



Атаки на веб- приложения: итоги **2018 года**

Содержание

Введение	2
Резюме	3
Общая статистика	3
Статистика по отраслям	5
IT-компании	6
Финансовые организации	7
Транспортные компании	8
Сфера услуг	9
Государственные учреждения	10
Сфера образования и науки	11
Выводы	12
Об исследовании	13

Г Введение

Исследование актуальных киберугроз 2018 года показало, что взлом веб-приложений является одним из наиболее часто используемых методов кибератак как на организации, так и на частных лиц. Взломанные сайты используются в различных целях — для распространения вредоносного ПО, кражи информации, размещения несанкционированной рекламы или запрещенной информации, мошенничества, проникновения во внутреннюю сеть компании. В настоящем исследовании мы постарались выделить основные угрозы для современных веб-ресурсов, основываясь на статистике веб-атак, выявленных с помощью межсетевого экрана уровня приложения PT Application Firewall. Подробнее о том, какие данные анализировались, можно прочитать в конце отчета. Кроме того, мы взглянули на статистику атак в разрезе отдельных отраслей экономики: это может помочь специалистам по ИБ при оценке актуальных рисков для корпоративных сайтов.

Резюме

Все сайты из любой отрасли ежедневно подвергаются кибератакам. При этом, если атака целенаправленная, отдельные ее шаги можно сопоставить и сложить в единую цепочку. Наибольшее число таких направленных цепочек атак ежедневно фиксировалось на сайтах финансовых организаций (151 цепочка), транспортных компаний (135) и компаний в сфере услуг (114).

Тройка наиболее распространенных атак на веб-сайты не меняется год от года: это «Внедрение SQL-кода» (SQL Injection), «Выход за пределы каталога» (Path Traversal) и «Межсайтовое выполнение сценариев» (Cross-Site Scripting, XSS). Особенности выделяются лишь при рассмотрении разных отраслей.

Вдвое увеличилась доля атак, направленных на получение информации о веб-приложении (Information Leakage). Особенно это видно на примере сайтов госучреждений, где доля подобных атак составила 67% из всех зарегистрированных. При этом, как и прежде, сайты госучреждений подвержены опасным атакам, направленным на получение контроля над сервером и информации из баз данных.

Сайты IT-компаний подвергались главным образом атакам, направленным на получение информации и контроля над приложением. Финансовые организации тем временем в первую очередь страдали от атак на их клиентов, наиболее распространенная из которых — XSS (29% всех атак на сайты в отрасли). Аналогичным атакам подвержены сферы услуг и образования.

Общая статистика

Перечень наиболее распространенных атак со временем практически не меняется: на верхних строчках рейтинга традиционно SQL Injection, Path Traversal и XSS. Суммарно они составляют более половины всех выявляемых кибератак на веб-ресурсы компаний. С одной стороны, это можно объяснить высокой эффективностью подобных атак: согласно нашему [исследованию](#), три четверти сайтов подвержены XSS-атакам, каждое второе веб-приложение содержит проблемы разграничения доступа к ресурсам и каждое третье может быть взломано с помощью внедрения кода. С другой стороны, подобные атаки просты в реализации и могут осуществляться низкоквалифицированными хакерами, в том числе автоматизированно, с использованием общедоступного ПО.

По сравнению с прошлым годом изменилось лишь расположение перечисленных атак в топ-3 рейтинга распространенности. На то, какая из атак окажется более распространенной, сильно влияет выборка рассматриваемых веб-приложений. Например, если в приложении отсутствует функциональность, подразумевающая ввод пользовательских данных, то вполне логично, что атакующие будут проводить какие-то другие атаки, не связанные с попытками повлиять на логику работы приложения через пользовательский ввод.

