ПРОБЛЕМЫ НАРУШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В УСЛОВИЯХ ИНФОРМАЦИОННОГО ОБЩЕСТВА

Аурика МИРОНЮК, Дарья ПОЛЮГА
National Forestry University of Ukraine
Silvia GANGAN
Universitatea Tehnică a Moldovei

Аннотация: *The article Discusses the basic concepts and issues, forms and methods of information security, the use of modern technologies of computer security, data security in computer systems, methods of information protection, formation of the information security policy.*

Ключевые слова: *компьютерная безопасность, информационная безопасность, защита, информация.*

1. Проблемы, формы и способы информационной безопасности.

В общем случае информационную безопасность общества, государства, личности можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью. Информационная безопасность касается обеспечения таких необходимых качеств информации как конфиденциальность, целостность и доступность.

При анализе проблем информационной безопасности в методологическом плане наиболее важным является:

- определение и обоснование понятийного аппарата;
- налаживание структурно-функциональных связей базовых понятий и разработка на этой основе соответствующих нормативно-правовых основ системы информационной безопасности общества;
- совершенствование системы управления информационной безопасностью на государственном и местном уровнях;
- определение критериев эффективности системы информационной безопасности в различных сферах жизни и деятельности общества (политической, экономической, науки и техники, духовной и т.д.).

В целом система информационной безопасности должна отражать состояние защищенности общественных, национальных, личных интересов именно в информационной сфере от внешних и внутренних угроз, как для самого социума, так и для конкретного человека. Система информационной безопасности является одновременно и элементом в системе высшего уровня - международного, национального, местного. Но сегодня ряд подсистем, входящих в состав этой макросистемы, еще не изучены на должном уровне, а также не имеют комплексного, системного исследования с выходом на современные конструкции и предложения. Изучение научно-теоретических и практических проблем информационной безопасности позволит определить и решить задачи по созданию глобальных систем информационной безопасности, которые бы функционировали эффективно.

Государственная система составляет важнейшее звено системы информационной безопасности личности, общества и государства в правовом государстве.

Основными задачами такой системы являются :

- выявление и прогнозирование дестабилизирующих факторов и информационных угроз жизненно важным интересам личности, общества и государства;
- осуществление комплекса оперативных и долговременных мер по их предупреждению и устранению;
- создание и поддержание в готовности сил и средств обеспечения информационной безопасности.

В основу обеспечения информационной безопасности в условиях информационного общества должны быть положены следующие принципы: законность, соблюдение баланса интересов личности, общества и государства; взаимная ответственность субъектов обеспечения информационной безопасности; интеграция систем национальной и международной безопасности. Специфическими принципами обеспечения информационной безопасности являются как превентивный характер

проведения ее мероприятий по отношению к мероприятиям других видов безопасности, так и адекватная информированность объектов безопасности, в том числе и международных.

Формы и способы обеспечения информационной безопасности образуют собственно инструмент, с помощью которого силы информационной безопасности решают весь комплекс задач по защите жизненно важных интересов личности, общества и государства. Поэтому необходимо их четкое юридическое оформление при разработке нормативных актов, регулирующих деятельность органов информационной безопасности. Важнейшее требование к обоснованию способов, форм и механизмов их реализации заключается в абсолютном верховенстве права в любой, в том числе и политической деятельности. В свою очередь, каждый субъект информационного процесса должен иметь соответствующую правовое сознание, быть законопослушным, хорошо представлять последствия своих действий для других субъектов и меру ответственности в случае нарушения их жизненно важных интересов. Это является принципиальным, поскольку применение тех или иных форм и способов зависит от того, являются информационные угрозы следствием непреднамеренных или же умышленных действий субъектов информационного процесса. В первом случае обеспечение информационной безопасности осуществляется соответственно в формах информационного патроната и информационной кооперации, во втором - в форме информационного противоборства.

