Утверждаю

Генеральный директор
ОИПИ НАН Беларуси

_____ Тузиков А.В.

“____” _____ 2011 г.

Политика безопасности интернет-сайтов, размещенных на хостинге сети BASNET

1. Цель политики безопасности

Целью данной политики безопасности является установка правил размещения, управления и функционирования интернет-сайтов абонентов на хостинге сети BASNET, определение прав и обязанностей хостинг-провайдера и абонента, общие положения по управлению доступом пользователей к интернет-сайтам, определение стандарты создания сильных паролей, их защиту, хранение и частоту изменения.

2. Область применения

Областью применения данного документа является сфера оказания услуг веб-хостинга в сети BASNET.

3. Требования политики

3.1 Выдача идентификационной информации

Пользующаяся услугами сети BASNET организация (в дальнейшем Абонент), должна назначить лиц, ответственных за сопровождение сайта (сетевых администраторов), и указать их контактные данные в приложении к договору на предоставление телекоммуникационных услуг сети BASNET.

После получения подписанного Абонентом договора администраторы Центра управления сетью заносят реквизиты Абонента вместе с указанными в договоре контактными данными сетевого администратора и требованиями по ограничению доступа в абонентскую базу данных BASNET.

После занесения Абонента в абонентскую базу данных уполномоченное лицо Центра управления сетью визирует договор и передает его на подпись в приемную ОИПИ НАН Беларуси.

Абонентский экземпляр договора, а также присвоенная Абоненту идентификационная информация (логин и пароль) передается Центром управления сетью лично в руки указанному в договоре сетевому администратору Абонента по предъявлению им паспорта либо другого удостоверяющего личность документа.

Абонент в дальнейшем ответственен за безопасное использование идентификационной информации и должен предпринимать все необходимые меры, чтобы надлежащим образом гарантировать ее от компрометации.

Абонент полностью принимает на себя ответственность за все действия, произведенные под своим логином и паролем – с его ведома или без него.

Для своевременного получения оповещений о предстоящих регламентных технических работах, возможных перебоях в работе сети, других публичных оповещений Абонент должен подписаться на рассылку сетевых анонсов BASNET по адресу www.basnet.by.

При изменении в последующем контактных данных сетевого администратора Абонент сообщает об этом в ОИПИ НАН Беларуси в письменном виде. Изменение контактной информации в абонентской базе данных BASNET производятся Центром управления сетью только на основании письменного извещения от Абонента.

3.2 Удаленный доступ

Администраторы и редакторы интернет-сайтов могут получать доступ к ним только с определенного в договоре на оказание услуг перечня сетевых адресов и по определенным в договоре портам протоколов транспортного уровня. Удаленный доступ обеспечивается через защищенные протоколы обмена посредством соединения, изолированного от сети Интернет.

Попытки несанкционированного удаленного доступа к интернет-сайтам регистрируются, и сетевому администратору Абонента передается соответствующее уведомление.

3.3 Обеспечение информационной безопасности и целостности данных

Провайдер проводит постоянный мониторинг состояния серверов хостинга.

Провайдер вправе приостанавливать, блокировать или запрещать использование программного обеспечения (ПО) пользователей в случае, если эксплуатация такого программного обеспечения приводит или может привести к аварийным ситуациям, нарушению системы безопасности, нарушению установленного регламента или условий договора.

Не допускается размещение:

- ПО массовой рассылки почты и т.п. деятельности, которую можно расценивать как рассылку спама;
- скриптов с уязвимостями, представляющими угрозу безопасности, к которым относятся разновидности шеллов, работающих без авторизации;

 IRC-серверов/клиентов/скриптов и P2P-приложений (при обнаружении такой активности на сервере аккаунт будет заблокирован).

Провайдер обеспечивает базовую информационную безопасность серверов и ресурсов Абонента в пределах, определяемых обычными условиями, если только в договоре явно не оговорено иное.

Провайдер не несет ответственности за возможную компрометацию паролей Абонента, произошедшую по его вине, но по заявке Абонента производит оперативную смену таких паролей.

Провайдер обеспечивает полное резервное копирование статической информации Абонента, размещенной на серверах Провайдера. Резервное копирование производится согласно «Регламенту полного резервного копирования информации интернет-сайтов».

В случаях, если потеря информации произошла по вине Провайдера, он принимает все необходимые меры для максимально быстрого восстановления информации. В том случае если потеря данных была вызвана действиями клиента, восстановление данных производится по официальному письму (факсу), со сроком исполнения до 48 часов. Если в условиях договора не оговорен особый режим резервного копирования (рассматриваемый как дополнительная услуга), восстановление производится из последнего архива, либо бэкап выкладывается на ftp-сервер Абонента.

