающие с данными за пределами своих стран или данными, принадлежащими клиентам за пределами страны ведения бизнеса.

Обсуждение совместимости стандартов безопасности личных данных, т. е. создание согласованных глобальных методов обеспечения их безопасности, стало более актуальным из-за роста облачных сервисов. Например, если американская компания приобретает у индийской компании облачное хранилище, а затем использует его для хранения данных клиентов из Германии, какие законы должны применяться по отношению к безопасности данных?

Рис. 38. Удовлетворение требований законодательства и клиентов

Другими факторами совместимости стандартов безопасности личных данных являются Интернет вещей (IoT) и большие данные (Big Data). По мере того как предприятия применяют новые способы соединения устройств и используют большие наборы данных для принятия решений, у них возникает потребность в структуре и правилах обработки этих данных в глобальном масштабе.

В различных регионах и группах стран разрабатываются меры по согласованию требований к обеспечению безопасности личных данных. Например, изменения в законодательстве ЕС предусматривают согласованное обновление существующей директивы по защите данных *(General Data Protection Regulation)*. Наращиваются усилия по согласованию отдельных законов, регулирующих обеспечение безопасности и суверенитета личных данных. Кроме повышения уровня согласованности, большое значение также придается тому, чтобы окончательный текст директивы был нацелен на достижение конечного результата, обеспечивал взаимодействие с другими регионами и соответствовал новым технологиям. В Азиатско-Тихоокеанском регионе было разработано соглашение по обеспечению трансграничной защиты данных (Cross-Border Privacy Enforcement Arrangement), регулирующее обмен данными между странами АТЭС. Правительства отдельных стран должны еще многое сделать для достижения более значительной цели – создания согласованных и закрепленных международными стандартами систем обеспечения безопасности личных данных, которые способствуют открытости Интернета и свободному обмену данными сквозь национальные и региональные границы.

Уточнение странами и регионами своих подходов к обеспечению конфиденциальности данных позволит предприятиям расширить глобальное применение согласованных методов защиты информации, изначально заложив в продукты и сервисы возможности защиты личных данных. Четкая и единообразная нормативная база по защите информации поможет компаниям удовлетворить требования к конфиденциальности, независимо от места предоставления услуг, способствуя разработке новых продуктов и способов использования данных.

Безопасность личных данных: единый взгляд

В опросе по защите данных участвовали эксперты в области обеспечения конфиденциальности из Северной Америки, Европейского союза и Азиатско-Тихоокеанского региона. Они выразили свое мнение о нормативном регулировании обмена данными в своем регионе, правительственных мерах, пользовательском контенте и стандартах обеспечения безопасности. Ответы показали высокий уровень согласия между респондентами в понимании значения безопасности личных данных и международных стандартов в этой области.

- **Место хранения и суверенитет данных.** Респонденты заявили, что в большинстве стран персональные и идентифицирующие данные должны храниться внутри страны.
- **Легитимный перехват данных.** Респонденты продемонстрировали универсальную интерпретацию условий для перехвата личных данных, например в целях расследования преступления.
- **Согласие пользователей на использование личных данных.** 73 % респондентов согласились с необходимостью декларации о защите личной информации потребителей, которая действовала бы не в отдельных регионах, а в общемировом масштабе. 65 % респондентов заявили, что такая декларация должна создаваться при активном участии ООН.
- **Принципы конфиденциальности.** Респондентам был задан вопрос, могут ли способствовать согласованному использованию информации принятые в ОЭСР принципы конфиденциальности или же они приведут к росту разногласий. Большинство экспертов высказалось за принятие этих принципов.

В целом исследование безопасности личных данных показало, что многие эксперты соглашаются с основными принципами конфиденциальности и считают, что их принятие в качестве общемирового стандарта будет способствовать развитию бизнеса. Результаты также указывают на то, что эксперты более склонны к адаптации принципов конфиденциальности к новым технологическим решениям, чем к попыткам изменить эти решения для соответствия требованиям конфиденциальности. Однако действующая нормативная база конфиденциальности находится на относительно ранней стадии развития и быстро эволюционирует.

Рост согласованности окажется выгодным как компаниям, так и отдельным пользователям. Но пока в отрасли продолжают наблюдаться противоречия глобальной структурной основы конфиденциальности, компаниям потребуется тщательно продумывать вопросы конфиденциальности и защиты данных и заранее адаптировать свои предложения и процессы к различным требованиям заказчиков и законодательства.

