УДК 004.771

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ ПРИ ВИРТУАЛИЗАЦИИ РАБОЧИХ СТОЛОВ

Таров Д.А., Тарова И.Н.

ФГБОУ ВО «Елецкий государственный университет им. И.А. Бунина, Елец, e-mail: tarov1970@rambler.ru, inesstarova@rambler.ru

Данная статья посвящена вопросу обеспечения безопасности информационной среды организации при виртуализации рабочих столов рабочих мест сотрудников. Виртуализацию рабочих столов авторы трактуют как возможность дистанционного их использования сотрудниками под контролем системного администратора, отвечающего за информационную безопасность. По мнению авторов, актуальной является проблема нестабильного функционирования рабочих столов сотрудников вследствие возможного несанкционированного доступа к различным сегментам информационной среды организации и могущего повлечь повреждение или утрату данных, перегруженность каналов, а также программно-аппаратные сбои, возникающие из-за работы вредоносного программного обеспечения, что требует реализации комплекса мер по защите и копированию конфиденциальных данных и поддержанию стабильной работы системы. В статье затрагивается проблема несоответствия должностных обязанностей пользователей их профессиональной деятельности, возникающая из-за того, что пользователь, кроме исполнения своих непосредственных профессиональных обязанностей, вынужден нести долю ответственности за информационную безопасность среды. Рассматриваются различные технологии, обеспечивающие безопасность сетевых подключений и защиту конфиденциальной информации. Авторы выделяют категории лиц, потенциально представляющих угрозу безопасности информационной среды организации, и предлагают профилактические меры, направленные на нейтрализацию этих угроз, среди которых новые пункты должностных обязанностей системных администраторов.

Ключевые слова: информационная среда организации, информационная безопасность, виртуализация рабочих столов

ORGANIZATION INFORMATION SECURITY AT VIRTUALIZATION OF DESKTOPS

Tarov D.A., Tarova I.N.

Bunin Yelets State University, Yelets, e-mail: tarov1970@rambler.ru, inesstarova@rambler.ru

This article is devoted to the issue of ensuring the security of the information environment of an organization during virtualization of desktops of workplaces of employees. The authors interpret desktop virtualization as an opportunity to remotely use their employees under the control of a system administrator responsible for information security. According to the authors, the urgent problem is the unstable functioning of employee desktops due to the possible unauthorized access to various segments of the organization's information environment and which could lead to data damage or loss, channel congestion, as well as hardware and software failures that arise due to the operation of malicious software , which requires the implementation of a set of measures to protect and copy confidential data and maintain stable operation of the system. The article addresses the problem of inconsistency of the duties of users of their professional activities, arising from the fact that the user, in addition to performing his immediate professional duties, is forced to bear a share of responsibility for the information security of the environment. Various technologies that ensure the security of network connections and the protection of confidential information are considered. The authors identify the categories of persons potentially posing a threat to the security of the organization's information environment and propose preventive measures aimed at neutralizing these threats, including new items in the duties of system administrators.

Keywords: organization's information environment, information security, desktop virtualization

Сокращение расходов на работу офисов и организаций в наше время является весьма животрепещущей темой. Существует множество решений, позволяющих минимизировать траты, но в нашей работе мы коснемся одной из них, а именно: перевод сотрудников на удаленную работу посредством механизмов виртуализации работы офиса. Однако охватить все стороны виртуализации в одной работе представляется затруднительным, поэтому мы рассмотрим лишь один аспект – виртуализацию рабочих столов.

Рабочим столом является главное окно графического пользовательского интерфейса, в том числе и элементы, добавляемые самой средой. Кроме того, отдельные среды, например среда операционной системы MS Windows, среды, основанные на предписаниях группы freedesktop.org, такие как GNOME, KDE могут считать рабочим столом также и каталоги файловых структур. Как элемент рабочего стола, в отдельных случаях, может считаться и панель задач.

Вышеизложенное позволяет трактовать виртуализацию пользовательского рабочего стола как использование облачных решений и виртуальных машин для обеспечения его удаленной работы, контролируемой системой.

Отметим основные преимущества виртуализации рабочих столов:

– повышение отказоустойчивости и безопасности всей системы;

– обеспечение эффективного мониторинга информационной среды организации;

– обеспечение возможности дистанционной работы сотрудников;

– экономия средств организации на закупке и последующей модернизации аппаратного обеспечения.

