Краткий отчет

Годовой отчет Cisco по безопасности за 2015 год

Какой бы изменичвой 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 защитники, а именно 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. *Годовой отчет Cisco по безопасности за 2015 год* разделен на четыре темы для обсуждения. Эти разделы, а также проблемы, рассматриваемые в них, могут на первый взгляд показаться совершенно несовместимыми. Однако при более внимательном изучении вы обязательно заметите взаимосвязи.

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

1. Анализ угроз.
2. Сравнительное исследование возможностей систем безопасности.
3. Геополитические и отраслевые тенденции.
4. Изменение взгляда на информационную безопасность – от пользователей к совету директоров.

Загрузить годовой отчет по безопасности Cisco за 2015 год: www.cisco.com/go/asr2015.

1. Анализ 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 по безопасности Cisco 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 к совету 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 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.

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.

Cisco и логотип Cisco – товарные знаки или зарегистрированные товарные знаки корпорации Cisco и/или ее дочерних компаний в США и других странах. Чтобы просмотреть список товарных знаков Cisco, перейдите по ссылке www.cisco.com/go/trademarks. Товарные знаки других организаций, упомянутые в настоящем документе, – собственность соответствующих владельцев. Использование слова «партнер» не означает партнерских отношений между Cisco и любой другой компанией. (1110R)