Дополнительные сведения о вопросах защиты данных см. в публикации блога Cisco Security Data Protection in the Balance—EU Citizen Protection and Innovation («Баланс защиты данных – инновации и защита жителей ЕС»).

4. Изменение взгляда на информационную безопасность – от пользователей до совета директоров

Эксперты Cisco полагают, что для предприятий наступило время пересмотра своего подхода к информационной безопасности и значительного усиления защиты своих организаций. Возможные стратегии включают в себя изучение новых подходов к взаимосвязям людей, процессов и технологий, решение вопросов безопасности на уровне руководства и внедрение более развитых инструментов защиты, которые способны сократить число уязвимых конечных устройств и фронт атаки, а также усилить защиту сети после атаки.

Защищенный доступ: сведения о пользователях, времени и способах использования сети

Руководители и специалисты отделов информационной безопасности сталкиваются со сложными проблемами доступа к сервисам и информации в сети. Рост использования мобильных и личных устройств на работе (BYOD) ставит задачу обеспечения доступа сотрудников к корпоративным ресурсам, независимо от места и способа входа в сеть.

Специалисты по безопасности также должны защитить сеть от несанкционированного доступа и злоумышленников, причем это необходимо сделать таким способом, который не препятствует доступу обычных пользователей. Например, в качестве стандартного решения для управления доступом к сети используются сети VPN. Однако процедура входа в некоторые сети VPN довольно сложна и требует специальных программ, что ограничивает время и способ доступа для пользователей. Кроме того, многие сети VPN не позволяют администраторам определить личность, место доступа и устройство, используемое для входа в сеть. Развитие сетей VPN открывает больше возможностей для мониторинга и повышает прозрачность работы пользователей, что обеспечивает более надежную защиту конечных устройств.

Элементы управления доступом к сети (NAC, network access control) из базовых средств защиты превращаются в более сложные и совершенные инструменты контроля, доступа и защиты конечного устройства (EVAS, endpoint visibility, access and security). В отличие от прежних технологий NAC, инструменты EVAS используют более подробную информацию для применения политик доступа, например данные о роли пользователя, его местонахождении, факторы, связанные с бизнес-процессом и управлением рисками. Инструменты EVAS также помогают сетевым администраторам распространить предоставление доступа за пределы компьютеров на область мобильных устройств и объектов Интернета вещей.

Технологии EVAS позволяют использовать сеть как датчик, разрешая или блокируя доступ к сети при входе с удаленного устройства (для VPN), до подключения к сетевым сервисам или даже внутри самой сети при обращении к наиболее важным ресурсам. Инструменты EVAS также помогают организациям сократить число уязвимых конечных устройств и фронт сетевой атаки, ограничить ее масштаб, запустить процессы восстановления и даже усилить защиту сети после атаки.

Дополнительные сведения о решениях EVAS и повышении безопасности организаций с их помощью см. в публикации блога Cisco Security New White Paper from Enterprise Strategy Group on the Evolution of and Need for Secure Network Access.

Рис. 39. Превращение элементов управления доступом к сети (NAC) в инструменты контроля, доступа и защиты конечного устройства (EVAS)

Возможности EVAS до атаки

- **Определение активов в зоне риска.** Постоянный мониторинг всех активов, подключенных к сети, выявление несоответствующих пользователей, устройств и приложений, сопоставление этой информации с данными сторонних инструментов оценки уязвимостей.
- **Снижение рисков.** Сбор практически значимой информации, которую можно использовать в других сетевых приложениях и системах защиты для улучшения рабочих процессов, рационализации действий и определения приоритетов при восстановлении.
- **Применение детализированных политик доступа к сети.** Предоставление контекстной информации для применения детализированных политик, ограничение доступа к наиболее важному содержимому, активам или сегментам сети.

Возможности EVAS во время атаки

- **Интеграция с расширенными системами сетевой защиты.** Использование информации при обнаружении вредоносной деятельности для корреляции данных об атаке с подключениями конечных устройств, конфигурациями и моделями поведения.
- **Блокирование распространения угрозы от взломанных систем.** Ограничение горизонтального распространения атаки посредством блокирования несанкционированного доступа взломанных систем к сетевым активам под управлением политик с целью расширения прав доступа, похищения учетных данных и ценной информации.
- **Ограничение области атаки.** Блокирование систем с аномальным поведением и помещение их в карантин.