3.4 Обработка заявок Центром управления сетью

Основанием для выполнения работ Центром управления сетью является заявка Абонента. Центр управления сетью принимает заявки только с авторизационной информацией (логин и пароль) для аутентификации Абонента.

Экстренные заявки, такие, как просьба о смене паролей в случае их компрометации, восстановление работоспособности основных сервисов принимаются по телефону, для аутентификации производится обратный звонок Абоненту по телефону, указанному в договоре на оказание услуг.

В случаях, требующих существенного изменения настроек, влекущих за собой изменение условий договора, изменения производятся только на основании официальных письменных заявок Абонента за подписью руководителя организации, при этом для ускорения решения проблем допускается использование факса.

3.5 Защита серверов хостинга

Сегмент сети, где расположен ЦОД (центр обработки данных), находится в отдельном vlan и экранируется межсетевым экраном (Cisco ASA).

Администраторы регулярно отслеживают информацию о новых уязвимостях, типах атак, своевременно обновляют программные средства защиты информации и периодически тестируют системы защиты информации.

4. Требования парольной политики

4.1 Описание

Пароли – один из важнейших аспектов информационной безопасности, так как плохо подобранный пароль повышает потенциальный риск несанкционированного доступа в информационную систему компании. Все сотрудники (включая подрядчиков и третью сторону) несут ответственность за выполнение требований настоящей политики.

4.2 Цель

Цель этой политики установить стандарты создания сильных паролей, их защиту, хранение и частоту изменения.

4.3 Область применения

Эта политика относится ко всему персоналу, кто имеет или ответственен за доступ к конфиденциальной информации всех уровней (или любая форма доступа, которая поддерживает или требует пароля) на любой системе, оборудовании, имеющем доступ (или хранящем конфиденциальную информацию) к сети.

4.4 Политика

Пароли системных учетных записей (администратора домена, локального администратора, root и т. д.) должны изменяться ежеквартально.

Все пароли системных учетных записей, а также пароли приложений и активного оборудования необходимо хранить в базе данных в зашифрованном виде, доступ к которой ограничен.

Срок действия паролей учетных записей домена должен составлять не более 9 месяцев. Рекомендуемый интервал смены пароля 6 месяцев.

Пароль учетной записи пользователя, имеющего административные привилегии, полученные при помощи членства в группе или при помощи программ, таких как sudo, должен быть уникален по отношению к другим паролям учетных записей данного пользователя.

Запрещается передача паролей пользователям при помощи почтовых сообщений либо иным другим открытым способом через Интернет.

Пароль, полученный пользователем, необходимо сменить при первом входе в систему.

При использовании SNMP протокола, необходимо использовать отличные от стандартных значений строк подключений (Community Name) "public", “private", "system" и отличными от пароля, используемого для входа в систему.

Все пароли пользователей, а также системные пароли должны соответствовать данной политике.

4.5 Инструкция по созданию пароля

Пароли используются для различных целей. Среди них: доступ к учётной записи пользователя, к веб-интерфейсам, к электронной почте, для защиты хранителя экрана, пароли голосовой почты и доступ к маршрутизаторам. Поскольку очень мало систем поддерживают токены с одноразовыми паролями (динамические пароли, которые используются только один раз), следует знать, как выбрать стойкий пароль.

Плохие, слабые пароли обладают следующими признаками:

- содержат менее восьми символов;
- являются словом, которое содержится в словарях (русских или иностранных);
- являются часто употребляемым словом;
- содержат фамилию, кличку животного, имена друзей, сотрудников, вымышленных персонажей и т. д.;
- содержат компьютерные термины и названия, команды, названия сайтов, компаний, оборудования, программного обеспечения;
- содержат название компании и географические наименования или их производные;
- содержат даты рождения и иную личную информацию, например, адреса и номера телефонов;
- слово или число по шаблону типа аааббб, qwerty, zyxwvuts, 12345 и т.д.;
- предыдущий пример, вводимый в обратной последовательности;
- два предыдущих примера с цифрой в начале или конце пароля.

4.6 Параметры сильных паролей:

- содержат сочетание букв верхнего и нижнего регистров (например, a-z, A-Z);
- включают цифры и знаки пунктуации, например, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- состоят из восьми и более символов;
- не являются словом на любом языке, диалекте, сленге, жаргоне и т.д.;
- не основаны на персональной информации, например фамилии, дате рождения и т.д.;
- никогда не записываются и не хранятся on-line.