В основе прав и свобод государства в сфере его информированности по вопросам мировой политики, экономики, науки, ресурсов, экологии, обороны и т.д. лежат действующие нормы и принципы межгосударственного права. Главным следует считать принцип равной безопасности. Применительно к информационной сфере можно говорить о его трансформации в принцип адекватной информированности государств мирового сообщества. Данный принцип предусматривает право каждого государства на информационную безопасность, обеспечение информационной безопасности всех членов сообщества в равной степени, учета интересов всех сторон без какой-либо дискриминации, исключения односторонних преимуществ, отказ от действий, которые наносят ущерб другому государству.

Законодательная база, которая определяет перечень сведений, отнесенных к государственной тайне, механизм и порядок ее защиты должны разрабатываться, исходя из указанного принципа, а также многосторонних соглашений государств, которые входят в международную систему информационной безопасности. Формирование последней будет, очевидно, делом далекой перспективы, которая ознаменует собой высший уровень проявления доверия и заинтересованности государств мирового сообщества в обеспечении выполнения на практике принципа адекватной информированности. Такая система должна стать подсистемой в системе коллективной безопасности.

Широкое использование информационных технологий во всех сферах жизни общества делает весьма актуальной проблему защиты информации, ее пользователей, информационных ресурсов, каналов передачи данных. Возрастает осознание того, что наиболее опасными источниками угроз личным и общественным интересам в информационном обществе может стать неконтролируемое распространение информационного оружия и попытки реализации концепции ведения информационных войн. Разрушительное влияние информационного оружия в информационном обществе может быть более мощным и эффективным, чем это представляется сейчас. Это особенно опасно в условиях существования почти монопольного положения компаний небольшого количества стран на рынке информационных продуктов, поскольку это способно спровоцировать желание использовать имеющееся преимущество для достижения той или иной политической цели.

Вместе с нарастающим внедрением современных информационных технологий постоянно возрастает угроза, как для общественных компьютерных систем, так и для частных организаций и отдельных граждан. Киберпреступность - это явление международного значения, уровень которого находится в прямой зависимости от уровня развития и внедрения современных компьютерных технологий, сетей общего пользования и доступа к ним. Таким образом, стремительное развитие информатизации несет за собой реальную возможность злоупотреблений в использовании компьютерных технологий из корыстных и иных мотивов, что в определенной степени ставит под угрозу национальную безопасность стран, безопасность организаций, личную безопасность.

Ни одно государство сегодня не способно противостоять этому злу самостоятельно. Насущной является необходимость активизации международного сотрудничества в этой сфере. Весомое место в таком сотрудничестве принадлежит, безусловно, международно-правовым механизмам регулирования. Это особенно актуально в современных условиях, когда значительная доля средств борьбы с киберпреступлениями, как и с другими преступлениями международного характера, относится к внутренней компетенции каждого отдельного государства. Международное сотрудничество по борьбе с киберпреступлениями вовсе не исключает, а, наоборот, активизирует

параллельное развитие национального законодательства по борьбе с компьютерными преступлениями, согласовывая его с нормами международного права и опираясь на существующий мировой положительный опыт. Отсутствие эффективных механизмов борьбы с киберпреступлениями определяется сегодня как одна из угроз национальной безопасности любого государства.

Проблема борьбы с компьютерными преступлениями - это комплексная проблема. Преступления в сфере использования информационных технологий не поддаются результативному расследованию теми средствами и мерами, которые были эффективны в прошлом веке, когда информатизация нашего общества только начиналась. Законы должны сегодня отвечать тем требованиям, которые предъявляет современный уровень развития технологий, чтобы отправления правосудия происходило в независимости от того, было ли такое преступление совершено с помощью обычных средств или персонального средства спутниковой связи и сети Internet.

2. Методы защиты информации, формирование политики информационной безопасности.

В сфере информационно-технической безопасности наблюдается постоянно возрастающее количество пользователей компьютерными системами. Дополнительным фактором, усиливающим угрозу информационной безопасности, является массовое распространение достаточно простых в использовании операционных систем и средств разработки, не требующих высокой квалификации и длительной подготовки. В свою очередь распространение и обмен новой информацией по использованию информационных технологий, в том числе представляющей угрозу безопасности, происходит очень быстро и мало контролируемо. В таких условиях создаются необходимые предпосылки для формирования многоуровневой политики информационной безопасности, причём как в отдельных организациях, так и для социума в целом, включая общенациональный и международный аспекты.