Из особенностей, которые мы отметили по результатам анализа атак в 2018 году: вдвое возросла доля атак, направленных на получение информации о приложении (Information Leakage), особенно заметна эта тенденция для сайтов госучреждений. При этом доля XSS-атак

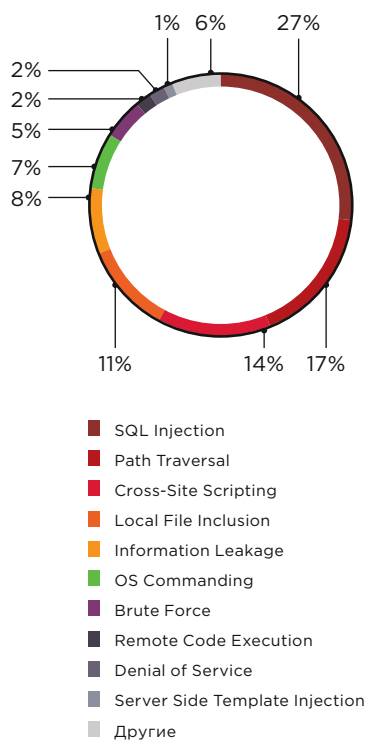


Рисунок 1. Топ-10 атак на веб-приложения

заметно сократилась. Но мы не делаем вывода, что атаки на клиентов теряют популярность, такая картина скорее следствие увеличения числа атак других категорий, например Path Traversal. Далее мы покажем, что вне зависимости от отрасли, к которой относится сайт, XSS непременно располагается на верхних строчках рейтингов по распространенности.

Любой сайт, доступный из интернета, ежедневно сканируется на наличие уязвимостей или подвергается различного рода атакам. Такие сканирования не означают, что каждый сайт непременно пытаются взломать. Например, преступник может просто проверять доступные адреса на наличие уязвимых систем или отрабатывать какой-то новый скрипт на большом списке адресов.

Если же злоумышленник поставил цель получить информацию или доступ к конкретному сайту, то его действия не ограничиваются единичными попытками, ведь он не знает точно, какие уязвимости присутствуют в системе. Поэтому в случае целенаправленного взлома сайта единичные события, даже распределенные по времени, складываются в общую цепочку. Такая цепочка может состоять из десятков, сотен или даже тысяч событий в день. Возможность обнаружить всю цепочку взаимосвязанных событий позволяет локализовать угрозу и эффективно защитить ресурсы. Используя функциональность РТ Application Firewall, мы определили связи между отдельными атаками и объединили их, это позволило подсчитать и сравнить среднее число именно целенаправленных цепочек атак, которые фиксируются на сайтах компаний из разных отраслей.

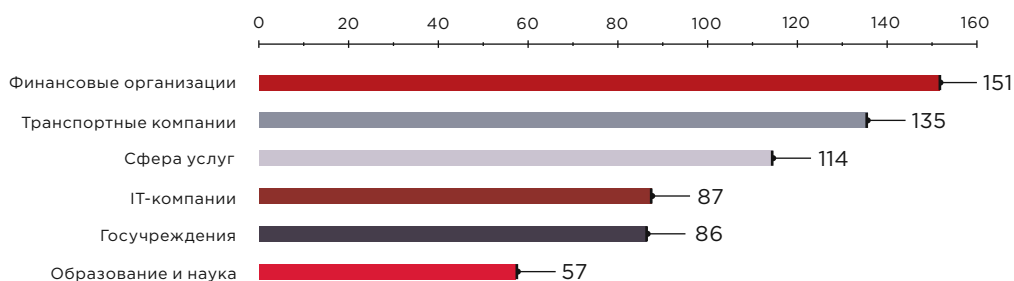


Рисунок 2. Среднее число целенаправленных атак в день на одно веб-приложение

Чтобы усложнить выявление и блокировку атак, хакеры могут скрывать IP-адрес источника запросов, данные User Agent и другие идентификаторы. Это довольно просто организовать с помощью автоматизированных скриптов и проксирования трафика через сторонние серверы. Такие прокси-серверы могут находиться в разных странах, поэтому определить реальное местонахождение атакующего непросто. Это усложняет атрибуцию атаки и при отсутствии дополнительной информации делает ее бессмысленной. К примеру, в рамках нашего исследования было зафиксировано в общей сложности более 12 000 источников атак из 90 стран.