Возможности EVAS после обнаружения атаки

- **Оценка профилей конечных устройств на наличие уязвимостей.** Использование информации из базы данных EVAS в инструментах анализа уязвимостей, которые могут помочь ИТ-отделам определить приоритеты для исправлений.
- **Восстановление взломанных систем.** После интеграции с системами управления событиями и информацией о безопасности (SIEM) и системами безопасности конечных устройств инструменты EVAS позволяют автоматизировать процесс исправлений и следить за его ходом.
- **Точная настройка политик доступа и инструментов защиты.** Взаимодействие EVAS с сетевым оборудованием и средствами защиты позволяет сегментировать трафик приложений, добавлять новые правила для межсетевых экранов или новые сигнатуры IPS.

В отличие от прежних, чрезмерно сложных элементов управления доступом к сети, инструменты решения EVAS способствуют развитию бизнес-процессов. Внедрение политик использования личных устройств, облачных вычислений и мобильных решений заставляет организации придавать все большее значение усилению контроля, уточнению контекстных данных для подключаемых пользователей и устройств, а также эффективному применению политик безопасности. Эксперты Cisco предполагают, что руководители подразделений информационной безопасности все чаще будут применять решения EVAS для управления сложной системой взаимосвязей пользователей, устройств, сетей и облачных сервисов.

Информационная безопасность сегодня зависит от заинтересованности совета директоров компании

По данным *Сравнительного исследования возможностей систем безопасности, проведенного Cisco*, в 91 % организаций имеется руководитель, непосредственно отвечающий за информационную безопасность. Но в организационной структуре современных предприятий руководство безопасностью должно подняться еще выше – на уровень совета директоров.

Недавние массовые утечки данных в известных компаниях, новые законы и нормативные акты, связанные с защитой данных, геополитическая динамика, ожидания акционеров – все эти факторы ставят информационную безопасность на повестку дня высшего руководства. По данным отчета Ассоциации аудита и контроля информационных систем (ISACA), в настоящее время 55 % директоров понимают проблемы информационной безопасности и управляют ею как областью повышенного риска[13].

Это хорошая новость, однако, по мнению экспертов Cisco, изменение подхода назрело давно. В современной экономике работа каждой компании зависит от ИТ-отдела. Поэтому информационная безопасность становится делом каждого члена организации, от директора до только что нанятого специалиста, а не только сотрудников, должность и список обязанностей которых содержит слово «безопасность». Каждый сотрудник должен нести ответственность и изучить основные правила информационной безопасности.

Эксперты Cisco утверждают, что информационная безопасность будет зависеть от заинтересованности совета директоров компании. Совет директоров любой компании должен знать риски, связанные с информационной безопасностью, и их потенциальное влияние на бизнес. Чтобы иметь четкое представление по вопросам безопасности, имеющим отношение к организации, в некоторые советы директоров должны быть включены члены с профессиональными знаниями в области информационных технологий и защиты данных.

Руководство также должно поставить ряд сложных вопросов о системе безопасности. *Какие инструменты управления безопасностью действуют в настоящее время? Насколько тщательно они были проверены? Действует ли процесс создания отчетов? Как быстро можно обнаружить взлом системы и устранить его последствия?* И, возможно, наиболее важный вопрос: *что еще мы должны знать?* Директорам по ИТ необходимо подготовить ответы на эти вопросы в терминах, понятных для членов совета, а также дать обзор возможных последствий для бизнеса.

В недавнем интервью журналу FORTUNE[14] директор Cisco Systems по информационной безопасности Джон Стюарт (John Stewart) рассказал, что постановка подобных вопросов на совете директоров способна вызвать «ряд интересных последствий», которые в конечном счете приведут к развитию отрасли информационной безопасности. Следующим важным шагом, как он надеется, станет признание производителями необходимости встроенной системы безопасности в их продуктах.

Стюарт прогнозирует, что развитие Интернета вещей и тот факт, что «количество полностью автоматических устройств в Интернете превышает количество живых пользователей», приведут к неизбежному возникновению «несчастных случаев» потенциально большого масштаба. Проектирование продуктов со встроенными средствами безопасности поможет избежать многих подобных проблем или, по крайней мере, уменьшить их последствия.

