электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056.53

Защита информации компьютерных сетей от внутренних и внешних пользователей

 # 08, август 2012

М.А. Логинова

Студентка,
кафедра «Программное обеспечение ЭВМ, информационные технологии и прикладная математика»

Научный руководитель: Ю.С. Белов,
к.ф.-м.н., доцент кафедры «Программное обеспечение ЭВМ, информационные технологии и прикладная математика»

МГТУ им. Н.Э. Баумана
lmbunny@yandex.ru

Область исследования.

Вместе с мировой глобализацией количество пользователей подключенных к интернету постоянно увеличивается. Интернет в этом отношении стал центральным рынком в мире, где каждая компания может иметь интернет-магазин или стремится приобрести его. Информация о финансовых учреждениях, предприятиях, школах, университетах, министерствах Российской Федерации, больницах это лишь малая часть из того, что доступно в Интернете. Быстрое развитие бизнеса в интернете и скорость технического прогресса, привнесли новую степень неустойчивости, которая угрожает репутации компаний, их надежности и конкурентоспособности.

Каждая компания должна защитить себя от внутренних и внешних угроз начиная с обеспечения безопасности компьютерной сети и заканчивая защитой коммерческой тайны. Например, один из банков Великобритании, потерял миллионы фунтов в течение двух лет, когда два сотрудника крупной компании совершили кражу важных документом по сети. Кражи оставались незамеченными в течение всего первого года, потому что компания не ожидала угроз безопасности в этом сегменте своей деятельности внутри компании [1].

Предприятия, которые полагаются на Интернет-технологии, чтобы поставлять и распространять свои товары и услуги все чаще сталкиваются с проблемами информационной безопасности. Атаки хакеров и другие кибер-преступников, включая внутренних пользователей или сотрудников компаний, становятся все более изощренными, агрессивными и, к сожалению, успешными, при использовании уязвимостей для проникновения и кражи информации в сети.

Исследование проблемы

Халатность при развертывании эффективной и современной системы безопасности компьютерных сетей и постоянно растущие расходы, связанные с этим

аппаратом, приведет к более значительным потерям для большинства компаний, использующих сетевые ресурсы.

Финансовые потери в следствии зарегистрированных в Интернете преступлений достигло рекордного количества в 2007 году, согласно Центру регистрации интернет-преступлений (IC3). IC3 получил 206884 жалоб в 2007 году через свой веб-сайт, меньше, чем количество представленных в 2006 году (207 492), 2005 (231493) или 2004 (207449). IC3 направил 90008 зарегистрированных преступлений в соответствующие правоохранительные органы для расследования, большинство из которых являются мошенничествами и финансовыми кражами. Общий убыток составил $ 239 090 000, со средним убытком в $ 680 за каждым заявителем. Это представляет собой увеличение по сравнению с 2006 в общей сложности на $ 198 440 000 [2].

В основном убытки несут сети, где электронная техника (средства защиты, например, межсетевые экраны Cisco), имеются, но как правило, не настроены должным образом за счет отсутствия соответствующих навыков персонала, необходимых для этого оборудования. Настройка, например, Cisco и Huawei сетевых устройств требует сертифицированного специалиста по созданию эффективной и оптимизированной системы. Постоянная эволюция этих устройств вынуждает специалистов идти в ногу с развитием их конфигураций. Хотя новые системы оборудования, как правило, основаны на старых настройках, там, как правило, находится больше изменений для решения проблем увеличения возрастающих угроз и уязвимостей старых версий[3].

Сетевые администраторы, которые имеют надлежащую подготовку по соответствующему оборудованию различных производителей могут эффективно и надежно настроить электронную технику, в следствии чего взлом изнутри или снаружи становится чрезвычайно сложным и практически невозможен, предполагая, что нет никакой халатности со стороны администраторов. Если вернуться к обеспечению безопасности сетевых устройств техники компании Cisco, продукция которой является одной из наиболее широко используемых в мире и при этом большинство администраторов едва имеют достаточные навыки по настройке этих устройств. Большинство этих устройств поставляются с настройками по умолчанию, что пользователи просто подключи аппаратуру и тут же использовали её [4]. Следствием этого является то, что большая часть таких устройств не оптимизированы и обычно оставляет множество лазеек для злоумышленников. Другой компанией широко известной на рынке сетевых устройств является Juniper, она также предоставляет пользователям устройства, которые иногда предварительно настроенны. Производители оборудования обычно предоставляют руководства для всех продуктов, но это, однако, не достаточно, чтобы настроить эти устройства правильно. Настройка этих устройств требует необходимого сочетания следующих сервисов: систем анти-вируса, анти-спама, предотвращения вторжений, веб-фильтрации, тестирования проникновений а также обеспечения контроля доступа к информации в сети. Настройка сетевого оборудования надлежащим образом как упоминалось выше, является первостепенной задачей в связи с динамичным характером развития методов атак.

Методология

В данном разделе рассматриваются несколько способов, в следствии которых сеть может быть надежно сконфигурирована. В этой главе мы рассмотрим, пути подготовки администраторов, покупку различных видов специализированного оборудования, сетевые системы контроля доступа а также политики компании в сфере обеспечения безопасности.