Статистика по отраслям

Рассмотрим, **какие атаки были характерны для веб-приложений в зависимости от сферы деятельности компании**

IT-компании

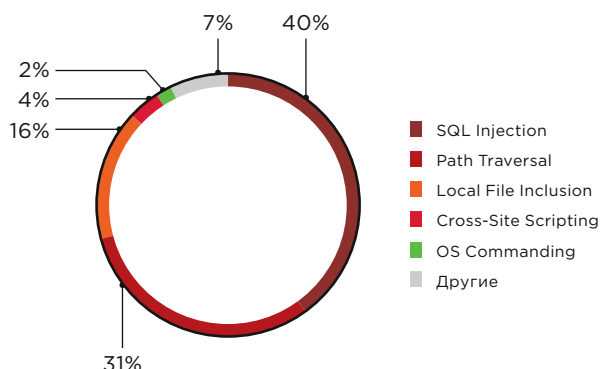


Рисунок 3. Топ-5 атак на веб-приложения IT-компаний

Подавляющее большинство атак на сайты IT-компаний направлены на получение информации. Это атаки «Внедрение SQL-кода» (SQL Injection) и «Выход за пределы каталога» (Path Traversal). Первая, как известно, позволяет получать информацию из базы данных веб-приложения (например, учетные данные пользователей сайта, персональные данные, информацию о самой базе и таблицах в ней и т. п.) или даже выполнять команды на сервере. Нередко успешная реализация такой атаки приводит к полной компрометации сайта и получению контроля над сервером. С помощью атаки Path Traversal злоумышленник может просмотреть содержимое тех папок на сервере, которые не должны быть доступны обычному пользователю даже в случае авторизации на сайте. Это могут быть конфигурационные файлы установленного ПО и ОС, исходный код сайта, другие важные данные. Для реализации атаки Path Traversal нарушителю необходимо знать или подобрать правильные название и путь к файлу, который он хочет прочитать. Поэтому такая атака, как правило, не ограничивается одной попыткой, и в консоли системы защиты можно заметить целую цепочку однотипных событий. Наиболее часто хакеры пытаются прочитать файл /etc/passwd, в котором хранится информация о пользователях Linux. На следующих скриншотах видно, как атакующий пытается определить место расположения этого файла, используя в GET-запросах символы точки и косой черты (%2f в формате URL Encoding) для перехода на каталог выше в файловой системе.

```
1 GET / source=..%2f%2fpasswd HTTP/1.1
2 Accept: Text/Html,Application/Xhtml Xml,Application/Xml;q=0.9,*/*;q=0.8
3 Connection: keep-alive
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Rv:50.0) Gecko/20100101 Firefox/50.0
5 Accept-Language: en-us,en;q=0.5
6 Referer: http://.com/ source=..%2f%2fpasswd
7 Accept-Encoding: gzip
```

Рисунок 4. Попытка прочитать файл /etc/passwd перейдя на один каталог выше относительно текущего

```
Скачать
1 GET / source=..%2f..%2f..%2f..%2f..%2f..%2fpasswd
2 Accept: Text/Html,Application/Xhtml Xml,Application/Xml;q=0.9,*/*;q=0.8
3 Connection: keep-alive
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Rv:50.0) Gecko/20100101 Firefox/50.0
5 Accept-Language: en-us,en;q=0.5
6 Referer: http://.com/ source=..%2f..%2f..%2f..%2f..%2f..%2fpasswd
7 Accept-Encoding: gzip
```

Рисунок 5. Попытка прочитать файл /etc/passwd перейдя на шесть каталогов выше относительно текущего

Обе атаки крайне опасны. Если приложение уязвимо и при этом обрабатывает данные пользователей, неизбежны утечки информации. По нашей статистике, 46% всех атак на организации сферы информационных технологий в 2018 году были нацелены именно на веб-ресурсы, а 40% атак преследовали цель кражи данных. Поэтому IT-компаниям следует обратить внимание на защищенность своих сайтов и безопасность обрабатываемой на них информации. Если сайт компании расположен не на хостинге, а внутри корпоративной инфраструктуры, необходимо учитывать риски проникновения злоумышленника в локальную сеть в результате компрометации веб-приложения.