Таким образом, руководители производства должны спросить своих экспертов по безопасности: *«Имеют ли наши продукты встроенную систему безопасности? И если нет, то когда мы можем это сделать?»*.

Видеоблог директора Cisco Systems по информационной безопасности Джона Стюарта о значении прозрачности процедур защиты и важности предоставления отчетов совету директоров: http://blogs.cisco.com/security/ensuring-security-and-trust-stewardship-and-accountability.

Манифест информационной безопасности Cisco: основные принципы обеспечения безопасности в реальном мире

Современные руководители отделов информационной безопасности должны ответить на сложные вопросы. *Как сделать мой отдел первым источником информации для бизнеса при возникновении потенциальных проблем с безопасностью? Как обеспечить мой отдел инструментами контроля для определения наиболее насущных проблем безопасности, требующих решения? Как поддерживать безопасность пользователей, основы успешного бизнеса, даже когда они находятся за пределами предприятия?*

Эксперты Cisco предполагают, что руководители отделов информационной безопасности могут ответить на эти вопросы, следуя набору принципов, известных под названием «Манифест информационной безопасности Cisco».

Этот манифест может помочь отделам ИБ и пользователям лучше понять и решить современные проблемы информационной безопасности. Эти принципы могут служить в качестве ориентира для организаций, стремящихся обойти своих конкурентов посредством более динамичного, адаптивного и инновационного подхода к обеспечению информационной безопасности.

1. **Информационная безопасность должна рассматриваться как движущий фактор бизнеса.** Информационная безопасность никогда не должна становиться барьером, который снижает производительность пользователя и стоит на пути бизнес-инноваций. Пока что специалисты навязывают технические решения, которые являются именно таким препятствием. Основная причина – их не пригласили на обсуждение бизнес-проектов, требующих внедрения новой технологии. Однако специалисты по информационной безопасности тоже виноваты, поскольку они просто ждут приглашения, которое могут никогда не получить. Вместо этого им следует заранее позаботиться о своем участии в обсуждении технологий и понять, каким образом процедуры безопасности могут способствовать динамичности и успеху организации, обеспечивая защиту данных, активов и имиджа.

2. **Система информационной безопасности должна быть удобной и работать в условиях существующей архитектуры.** Отделы информационной безопасности не должны создавать архитектуру для новых технических решений, направленных на усовершенствование системы защиты. Архитектура по своей природе является ограничивающим фактором. Организации не должны изменять способ ведения бизнеса для соответствия новым технологиям защиты, а существующие технологии не должны мешать изменениям способов деятельности. Конечным результатом «архитектурной перегрузки» станут попытки пользователей обойти систему защиты, снижающие безопасность организации. Кроме того, если технология защиты слишком сложна для понимания пользователями и требует поддержки со стороны дефицитного квалифицированного специалиста, то это создаст проблемы для организации.

3. **Система безопасности должна быть информативной и прозрачной.** Пользователям должны предоставляться пояснения, почему она не дает выполнить какое-либо конкретное действие. Им также надо знать, как можно выполнить желаемое действие безопасным образом вместо обхода системы защиты ради выполнения своей работы. Например, когда пользователь пытается зайти на веб-страницу и получает сообщение «Доступ к этому сайту заблокирован администратором», он не получает пояснения причин блокирования этой страницы. Но если в сообщении будет сказано «Доступ к этому сайту заблокирован, так как за последние 48 часов на нем была обнаружена вирусная активность», пользователь получит больше информации и будет понимать потенциальный риск не только для организации, но и для себя лично. Технологии информационной безопасности также должны помочь пользователям в безопасном выполнении своих задач, давая четкие рекомендации или направляя их на соответствующие ресурсы для получения своевременной помощи.

4. **Система безопасности должна обладать возможностями мониторинга и реагирования.** Решения с открытой архитектурой позволяют специалистам по информационной безопасности оценить их реальную эффективность. Специалистам также нужны инструменты для автоматизации мониторинга сети, позволяющие следить не только за трафиком, но и за ресурсами, составляющими сеть. Понимание принципов работы систем защиты и того, какие ситуации являются нормальными или ненормальными в ИТ-среде, уменьшает административную нагрузку ИТ-отделов, ускоряет обнаружение и нейтрализацию угроз, а также адаптацию защитных механизмов. Принимая такой подход, специалисты информационной безопасности могут использовать наиболее подходящие инструменты контроля для решения проблем.