Создавайте легко запоминаемые пароли. Одним из способов создания таких паролей, использовать песни, стихи и другие, легко запоминающиеся фразы. Например, из фразы: "This May Be One Way To Remember" можно получить такие пароли: "TmB1w2R!" или "Tmb1W>r~" и другие варианты.

Внимание: Не используйте ни один из предыдущих примеров в качестве пароля!

4.7 Правила парольной защиты

Не используйте один и тот же пароль для доступа к учётным записям внутри сети и к другим ресурсам (например, доступ в интернет из дома, системам электронной коммерции и т. д.). По возможности не используйте один и тот же пароль для доступа к различным ресурсам внутри сети. Например, используйте один пароль для прикладных программ и другой для администрирования ресурсов. Используйте различные пароли для учётных записей Windows и Unix-систем.

Не сообщайте ваш пароль никому, даже вашему секретарю или обслуживающему персоналу. Все пароли являются конфиденциальной информацией.

Не сообщайте никому свой пароль по телефону.

Не отправляйте свой пароль по электронной почте.

Не сообщайте свой пароль начальнику.

Не говорите о своём пароле рядом с посторонними.

Не упоминайте о содержимом пароля (например, "мой день рождения").

Не указывайте свой пароль в анкетах или опросниках.

Не сообщайте свой пароль членам своей семьи.

Не сообщайте свой пароль сослуживцам перед уходом в отпуск.

Не записывайте пароль и не храните его на рабочем месте.

Не храните пароль в файле на компьютере, включая переносной, без шифрования.

Не используйте функцию "Запомнить пароль" в приложениях.

Если кто-либо требует сообщить ваш пароль, сошлитесь на этот документ.

Если вы считаете, что учётная запись или пароль скомпрометированы – смените все пароли.

Уполномоченные лица могут регулярно проводить подбор или попытки взлома паролей. Если пароль будет угадан или взломан во время таких мероприятий, вас попросят сменить пароль.

4.8 Стандарт разработки приложений

Разработчики приложений должны обеспечить в своих программах следующие меры безопасности:

- приложения должны поддерживать аутентификацию отдельных пользователей, а не групп;
- приложения не должны хранить пароли в открытом или легко раскрываемом виде;
- приложения должны обеспечивать своего рода передачу прав, чтобы один пользователь мог выполнять функции другого, не зная его пароль;
- приложения должны по возможности всегда поддерживать TACACS+, RADIUS, и/или X.509 на основе LDAP.

4.9 Использование паролей и парольных фраз для удалённого доступа

Для контроля удалённого доступа к сетям используйте или одноразовые пароли или ассиметричную ключевую систему со стойкой парольной фразой.

Парольные фразы отличаются от паролей. Парольная фраза более длинная версия пароля и, таким образом, более надёжная. Парольные фразы обычно используются для аутентификации в ассиметричных системах шифрования. Ассиметричная ключевая система определяет математическую связь между открытым ключом, известным всем и закрытым ключом, известным только его владельцу. Без парольной фразы, дающей доступ к закрытому ключу, пользователь не получит доступ.

Парольная фраза обычно состоит из нескольких слов, являясь более устойчивой к атакам по словарю. Хорошая парольная фраза относительно длинная и содержит комбинацию букв в верхнем и нижнем регистре, а также цифры и знаки препинания. Вот пример хорошей парольной фразы: "The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

Все правила создания стойких паролей относятся и к парольным фразам.

5. Обучение персонала

Одним из наиболее важных элементов обеспечения информационной безопасности является обучение сотрудников в целях повышения уровня безопасности. Сотрудники должны понимать важность и ценность информации, которую они ежедневно обрабатывают. Обучение вопросам информационной безопасности должно предусматривать необходимость сохранения конфиденциальности всей информации, циркулирующей в информационной системе. Сотрудники должны быть проинформированы о том, что запрещено раскрывать любую информацию до тех пор, пока запрашивающая сторона не определена ими как имеющая право доступа.

6. Ответственность

К администраторам, нарушившим данную политику безопасности, могут быть применены дисциплинарные меры, вплоть до увольнения.

7. Порядок и периодичность пересмотра

Политика безопасности подлежит пересмотру при изменении нормативно-правовых, организационных и технических условий обеспечения данной политики.

Зав. отделом С.А. Анейчик