Финансовые организации

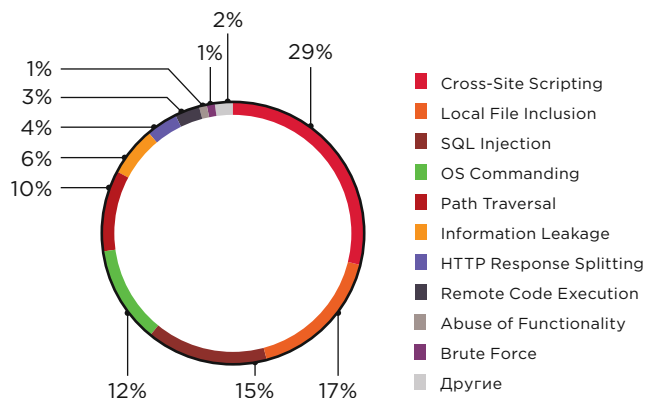


Рисунок 6. Топ-10 атак на веб-приложения финансовых организаций

Веб-приложения финансовых компаний с точки зрения рисков выделяются на фоне сайтов организаций из других отраслей. В первую очередь стоит отметить банковские сервисы, которые предоставляют пользователям возможность распоряжаться их деньгами — оплачивать услуги, открывать вклады и брать кредиты, переводить средства другим пользователям. Даже если не рассматривать системы онлайн-банкинга, а взять официальный сайт компании, то риски его компрометации будут не менее весомы. Например, если с сайта банка будет распространяться вредоносное ПО или будут вестись фишинговые атаки, в первую очередь пострадают клиенты. Именно атаки на клиентов располагаются на первой строчке по распространенности среди атак на веб-приложения финансовых организаций, в частности «Межсайтовое выполнение сценариев» (Cross-Site Scripting). Важно отметить, что это одна из самых распространенных уязвимостей веб-приложений в 2018 году.

Для самой финансовой организации риск атаки на клиентов не связан напрямую с финансовым ущербом, скорее речь идет о репутационных потерях. Поэтому если банк проводит анализ защищенности или тестирование на проникновение, то по результатам таких работ в первую очередь устраняются наиболее опасные уязвимости. Следовательно, крайне важно применять системы класса web application firewall для защиты сайтов от атак, это позволит обезопасить пользователей даже при наличии уязвимостей в приложении.

Транспортные компании

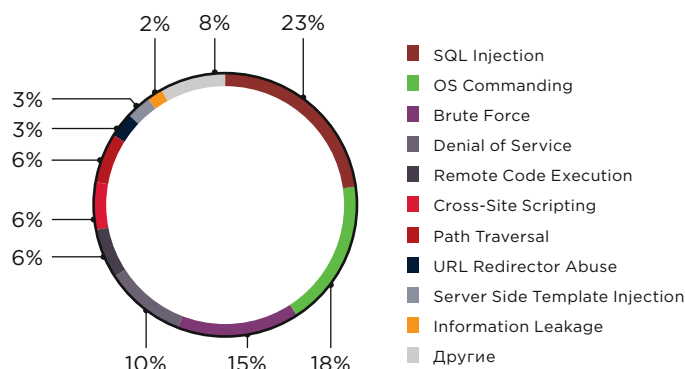


Рисунок 7. Топ-10 атак на веб-приложения транспортных компаний

Сайты транспортных компаний сегодня не ограничиваются информационными страницами с расписанием рейсов или условиями перевозки грузов. Как правило, такие веб-приложения предоставляют сервисы оплаты, например для покупки билетов. Это привлекает хакеров, которые рассчитывают взломать такие сервисы и похитить данные банковских карт клиентов. Живой пример подобной атаки — [кража данных клиентов авиакомпании British Airways](#) в августе-сентябре 2018 года. Хакеры взломали сайт и модифицировали один из скриптов, добавив в него собственный код (JS-сниффер). В итоге были похищены данные порядка 380 000 клиентов компании, в том числе платежная информация.

Чтобы осуществить подобную атаку нарушителю нужно получить контроль над сервером или доступ к странице администрирования веб-приложения. Согласно нашему исследованию, более половины атак на веб-сайты транспортных компаний так или иначе могут привести к их компрометации, в том числе обычный подбор учетных данных или использование уязвимостей устаревшего ПО. На рисунке ниже показано, как атакующие пытались использовать эксплойт для известной уязвимости в популярном фреймворке, чтобы перехватить управление сервером.

```
1 GET /signin.action HTTP/1.1
2 Accept-Encoding: gzip;q=1.0,deflate;q=0.6,identity;q=0.3
3 Accept: */*
4 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
5 Host:
6 Content-Type: multipart/form-data; (#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(# memberAccess?{# membe
Access=#dm):({#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInst
ance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcl
udedClasses().clear()).(#context.setMemberAccess(#dm))).(#cmd='ping -c 3 || ping -n 3
').(#iswin=@java.lang.System@getProperty('os.name').toLowerCase().contains('win')).(#cmds=
(#iswin?'cmd.exe','/c',#cmd):{'/bin/bash','-c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorSt
ream(true)).(#process=#p.start()).(#ros=@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())
```

Рисунок 8. Попытка эксплуатации уязвимости CVE-2017-5638 в фреймворке Apache Struts 2

Любая компания, которая предоставляет сервис оплаты на сайте, должна учитывать и минимизировать подобные риски.