Информационные системы отличаются по степени сложности, соответственно разной сложности бывают и атаки, против них направленные. Угрозу сетям IP представляют как собственно информационные атаки, так и действия, снижающие информационную защиту, приводящие к повышению рисков уязвимости информационных систем.

Рассмотрим ряд наиболее распространённых типов атак сетей IP. Среди часто встречающихся можно назвать снифферы пакетов. Эти прикладные программы используют сетевую карту, работающую в режиме promiscuous mode. В таком режиме все пакеты, полученные по физическим каналам, сетевой адаптер отправляет приложению для обработки, при этом сниффер перехватывает все сетевые пакеты, которые передаются через определенный домен. В настоящее время снифферы работают в сетях на вполне законном основании. Они используются для диагностики неисправностей и анализа трафика. Однако учитывая то, что некоторые сетевые приложения передают данные в текстовом формате (Telnet, FTP, SMTP, POP3 и т.д.), с помощью сниффера можно узнать полезную, а иногда и конфиденциальную информацию (например, имена пользователей и пароли). Перехват имен и паролей создает большую опасность, потому что пользователи часто применяют один и тот же логин и пароль для множества приложений и систем. Многие пользователи часто имеют один пароль для доступа ко всем ресурсам и приложениям. Если программа работает в режиме клиент/сервер, а данные для аутентификации передаются по сети в читаемом текстовом формате, эту информацию с большой вероятностью можно использовать для доступа к другим корпоративным или внешним ресурсам.

Начальным способом защиты от сниффинга пакетов являются сильные средства аутентификации, например, одноразовые пароли, технология двухфакторной аутентификации. Также используется для борьбы со сниффингом коммутируемая инфраструктура, которая не ликвидирует угрозу сниффинга, но заметно снижает ее остроту. Еще один способ борьбы заключается в установке аппаратных или программных средств, которые распознают снифферы, работающие в IP сети. Эти средства не могут полностью ликвидировать угрозу, но, как и много других средств сетевой безопасности, они включаются в общую систему защиты.

Самый эффективный способ борьбы со сниффингом пакетов не предотвращает перехват и не распознает работу снифферов, но делает эту работу бесполезной. Если канал связи является криптографически защищенным, это означает, что в случае атаки будет перехвачен зашифрованный текст, а не готовая к употреблению информация.

Довольно распространённым способом атаки на IP сети является IP-спуфинг, когда злоумышленник, находящийся внутри корпорации или вне ее, выдает себя за санкционированного пользователя. Это можно сделать двумя способами: воспользоваться IP-адресом, находящимся в пределах диапазона санкционированных IP-адресов, или же использовать уполномоченный внешний адрес, которому разрешается доступ к определенным ресурсам сети. Атаки IP-спуфинга часто

являются отправной точкой для других атак, например, атаки DoS, которая начинается с чужого адреса, что скрывает истинную личность злоумышленника. Обычно IP-спуфинг ограничивается вставкой ложной информации или вредоносных команд в обычный поток данных, передаваемых между клиентским и серверным приложением или по каналу связи между одноранговыми устройствами. Для двусторонней связи нужно изменить все таблицы маршрутизации, чтобы направить трафик на ложный IP-адрес. Если главная задача состоит в получении от системы важного файла, ответы приложений не имеют значения. Если же удается изменить таблицу маршрутизации и направить трафик на ложный IP-адрес, злоумышленник получает все пакеты и сможет отвечать на них так, будто он является санкционированным пользователем.

Угрозу спуфинга можно ослабить с помощью правильного управления доступом. Для предотвращения IP-нарушения подлинности контроль доступа настраивается на отсечение любого трафика из внешней сети с исходным адресом, обязанным располагаться внутри IP сети. Это поможет бороться с IP-спуфингом, когда санкционированными являются только внутренние адреса. Если санкционированными являются и некоторые адреса внешней сети, данный метод становится неэффективным. Также ослабляет угрозу спуфинга фильтрация RFC 2827. Для реализации этого метода защиты необходимо отбраковывать любой исходящий трафик, начальный адрес которого не является одним из IP-адресов организации. Этот тип фильтрации, может выполнять провайдер. В результате отбраковывается весь трафик, который не имеет исходного адреса, ожидающего на определенном интерфейсе.