Исходя из рассматриваемого вопроса, обязанности администратора связаны с обеспечением безопасности информационной среды организации и включают следующее:

– поддержка электронной почты и учетных записей;

– архивация данных, контроль состояния архивов;

– контроль безопасности информационной среды организации;

– ведение и контроль журнала действий.

Цель исследования: поиск технических и организационных путей обеспечения отказоустойчивости и безопасности информационной среды при организации дистанционной работы сотрудников под контролем системного администратора.

Материалы и методы исследования

Базой исследования выступает информационная среда ФГБОУ ЕГУ им. И.А. Бунина, функционирующая на основе совокупности локальных подсетей, объединенных в единую информационную систему университета. Исследование носит описательный и сравнительный характер.

Различные сочетания таких утилит, как например, Veeam Business View, Veeam Veeam, Reporter Monitor со средствами MS Windows позволяет системному администратору осуществлять контроль виртуальных машин, подключенных к кластеру организации в режиме реального времени. Текущий статус отчетов системы осуществляется посредством Microsoft Report Viewer 2018. В качестве альтернативы можно предложить YARG. Для экономии средств можно воспользоваться триальными версиями указанных утилит, обеспечивающими мониторинг системы и оповещение средствами sms и электронной почты. Следует заметить, что в данном случае экономия средства на лицензиях программного обеспечения, неизбежно снижает надежность системы из-за сниженного функционала триальных версий. Кроме того, следует учитывать значительные нагрузки на аппаратные компоненты информационной среды, создаваемые вышеназванными программами. Например, рекомендуемый объем ОЗУ backup-сервера, как показывает опыт, должен превышать 4Гб. Выходом может быть переход на утилиты, относящиеся к свободному программному обеспечению, такие как OpenNMS, Zabbix, Cacti или Nagios, с которыми имеется значительный положительный опыт работы.

Особое внимание следует уделить установке оптимального уровня конфиденциальности, обеспечивающего баланс между доступностью информационной среды для пользователей, с одной стороны, и ее защищенностью – с другой. Квалифицированный персонал может достаточно просто добиться этого как средствами браузера, так и встроенными средствами операционной системы [1].

Результаты исследования и их обсуждение

Комплекс аппаратных и программных средств, на базе которых функционирует информационная среда организации, является отказоустойчивым, если обеспечена возможность бесперебойной работы всей системы. К сожалению, это в настоящее время является недостижимым идеалом, поэтому следует исходить лишь из некоторой ее степени, которую можно вычислить следующим образом:

$$A = (F – (D + R))/F,$$

где A – отказоустойчивость всей системы, F – время устойчивой работы, D – время реакции системы на программный или аппаратный сбой, R – время, необходимое для нормализации системы [2].

Констатируем, что сейчас показателем отказоустойчивости любых рабочих столов является таковая характеристика виртуальных машин, в состав которых они входят [3]. Рассматривая стабильность функционирования рабочих столов и всей информационной среды в целом, лучше опираться на понятие «решение высокой доступности», т.е. показатель информационной системы, характеризующий способность системы противостоять отказам в обслуживании запросов посредством контроля программно-аппаратных сбоев и минимизации времени плановых простоев: виртуальные машины аварийных сегментов сети будут в режиме реального времени распределены между сегментами, сохраняющими устойчивость, что позволит не потерять данные аварийных машин и продолжить их обработку. Необходимо учитывать время, которое потребуется системе для переноса виртуальных машин из аварийного сегмента, зависящее от качества аппаратных ресурсов.

Актуальной является проблема нестабильного функционирования рабочих столов сотрудников вследствие несанкционированного доступа к различным сег-

ментам информационной среды организации. Перегруженность сетевых каналов, технические сбои, доступность конфиденциальных данных и их утрата, возникающие из-за воздействия вредоносного кода, требуют разработки и осуществления комплекса правовых, организационных и технических мер, направленных на защиту конфиденциальных данных. К ним следует отнести регулярное обновление антивирусного программного обеспечения, архивацию данных на изолированных серверах, разработку и соблюдение правил доступа в помещения, в которых находятся рабочие места, имеющие подключение к закрытым сегментам сети, поддержание дисциплины на рабочих местах.