5. **Безопасность должна рассматриваться как комплекс человеческих факторов.** Исключительно технологический подход к построению системы защиты не повышает безопасность, а лишь усугубляет ее проблемы. Технологии – всего лишь инструменты, усиливающие способности людей к защите своей среды. Специалисты по безопасности должны обучить пользователей основным правилам безопасности, которых им следует придерживаться везде – в офисе, дома или в дороге. Это позволит им принимать правильные решения и получить своевременную поддержку в случае проблем. Налаженный диалог со специалистами по безопасности также поможет пользователям понять, что одна лишь технология не может гарантировать безопасность. В защите от современных угроз должны учитываться все факторы: люди, процессы и технологии. Успешная работа системы защиты зависит от ответственности и бдительности всех сотрудников организации – от руководителей до подчиненных.

Манифест информационной безопасности Cisco – это призыв к переменам. На практике технологии, политики и передовые методы защиты должны повысить средний уровень безопасности каждого сотрудника организации и помочь бизнесу принимать решения на основе более полной информации о рисках вплоть до каждого отдельного пользователя. Следуя строгим принципам, пользователи могут четко определять, почему им не разрешено выполнение некоторых действий и каковы могут быть последствия в случае обхода системы безопасности.

Манифест информационной безопасности Cisco или документ, повторяющий его основные принципы, поможет пользователям и специалистам увидеть общую картину информационной безопасности. Несмотря на то что многих угроз можно избежать, взлом защиты неизбежен, но восстановление системы можно выполнить быстро. Основная цель – ускорить решение проблем, когда защита окажется взломанной, а не сосредоточивать усилия исключительно на попытках предотвращения таких событий.

О компании Cisco

Компания Cisco создает интеллектуальные системы информационной безопасности для реального мира. Предлагаемый ею комплекс решений является одним из наиболее полных в отрасли и защищает от широкого спектра угроз. Подход Cisco к информационной безопасности, ориентированный на нейтрализацию угроз и восстановление работоспособности, упрощает систему безопасности, делает ее более цельной, предоставляет возможности детального мониторинга, согласованного управления и усовершенствованной защиты от угроз до, во время и после атаки.

Исследователи угроз из экосистемы коллективной информационной безопасности (CSI) объединяют наиболее полные в отрасли аналитические данные по угрозам, данные телеметрии от огромного количества устройств и датчиков, информацию из общедоступных и частных веб-каналов по уязвимостям, а также от сообщества разработчиков открытого ПО, поддерживаемого Cisco. Ежедневный объем этой информации составляют миллиарды веб-запросов, миллионы сообщений электронной почты, образцов вредоносного ПО и данных о сетевых проникновениях.

Эти данные обрабатываются в развитой инфраструктуре, которая позволяет исследователям и самообучающимся системам отслеживать угрозы в различных сетях, центрах обработки данных, терминалах, мобильных устройствах, виртуальных системах, веб-сайтах, электронной почте и облачных системах с целью определения основных причин и масштабов распространения угроз. Итоговые данные анализа немедленно распространяются по всему миру среди клиентов Cisco и используются для защиты наших продуктов и сервисов в режиме реального времени.

Экосистему CSI составляют несколько групп с различными функциями: Talos, Security & Trust Organization, Managed Threat Defense (MTD) и Security Research and Operations (SR&O).

Дополнительные сведения о подходе к безопасности, ориентированном на угрозы, см. на веб-странице www.cisco.com/go/security.

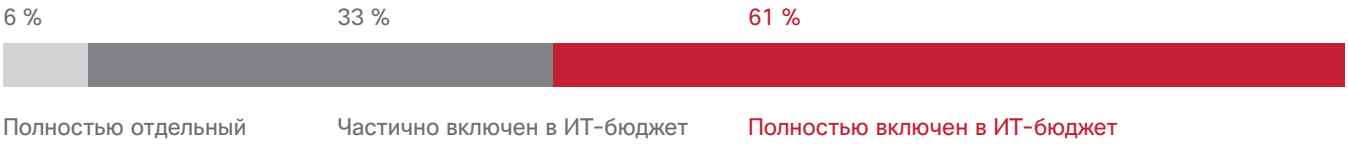
Приложение

Дополнительные результаты сравнительного исследования возможностей систем безопасности

Ресурсы

Является ли бюджет на средства защиты частью ИТ-бюджета?