Администраторам необходимо иметь определенную подготовку для каждого типа сетевого оборудования, которыми они управляют. Это очень важно для оптимальной настройки. Поэтому многие компании каждый год проводят ряд специализированных тренингов, с участием специалистов компаний предоставляющих оборудование [5]. По окончании обучения, лабораторных работ и тестирования, сотрудники получают сертификаты. Они являются подтверждением того, что физическое лицо является компетентным и компания может нанять квалифицированного администратора для работы в области компьютерных сетей.

Но даже на небольших предприятиях сетевые устройства, имеющие, параметры по умолчанию, в большинстве случаев, должны подвергаться обязательной перенастройке специалистами для уменьшения риска потери данных и финансовых потерь из за действий для злоумышленников [6].

Последствия для бюджета компании при покупки сетевого оборудования без оптимального использования иногда могут быть катастрофическими. Обучение администраторов может помочь в разработке сетей и реализации стоимости оборудования при использовании правильной спецификации. Преимуществом этого является эффективная экономии средств. Накопленные сбережения могут быть использованы для активной модернизации других уязвимых сегментов сети. Защита сети от внутренних атак требует хорошей сегментации сети и контроля доступа. Доступ должен быть разделен по принципу "необходимости использования" сегментов сети. В прошлом, большинство компьютеров, подключенных к сети, имели полный доступ практически к любому другому компьютеру в сети, а также полный доступ к Интернету. Политика управление доступом в сети описывает роли каждого домена ресурсов, таких как серверы, интернет-серверы, принтеры, сканеры, компьютеры пользователей и определяет допустимые потоки связи между ними. Это позволяет администраторам проводить широкие мониторинги, активно контролировать и отслеживать любое незаконное вторжение.

Оценка влияния

На основании собранных нами данных, мы смогли провести статистический анализ, чтобы убедиться, что существует корреляция между сетевым уровнем знаний и сертификации сетевых администраторов и количеством успешных атак на сеть.

Для этого мы рассмотрели уровень сертификации администраторов и сравнили его с числом успешных атак. Мы также рассмотрели компании, которые могут нанять специалистов для тренинга сертифицированных администраторов и компании, которые не могут себе этого позволить. Это позволило нам сделать вывод относительно отдачи от инвестиций и типа нанимаемых администраторов. Также был оценен тип оборудования и уровень компетентности сотрудников.

Большинство компаний будут рады видеть снижение финансовых потерь за счет снижения уровня успешных атак на сеть. Это является хорошим стимулом для компании чтобы нанять сертифицированных специалистов. Еще одной важной областью, является повышение уровня общественного доверия. Покупатели интернет-магазинов будут гораздо охотнее иметь дело с компанией, в которой информация о пользователях будет надежно защищена. При увеличении общественного доверия повышается и имидж компании. Инвесторы, также будут больше заинтересованы и смогут предложить больше средств надежной компании [7].

Так как безопасность сети во многом зависит от действий администраторов и их способности эффективно настраивать и управлять оборудованием, это имеет

первостепенное значение. Необходимо быть в курсе современных тенденций нападения, предупреждения атак, технологий и способов борьбы с постоянно меняющейся обстановке. Люди все еще беспокоятся о конфиденциальности, уровне доверия, безопасности, и надежности. Существуют также опасения по поводу доступа, репутации, устойчивости, ответственности, подлинности авторства, права собственности, надзора и контроля, компьютерной грамотности [8].

Можно сделать вывод в том, что все мы должны быть бдительными и помнить о преимуществах и последствиях быстро распространяющихся компьютерных сетей. Из-за отсутствия обучения или чистой небрежности, компании иногда оказываются беспомощными перед лицом атак, которые становятся все более и более сложными и закулисными.

Решения обеспечения безопасности от известных производителей, реализующих средства и программное обеспечение для управления записями и уязвимостями помогают компаниям соответствовать стандартам безопасности. На другом конце цепи, повышения осведомленности пользователей и наличие более интуитивно понятных и прозрачных средств защиты для сетей. Это будет являться ключевыми направлениями развития в будущем.

Список литературы:

1. Chinese man in US accused of trade secret theft // Business Week. – 2009. – April 10. http://www.businessweek.com/ap/financialnews/D97FOTH80.htm (дата обращения: 17.11.2011).

2. Financial Fraud and Internet Banking: Threats and Countermeasures By François Paget/ / McAfee® Avert® Labs. http://www.mcafee.com (дата обращения: 21.11.2011).

3. Parent F. Managing Cisco network security, Syngress, 2000. – 497 с.

4. Timm C., Edwards W. CCNP: Building scalable Cisco internetworks. Stydy guide, Sybex, 2004. – С. 112-115.

5. Rhee M.Y. Internet security: cryptographic principles, algorithms, and protocols, Wiley, 2003. – 426 с.

6. Xia Zheng You, Zhang Shiyong. A kind of network security behavior model // Parallel and Distributed Computing, Applications and Technologies, 2003. – P. 950-954.

7. Morris B.S. Network Management, MIBs and MPLS: Principles, Design and Implementation, Prentice Hall, 2003. – 416 с.

8. Popoviciu N., Baicu F. A new approach for an unitary risk theory // Proceedings ofthe 7th WSEAS International Conference on Signal Processing, Computational Geometry & Artificial Vision. Athens, Greece, 2007 – P. 216-220.