Наиболее известной формой атак сетей IP является «отказ в обслуживании» (Denial of Service - DoS). При всей тривиальности именно простота реализации и огромный ущерб привлекают к DoS пристальное внимание администраторов, отвечающих за сетевую безопасность. Атаки DoS отличаются от атак других типов. Они не нацелены на получение доступа к IP сети или на получение из этой сети любой информации. Атака DoS делает IP сеть недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения. В случае использования некоторых серверных приложений (таких как Web-сервер или FTP-сервер) атаки DoS могут заключаться в том, чтобы занять все соединения, доступные для этих приложений, и держать их в занятом состоянии, не допуская обслуживания обычных пользователей.

Парольные атаки проводятся с помощью целого ряда методов, таких как простой перебор, "троянский конь", IP-спуфинга и сниффинг пакетов. Если в результате хакер получает доступ к ресурсам, он получает его на правах обычного пользователя. Когда этот пользователь имеет значительные привилегии доступа, можно создать "проход" для будущего доступа, который будет действовать, даже если пользователь изменит свой пароль и логин. Парольных атак можно избежать, если не пользоваться паролями в текстовой форме. Одноразовые пароли или криптографическая аутентификация могут практически свести на нет угрозу таких атак. К сожалению, не все программы, хосты и устройства поддерживают указанные выше методы аутентификации.

Для атаки типа «Man-in-the-Middle» нужен доступ к пакетам, передаваемым по сети. Для атак этого типа часто используются снифферы пакетов, транспортные протоколы и протоколы маршрутизации. Атаки преследуют следующие цели:

- кража информации,
- перехват текущей сессии и получение доступа к частным сетевым ресурсам,
- анализ трафика и получение информации о сети и ее пользователях,
- проведение атак типа DoS,
- искажение передаваемых данных и ввода несанкционированной информации в сетевые сессии.

Эффективно бороться с атаками типа «Man-in-the-Middle» можно только с помощью криптографии. Но в случае перехвата информации о криптографической сессии (например, ключ сессии), это может сделать возможной атаку Man-in-the-Middle даже в зашифрованной среде.

Атаки на уровне приложений могут проводиться несколькими способами. Самый распространенный из них заключается в использовании хорошо известных слабостей серверного программного обеспечения, которые широко публикуются, чтобы дать возможность администраторам исправить проблему с помощью коррекционных модулей (патчей). Главная проблема с атаками на уровне приложений заключается в том, что они часто пользуются портами, которым разрешен проход через межсетевой экран. Полностью исключить атаки на уровне приложений невозможно. Постоянно открываются и публикуются все новые уязвимые места прикладных программ. Самое главное здесь - хорошее системное администрирование.

При подготовке атаки против любой IP сети, как правило, проводится сбор информации о сети с помощью общедоступных данных и приложений, который иногда называют сетевой разведкой. IP сеть исследуется с помощью запросов DNS, эхо-тестирования (ping sweep) и сканирования портов. DNS-запросы помогают понять, кто владеет тем или иным доменом и какие адреса этого домена присвоены. Эхо-тестирование (ping sweep) адресов, раскрытых с помощью DNS, позволяет увидеть, какие хосты реально работают в данной среде. Получив список хостов, используется средства сканирования портов, чтобы составить полный список услуг, предоставляемых этими хостами. И наконец, анализируются характеристики приложений, работающих на хостах. В результате добывается информация, которую можно использовать для взлома. Полностью избавиться от сетевой разведки невозможно. Однако системы IDS на уровне сети и хостов обычно хорошо справляются с задачей уведомления администратора о сетевой разведке. Это позволяет лучше подготовиться к предстоящей атаке и оповестить провайдера (ISP), в сети которого установлена система, проявляющая излишнее любопытство.