Сотрудники департамента ИТ; n = 1720

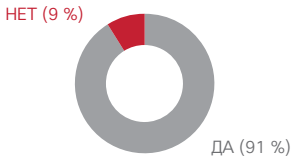


Политики, процедуры и операции

Highest ranking executive accountable for security is most often a CISO or CSO.

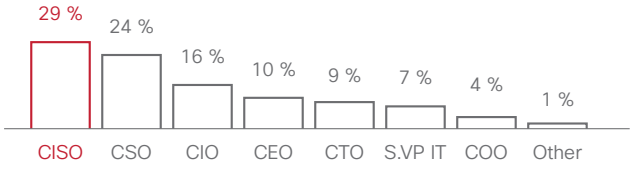
Есть ли в вашей организации руководитель высшего звена, несущий непосредственную ответственность за состояние информационной безопасности?

Респонденты, сообщившие о распределении ролей и сфер ответственности; n = 1603



Должность руководителя

Респонденты, сообщившие о высшем руководителе, отвечающем за безопасность; n = 1465



Организации в области здравоохранения реже других определяют высшего руководителя, отвечающего за безопасность.

Поделиться отчетом

Почти две трети респондентов сообщили, что высшее руководство их компании считает информационную безопасность приоритетной задачей.

Участие руководства (n = 1738)	Специалисты по безопасности (n = 797)			Руководители отделов информационной безопасности (n = 941)		
	Не согласен/согласен/ полностью согласен			Не согласен/согласен/ полностью согласен		
Высшее руководство моей организации считает, что вопросы безопасности имеют высокий приоритет.	8 %	34 %	58 %	3 %	30 %	67 %
Высшее руководство моей организации четко представляет распределение ролей и обязанностей в области безопасности.	9 %	39 %	52 %	2 %	32 %	64 %
Высшим руководством моей организации определены показатели для оценки эффективности программы защиты.	11 %	44 %	45 %	4 %	37 %	59 %

Большинство респондентов, сообщивших о том, что им не приходилось проводить расследование нарушения безопасности в организации, полностью согласны с утверждением «высшее руководство моей организации считает, что вопросы безопасности имеют высокий приоритет».

Значительная часть респондентов отметила процедуры защиты, поощряющие участие сотрудников.

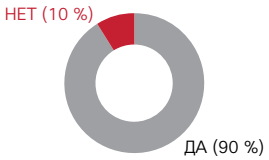
Процедуры защиты (n = 1738)	Специалисты по безопасности (n = 797)			Руководители отделов информационной безопасности (n = 941)		
	Не согласен/согласен/ полностью согласен			Не согласен/согласен/ полностью согласен		
В моей организации поощряется участие руководителей бизнес-направлений в разработке политик и процедур защиты.	12 %	39 %	49 %	6 %	40 %	54 %
Моя организация способна обнаружить уязвимости в системе безопасности до возникновения полномасштабных инцидентов.	13 %	43 %	44 %	4 %	39 %	57 %
В моей организации поощряются сообщения сотрудников о сбоях и проблемах безопасности.	11 %	34 %	55 %	4 %	36 %	60 %
Процедуры защиты в моей организации прозрачны и понятны.	13 %	39 %	48 %	4 %	37 %	59 %
Процедуры защиты в моей организации позволяют заранее предупредить о проблемах и уменьшить их последствия.	14 %	40 %	46 %	3 %	40 %	47 %
Процедуры защиты в моей организации оцениваются и контролируются с использованием количественных показателей.	13 %	40 %	47 %	4 %	35 %	61 %
Моя организация уже оптимизировала свои процедуры безопасности и занимается их усовершенствованием.	12 %	42 %	46 %	4 %	36 %	60 %

Специалисты по безопасности из организаций среднего размера склонны выражать большее согласие с процедурами защиты по сравнению со специалистами крупных предприятий.

9 из 10 респондентов сообщают, что сотрудники отделов информационной безопасности регулярно проходят обучение, которое обычно проводится специалистами по информационной безопасности.