Сфера услуг

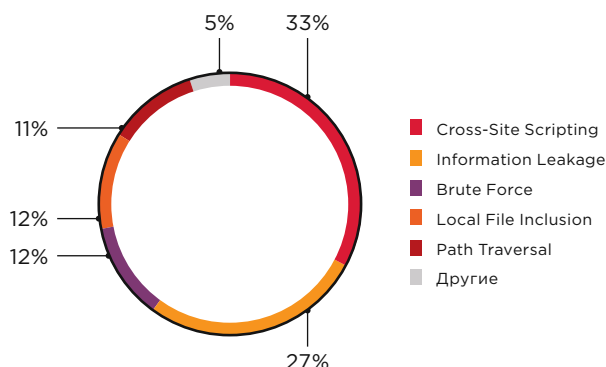


Рисунок 9. Топ-5 атак на веб-приложения компаний сферы услуг

В зависимости от предоставляемых сервисов организации из сферы услуг могут иметь на своих сайтах различную функциональность. Например, на сайтах гостиниц будет форма заявки на бронирование, где клиенту предлагается оставить персональные данные. Кроме того, любой посетитель желает найти на сайте такой компании и удобную форму оплаты услуг, а значит, сайт может быть взломан с целью внедрения в его код сниффера для кражи платежных данных пользователей. В любом случае все подобные веб-приложения ориентированы на клиентов, и данные пользователей должны быть ценным активом для этих организаций.

Утечка базы данных или удар по репутации компании, вызванные кибератакой, могут существенно сказаться на развитии бизнеса и конкурентоспособности компании на рынке. При этом наше исследование подтверждает, что большинство кибератак в отношении сайтов в сфере услуг проводятся либо непосредственно на клиентов, либо с целью получения информации, обрабатываемой в веб-приложении. Поэтому, чтобы избежать вреда для репутации компании, необходимо серьезно относиться к защите веб-ресурсов. Например, если вы заказали разработку веб-сайта, то необходимо учитывать в техническом задании и при приемке кода не только красивый дизайн, удобство и широкий набор функций, но и безопасность.

Государственные учреждения

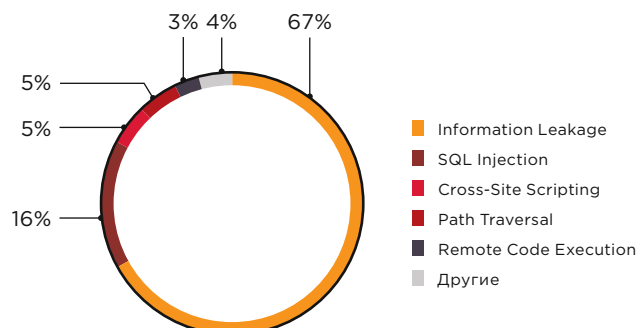


Рисунок 10. Топ-5 атак на веб-приложения госучреждений

В 2017 году мы фиксировали в основном типовые атаки на сайты госучреждений — «Межсайтовое выполнение сценариев» (Cross-Site Scripting) и «Внедрение SQL-кода» (SQL Injection). В 2018 году подобные атаки также фиксировались в достаточном объеме (как и крайне опасные Remote Code Execution, позволяющие получить контроль над сервером), но на их фоне заметно выделяются другие — направленные на раскрытие информации о веб-приложении (Information Leakage). В частности, были обнаружены множественные попытки получить доступ к каталогам .svn или .git, в которых могут храниться актуальные файлы исходного кода системы. Доступ к таким файлам позволяет злоумышленнику проанализировать сайт на наличие уязвимостей, которые обычно не могут быть выявлены со стороны типового внешнего нарушителя. По сути злоумышленник получает возможность взглянуть на сайт глазами его разработчика, а значит — увидеть все допущенные этим разработчиком ошибки.

```
1 GET /.git/config HTTP/1.1
2 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.12) Gecko/20101026 Firefox/3.6.12
3 Host:
4 Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
5 Cache-Control: no-cache
6 Connection: Keep-Alive
7 Keep-Alive: 300
```

