DOI: 10.17117/na.2016.11.02.210

<http://ucom.ru/doc/na.2016.11.02.210.pdf>

Поступила (Received): 03.11.2016

Петькина Е.Д., Марченко Л.С. Возможные уязвимости хранения информации

Petkina E.D., Marchenko L.S.
Possible information storage vulnerabilities

Данная статья посвящена проблемам хранения информации и выявлению существующих угроз. В современном мире очень сложно постоянно следить за безопасностью всех файлов, особенно в каких – либо организациях. Поэтому мы хотели бы сделать небольшой обзор главных уязвимостей информации

Ключевые слова: информация, уязвимость информации, хранение информации

This article describes problems of information storage and detection of it's possible vulnerabilities. In nowadays, it's difficult to provide data security, especially in organization, so we want to review main information vulnerabilities

Key words: information, exposure of information, information storage

Петькина Екатерина Дмитриевна

Магистрант

Красноярский государственный педагогический университет им. В.П. Астафьева

г. Красноярск, ул. Перенсона, 7

Petkina Ekaterina Dmitriyevna

Master

Krasnoyarsk state pedagogical University named V.P. Astafiev

Krasnoyarsk, Perenson st., 7

Марченко Любовь Сергеевна

Магистрант

Красноярский государственный педагогический университет им. В.П. Астафьева

г. Красноярск, ул. Перенсона, 7

Marchenko Lubov Sergeevna

Master

Krasnoyarsk state pedagogical University named V.P. Astafiev

Krasnoyarsk, Perenson st., 7

Информация является движущей силой и одним из важных активов любой современной организации. Объемы данных, которые хранят и обрабатывают современные организации (даже не самые большие), измеряются в сотнях гигабайт и продолжают возрастать. Со временем аппаратное обеспечение устаревает и может уже не справляться с текущей нагрузкой. Поэтому для безопасности и сохранности данных нужно постоянно следить за его работоспособностью.

Потеря такой информации, как база данных сотрудников, информация о реальных проектах организации, корпоративный документооборот очень критична для любой организации.

Утраченное аппаратное обеспечение, либо вычислительные ресурсы можно восстановить, а утраченные данные, при отсутствии хорошо спроектированной системы резервирования, уже не подлежат восстановлению.

По данным исследовательской компании Gartner, среди организаций, пострадавших от катастроф и переживших крупную необратимую потерю корпоративных данных, 43% не смогли продолжить свою деятельность.

Ввиду всего этого, накопленная информация обладает определенной ценностью и для защиты и сохранности своих данных компании, и даже небольшие офисы платят огромные деньги на поиск и покупку решения, удовлетворяющего его потребности.

Цель данной статьи заключается в обзоре уязвимостей хранения информации.

Уязвимость информации – объективное свойство информации подвергаться различного рода воздействиям (опасностям, угрозам), нарушающим ее целостность, достоверность и конфиденциальность. Воздействия носят дестабилизирующий по отношению к информации характер и приводят к утрате носителя конфиденциальной информации или утрате конфиденциальности информации. Уровень уязвимости информации находится в прямой зависимости от степени совершенства применяемой в фирме системы защиты информации, перекрытия этой системой всей сферы возможных угроз и предполагаемых каналов несанкционированного доступа к информации. [1]

Среди возможных уязвимостей в отношении хранения информации, можно выделить следующие:

- физическая потеря данных (вышел из строя жесткий диск, потеря электропитания и т.д.);
- потеря доступа к массиву данных;
- низкая степень конфиденциальности и надежности;
- сложность управления распределенными потоками информации;
- невозможность полноценного резервного копирования;
- недостаточная скорость чтения, записи и обработки информации;
- сложность или невозможность архивирования данных;
- проблема выбора дисковых массивов и расчета физической памяти;
- неэффективная утилизация ресурсов.

Возникновение хотя бы одной из этих угроз может привести к простоя предприятия, потере корпоративных данных, что влечет за собой убытки, а это в свою очередь препятствуют нормальному функционированию предприятия и его развитию [2].

К примеру, у интернет-провайдера вышел из строя массив данных, на котором хранилась часть базы данных подключенных клиентов. Для таких организаций стоимость простоя очень велика. Это означает, что некоторые клиенты данного провайдера перестали получать его услуги, что влечет за собой резкий негатив, а так же вероятность ухода клиентов к другим интернет-провайдерам.

Таких примеров может быть множество и для решения вышеперечисленных проблем необходимо внедрить комплексное программно-аппаратное решение по организации централизованного надежного хранения большого объема данных.

Список используемых источников:

1. Нестеров С.А. Информационная безопасность и защита информации. СПб.: Изд-во Политехн. ун-та, 2009. 126 с.
2. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. М.: ИНФРА-М, 2001. 304 с.

© 2016, Петькина Е.Д., Марченко Л.С.

Возможные уязвимости хранения информации

© 2016, Petkina E.D., Marchenko L.S.

Possible information storage vulnerabilities