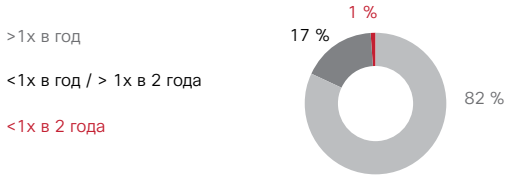
Проводится ли регулярное информирование и/или обучение сотрудников отделов информационной безопасности?

Респонденты, специалисты по безопасности; n = 1726



Как часто проводится обучение по безопасности?

Респонденты, специалисты по безопасности; n = 1556



Кто проводит обучение по безопасности?

Респонденты, в чьих отделах информационной безопасности проводится обучение; n = 1556

Внутренняя группа по безопасности 79 %

Сторонние специалисты 38 %

Отдел кадров 25 %

Другие сотрудники 10 %

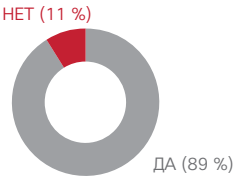
Другое 1 %

15 % специалистов из отрасли финансовых услуг сообщили об отсутствии регулярного обучения.

Сотрудники обычно участвуют в конференции или проходят обучение. Почти две трети опрошенных сообщили, что они являются членами отраслевых ассоциаций специалистов по безопасности.

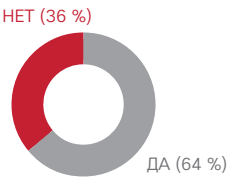
Участвуют ли сотрудники отделов информационной безопасности в конференциях и/или проходят ли внешнее обучение с целью поддержки и совершенствования своих навыков?

Респонденты, специалисты по безопасности; n = 1715



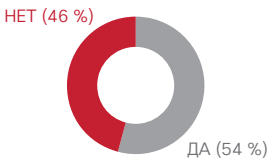
Являются ли специалисты по безопасности членами отраслевых организаций или комиссий?

Респонденты, специалисты по безопасности; n = 1690



Более половины респондентов сообщили, что их организации пришлось провести расследование нарушения безопасности.

Приходилось ли вашей организации проводить расследование нарушения безопасности?
Респонденты, специалисты по безопасности; n = 1701



Размещение сетей организации на своей территории является наиболее частым вариантом. О размещении своих сетей в общедоступном облаке сообщили менее 10 % опрошенных.

О размещении сетей за пределами своей организации (в частном или общедоступном облаке) значительно чаще сообщали специалисты по безопасности, чем руководители подразделений.

Уровень развития

Сегменты предсказуемо изменяются после различных действий по развитию систем безопасности.

	Низкий	Ниже среднего	Средний	Выше среднего	Высокий
Руководство компании считает информационную безопасность приоритетной задачей...	22 %	38 %	45 %	71 %	81 %
...и имеет четкие показатели для оценки эффективности программы защиты.	17 %	19 %	32 %	52 %	79 %
Компания имеет четкие и понятные процедуры защиты...	0 %	22 %	15 %	72 %	88 %
...которые оцениваются и контролируются с использованием количественных показателей.	0 %	17 %	33 %	65 %	76 %
...проводятся регулярные проверки методов и инструментов защиты, обеспечивающие их актуальность и эффективность.	0 %	17 %	33 %	65 %	76 %
Компания отлично управляет безопасностью кадровых подразделений, используя процедуру введения в должность и процессы переводов и увольнений.	16 %	27 %	36 %	52 %	76 %
В организации проведена инвентаризация и классификация информационных активов.	17 %	26 %	40 %	58 %	73 %
Компьютерное оборудование моей организации надежно защищено.	17 %	21 %	41 %	63 %	80 %
Уровень интеграции технологий безопасности обеспечивает их эффективную совместную работу.	17 %	21 %	38 %	59 %	78 %
Компания способна обнаружить уязвимости в системе безопасности до возникновения полномасштабных инцидентов.	0 %	23 %	25 %	63 %	70 %

Но не всех...