Рисунок 11. Попытка получения доступа к файлам каталога .git

```
1 GET /.svn/entries HTTP/1.1
2 Host:
3 Connection: keep-alive
4 Accept: */*
5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/71.0.3578.98 Safari/537.36
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
```

Рисунок 12. Попытка получения доступа к файлам каталога .svn

Проблема небезопасного хранения папок с информацией о файлах проекта и их изменениях известна довольно давно. Мы обращали на нее внимание еще в исследовании 2017 года, рассказывая о наиболее распространенных сценариях атак для проникновения внешнего нарушителя в локальную сеть организаций. Эти атаки актуальны и сегодня. Чтобы определить, уязвим ли ваш сайт, необходимо обратиться к нему по адресам `http://example.com/.git/HEAD` и `http://example.com/.svn/entries`. Если приложение безопасно, должна вернуться ошибка с сообщением о том, что страница не найдена. В противном случае стоит удалить каталоги .git и .svn. Для работы веб-сайта они не требуются, их наличие можно считать ошибкой администрирования.

Сфера образования и науки

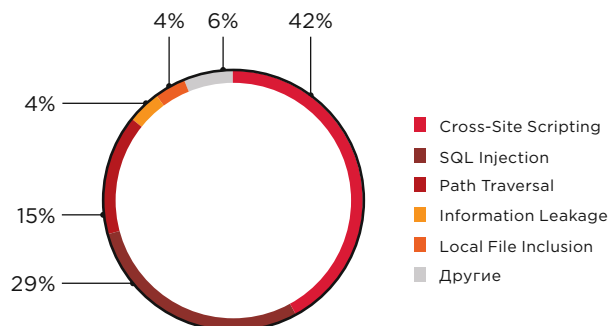


Рисунок 13. Топ-5 атак на веб-приложения организаций сферы образования и науки

Распределение атак на организации сферы образования и науки отражает общие тренды кибератак на веб-ресурсы, отмеченные в начале данного отчета при рассмотрении общей статистики (см. рисунок 1). В исследовании актуальных киберугроз 2018 года мы отмечали, что хакеры атакуют такие организации не только с целью получения информации о сотрудниках и учащихся или экзаменационных вопросах, но и с целью кражи важных сведений о новых разработках, а взлом веб-приложений входит в пятерку наиболее распространенных методов злоумышленников, он был использован в 12% кибератак на сайты университетов и других учебных заведений. Поэтому при организации защиты интеллектуальной собственности от хищения необходимо учитывать и риски проникновения нарушителя в сеть учреждения через уязвимые веб-сайты.

В то же время другое исследование, проведенное нами на основании опроса руководителей российских региональных компаний, показало, что бюджет современных образовательных учреждений на информационную безопасность достаточно низок, для 83% таких организаций он не превышает 2 млн рублей. Это приводит к тому, что организации не могут эффективно выявлять и предотвращать инциденты ИБ, в том числе атаки на сайты: средств недостаточно для внедрения систем защиты. В итоге 67% образовательных учреждений отметили прямые финансовые убытки от кибератак. В условиях ограниченности бюджета мы советуем выделить наиболее ценные активы и обеспечить их комплексную защиту. Кроме того, стоит растить собственных специалистов по ИБ внутри учебного заведения.

Г Выводы

Наиболее распространены самые простые и эффективные атаки — «Внедрение SQL-кода» (SQL Injection), «Выход за пределы каталога» (Path Traversal) и «Межсайтовое выполнение сценариев» (Cross-Site Scripting). Хакер может проводить атаку не только для получения доступа к конкретному сайту. Сегодня все чаще целью атаки становятся данные клиентов — персональные, платежные. Кроме того, мы наблюдаем атаки, направленные на заражение сайта вредоносным ПО; это позволяет злоумышленникам охватить большее число жертв, а также использовать уязвимые веб-ресурсы в целевых заражениях методом watering hole.

Полученные результаты подтверждают и еще один важный вывод: вне зависимости от отрасли сайт любой компании ежедневно находится под угрозой. И если организация стремится обезопасить свои ресурсы и не желает потерять репутацию из-за атак на клиентов, необходимо задуматься о защите. Наше [исследование](#) защищенности корпоративной инфраструктуры современных организаций показало, что для проникновения во внутреннюю сеть компании хакеру достаточно использовать всего одну или две уязвимости, причем 75% векторов проникновения основаны именно на недостатках защиты веб-сайтов.