Действием, снижающим информационную защиту и приводящим к повышению рисков уязвимости информационных систем, часто бывает злонамеренное использование отношений доверия, существующих в сети. Риск злоупотребления доверием можно снизить за счет более жесткого контроля уровней доверия в пределах IP сети. Системы, расположенные с внешней стороны межсетевого экрана, никогда не должны пользоваться абсолютным доверием со стороны защищенных экраном систем. Отношения доверия должны ограничиваться определенными протоколами и, по возможности, аутентифицироваться не только по IP-адресам, но и по другим параметрам.

К разновидности злоупотребления доверием относится переадресация портов, когда взломанный хост используется для передачи через межсетевой экран трафика, который в противном случае был бы обязательно отбракованным. Основным способом борьбы с переадресацией портов является использование надежных моделей доверия. Кроме того, помешать несанкционированному пользователю в установке на хосте своих программных средств может хост-система IDS (HIDS).

Большинство сетевых атак проводятся ради получения несанкционированного доступа. Способы борьбы с несанкционированным доступом довольно простые. Главным здесь является сокращение или полная ликвидация возможностей получения доступа к системе с помощью несанкционированного протокола. Что же касается межсетевого экрана, то его основной задачей является предотвращение простейших попыток несанкционированного доступа.

Рабочие станции конечных пользователей очень уязвимы для вирусов и "троянских коней". Вирусами называются вредоносные программы, которые внедряются в другие программы для выполнения определенной нежелательной функции на рабочей станции конечного пользователя. Борьба с вирусами и "троянскими конями" ведется с помощью эффективного антивирусного программного обеспечения, работающего на уровне пользователя и, возможно, на уровне сети. Антивирусные средства обнаруживают большинство вирусов и "троянских коней" и прекращают их распространение. Получение самой свежей информации о вирусах поможет эффективнее бороться с ними.

Выводы:

Политикой информационной безопасности можно назвать как простые правила использования информационных ресурсов, так и детальные описания всех их особенностей, которые занимают сотни страниц. Важно понять, что сетевая безопасность - это эволюционный процесс. Нет ни одного продукта, способного предоставить корпорации полную безопасность. Надежная защита сети достигается сочетанием продуктов и услуг, а также грамотной политикой безопасности и ее соблюдением всеми сотрудниками сверху донизу. Можно заметить, что правильная политика безопасности даже без выделенных средств защиты дает лучшие результаты, чем средства защиты без политики безопасности.

Политика безопасности сети предприятия является результатом оценки риска и определения важных средств и возможных угроз. Базовыми элементами политики в области безопасности является идентификация, целостность и активная проверка. Идентификация призвана предотвратить угрозу обезличивания и несанкционированного доступа к ресурсам и данным. Целостность обеспечивает защиту от подслушивания и манипулирования данными, поддерживая конфиденциальность и неизменность передаваемой информации.

И наконец, активная проверка (аудит) означает проверку правильности реализации элементов политики безопасности и помогает обнаруживать несанкционированное проникновение в сети и атаки типа DoS.

При разработке политики безопасности необходимо сбалансировать легкость доступа к информации и адекватный механизм идентификации зарегистрированного пользователя и обеспечения целостности и конфиденциальности данных. Политика безопасности должна внедряться принудительно как технически, так и организационно - тогда она будет по-настоящему эффективна.

Библиография

1. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети — анализ технологий и синтез решений. М.: ДМК Пресс, 2004. — 616 с. — ISBN 5-94074-244-0.
2. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем. В 2-х томах: Том 1. — Угрозы, уязвимости, атаки и подходы к защите. — М.: Горячая линия - Телеком, 2006. — 536 с. — ISBN 5-93517-291-1, ISBN 5-93517-319-0; Том 2. — Средства защиты в сетях. — М.: Горячая линия - Телеком, 2008. — 560 с. — ISBN 978-5-9912-0034-9.
3. Малюк А.А. Теория защиты информации. — М.: Горячая линия - Телеком, 2012. — 184 с. — ISBN 978-5-9912-0246-6.
4. Петренко С. А., Курбатов В. А. Политика информационной безопасности. — М.: Компания IT, 2006. — 400 с. — ISBN 5-98453-024-4.