	Низкий	Ниже среднего	Средний	Выше среднего	Высокий
Определен руководитель высшего звена, непосредственно ответственный за состояние информационной безопасности.	85 %	91 %	88 %	93 %	93 %
Компания имеет документированную формальную стратегию защиты для всей организации и регулярно ее проверяет.	59 %	47 %	58 %	65 %	60 %
Компания следует одному из общепринятых стандартов информационной безопасности (например, ISO 27001).	47 %	44 %	50 %	59 %	54 %

Примечания

1. *Полугодовой отчет Cisco по безопасности, лето 2014 года:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
2. Дополнительные сведения об уязвимостях CMS см. «Wordpress Vulnerabilities: Who Is Minding the Store?», *Отчет Cisco по безопасности, лето 2014 года:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
3. "Goon/Infinity/RIG Exploit Kit Activity," Cisco IntelliShield: Security Activity Bulletin, July 2014: http://tools.cisco.com/security/center/mviewAlert.x?alertId=34999.
4. *Полугодовой отчет Cisco по безопасности, лето 2014 года:* http://www.cisco.com/web/offers/lp/midyear-security-report/index.html?keycode=000489027.
5. "Cisco Event Response: POODLE Vulnerability," 15 октября 2014 г.: http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_Poodle_10152014.html.
6. "OpenSSL Heartbleed vulnerability CVE-2014-0160 – Cisco products and mitigations," блог Cisco по безопасности, 9 апреля 2014 г.: http://blogs.cisco.com/security/openssl-heartbleed-vulnerability-cve-2014-0160-cisco-products-and-mitigations
7. "JP Morgan and Other Banks Struck by Hackers," by Nicole Perlroth, *The New York Times,* 27 августа 2014 г.: http://www.nytimes.com/2014/08/28/technology/hackers-target-banks-including-jpmorgan.html?_r=0; "'Trojan Horse' Bug Lurking in Vital U.S. Computers Since 2011," by Jack Cloherty and Pierre Thomas, ABC News, 6 ноября 2014 г.: http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.
8. "4 Things We Learned from China's 4th Plenum," by Shannon Tiezzi, *The Diplomat,* 23 октября 2014 г.: http://thediplomat.com/2014/10/4-things-we-learned-from-chinas-4th-plenum/.
9. "Brazil's New Internet Law Could Broadly Impact Online Privacy and Data Handling Practices," *Chronicle of Data Protection,* 16 мая 2014 г.: http://www.hldataprotection.com/2014/05/articles/international-eu-privacy/marco-civil-da-internet-brazils-new-internet-law-could-broadly-impact-online-companies-privacy-and-data-handling-practices/.
10. "Russian data localization law may now come into force one year ahead of schedule, in September 2015," by Hogan Lovells, Natalia Gulyaeva, Maria Sedykh, and Bret S. Cohen, Lexology.com, 18 декабря 2014 г.: http://www.lexology.com/library/detail.aspx?g=849ca1a9-2aa2-42a7-902f-32e140af9d1e.
11. "GCHQ Chief Accuses U.S. Tech Giants of Becoming Terrorists' 'Networks of Choice,'" by Ben Quinn, James Ball, and Dominic Rushe, *The Guardian,* 3 ноября 2014 г.: http://www.theguardian.com/uk-news/2014/nov/03/privacy-gchq-spying-robert-hannigan.
12. "Internet Security Necessary for Global Technology Economy," by Mark Chandler, Cisco Blog, 13.05.2014: http://blogs.cisco.com/news/internet-security-necessary-for-global-technology-economy.
13. "Cybersecurity: What the Board of Directors Needs to Ask," ISACA and The Institute of Internal Auditors Research Foundation, август 2014 г.: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cybersecurity-What-the-Board-of-Directors-Needs-to-Ask.aspx.
14. "It's Time for Corporate Boards to Tackle Cybersecurity. Here's Why," by Andrew Nusca, FORTUNE magazine, 25 апреля 2014 г.: http://fortune.com/2014/04/25/its-time-for-corporate-boards-to-tackle-cybersecurity-heres-why/.

Штаб-квартира в США
Корпорация Cisco Systems.
Сан-Хосе (Калифорния)

Штаб-квартира в Азиатско-Тихоокеанском регионе
Cisco Systems (USA) Pte. Ltd.
Сингапур

Штаб-квартира в Европе
Cisco Systems International BV
Амстердам, Нидерланды

Компания Cisco насчитывает более 200 офисов и представительств по всему миру. Адреса, номера телефонов и факсов приведены на веб-сайте Cisco по адресу www.cisco.com/go/offices.