Для защиты веб-приложений мы рекомендуем следующие меры:

- Используйте межсетевые экраны уровня приложения (web application firewalls, WAF) для защиты сайтов от атак. Это позволит обезопасить веб-приложение даже в случае наличия в нем уязвимостей или появления в будущем новых угроз. Межсетевой экран должен не только обеспечивать противодействие известным атакам на уровне приложения и бизнес-логики, но и выявлять эксплуатацию уязвимостей нулевого дня, предотвращать атаки на пользователей, анализировать и сопоставлять множество событий для выявления цепочек атак, что возможно только при использовании инновационных технологий нормализации, эвристического и поведенческого анализа и самообучения. Полезной функцией будет также взаимодействие с внешними системами сбора и анализа событий (SIEM) и оповещение средств защиты от DDoS сетевого уровня. Возможность интеграции WAF со средствами автоматизированного анализа исходного кода позволит использовать так называемый virtual patching, который может закрыть от атаки уязвимость до ее устранения на уровне кода.
- Регулярно проводите анализ защищенности веб-приложений и устраняйте выявленные уязвимости. Наиболее эффективен анализ методом белого ящика (когда специалистам по безопасности доступен исходный код системы). Рекомендуется проводить такой анализ на всех этапах жизненного цикла сайта, а не только при приемке кода или перед вводом системы в эксплуатацию.
- Не используйте устаревшие версии веб-серверов, ОС, систем управления контентом, библиотек и другого ПО. Регулярно обновляйте системы и устанавливайте актуальные патчи.
- Регистрируйте обнаруженные киберинциденты и проводите их расследование, чтобы своевременно определить источник угрозы и минимизировать риски.

Об исследовании

Компания Positive Technologies завоевала лидирующие позиции на отечественном и европейском рынке систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Ежегодно мы осуществляем сотни пилотных проектов и внедрений наших средств защиты информации в корпоративные системы ведущих российских и международных компаний. Для данного исследования были выбраны 28 веб-приложений, расположенные на сетевом периметре организаций из разных отраслей экономики и защищенные с помощью PT Application Firewall. Цель исследования — продемонстрировать актуальные тренды атак на веб-приложения, которые мы отметили по итогам 2018 года. Исследование проведено на основе пилотных проектов, заказчики которых дали согласие на использование результатов работ в исследовательских целях, а также на основе данных от экземпляров PT Application Firewall, защищающих сайты нашей компании (эти данные вошли в отрасль IT).

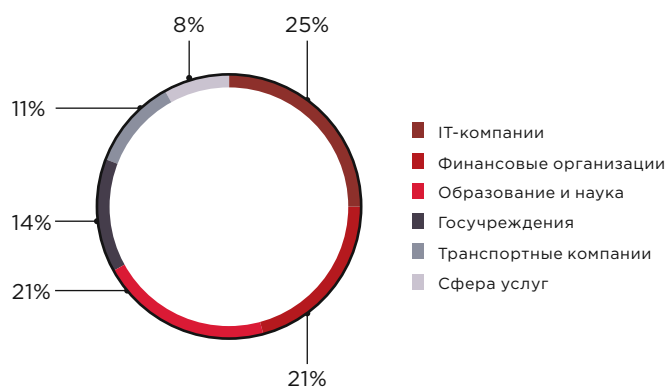


Рисунок 14. Портрет участников

Всего в рамках исследования было проанализировано порядка 140 000 атак. Инциденты, связанные с обнаружением сканеров веб-уязвимостей, были изначально исключены из рассмотрения и не входят в это число. Также были исключены ложные срабатывания, которые неизбежны при работе систем защиты.

Выводы, сделанные по итогам работ, могут не отражать актуальное состояние защищенности информационных систем в других компаниях рассмотренных отраслей. Исследование проведено с целью обратить внимание специалистов по ИБ в различных отраслях на наиболее актуальные проблемы безопасности веб-приложений и помочь им своевременно определить и минимизировать риски.

О компании

ptsecurity.com

pt@ptsecurity.com

facebook.com/PositiveTechnologies

facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.