Виртуализация рабочих столов помогла снять проблему, возникающую из-за того, что сотрудники организации были вынуждены кроме исполнения своих непосредственных должностных обязанностей нести долю ответственности за информационную безопасность организации, связанную с настройкой и обслуживанием рабочих мест,, что проблематично из-за, как правило, низкой квалификации обычного пользователя в IT-технологиях и малой эффективности регулярных инструктажей из-за высокой мобильности современных сетевых угроз. Виртуализация рабочих столов дала возможность перераспределения ответственности за информационную безопасность среды с обычных пользователей на системных администраторов, имеющих вполне достаточную квалификацию для нейтрализации угроз.

Существенным элементом обеспечения безопасности конфиденциальных данных является двухфакторная аутентификация, осуществляющаяся с помощью токенов, персональных смарт-карт и сертификатов, интегрированных в унифицированную систему управления доступом к различным сегментам информационной среды ЕГУ им. И.А. Бунина, что позволило значительно повысить ее защищенность.

Эффективным средством защиты информационной среды является использование технологии построения доверенного сеанса связи, которую можно реализовать как средствами MS Windows, так и сторонними средствами обеспечения изолированной программной среды, например, такими средствами защиты информации, как Secret Net, Dallas Lock 8.0-K и т.д., основанных на ключах, содержащих эталонный образ программной среды, включая операционную систему, а также настроенный P2P-клиент на основе Chrome Remote Desktop или какой-либо аналог. Подобные решения позволяют осуществлять не только идентификацию и аутентификацию пользователей, но и осуществлять централизованное управление, разграничивать права доступа, обеспечивать доверенные загрузки, производить аудит пользовательских действий и т.д.

Кроме вышеуказанной СПДС-технологии для защиты информационной среды широко применяются следующие технологии и их сочетания:

1. Терминальный режим:

– дополнительное использование гипервизора;

– использование полного стека сетевых протоколов;

– возможность использования нулевого клиента.

2. Защита передачи данных:

– использование режима разделения ролей:

– ведение журнала событий и работы BIOS;

– использование протокола TLS.

3. Режим администрирования удаленного рабочего стола:

– использование технологии Intel Active Management Technology (AMT);

– использование централизованного управления настройками удаленных рабочих столов, в том числе контроль сертификатов устанавливаемых программных продуктов;

– использование удаленного управления тонкими клиентами и пользователями.

Тем не менее использование СПДС-технологии, по сравнению с вышеуказанными, дает системному администратору ряд следующих преимуществ:

– аутентификация пользователя происходит по традиционной двухфакторной схеме, а именно: проверка пароля, предоставленного администратором, проводится при ограничении количества попыток его ввода, сетевые ресурсы организации предоставляются в соответствии с цифровым сертификатом, находящимся в удаленном хранилище. Компоненты приложений, отвечающие за аутентификация пользователей, могут использоваться средой как дополнительным элементом защиты;

– обеспечивается изоляция процессов, запущенных на удаленном рабочем столе в течение доверенного сеанса, т.к. загрузочный модуль среды блокирует запуск программного обеспечения, сертификаты которых не соответствуют сертификатам, находящемся в удаленном хранилище, что исключает несанкционированное влияние стороннего программного обеспечения на сетевые ресурсы организации;

– все потоки данных организации во время доверенного сеанса шифруются посредством одно- или двухключевого криптографического алгоритма, например e2, Xtea или RSA, что в достаточной мере изолирует сетевые ресурсы организации от несанкционированного внешнего воздействия. Использование криптографических алгоритмов позволяет придать им криптографическую стойкость;

– программная среда терминала, обеспечивающего доступ сотрудников к закрытым сегментам сети, поддерживает соответствие эталонной, т.е. любой запрос на подключение приводит к сравнению с эталонным образом программной среды для выявления ее возможных модификаций и блокировки сеанса в случае их обнаружения;

– результаты деятельности пользователей не влияют на эталонную программную среду, что снижает финансовые и трудовые затраты на администрирование удаленных терминалов, позволяет увеличить время между процедурами контроля их конфигураций и минимизирует затраты на программное обеспечение средств поиска и удаления скрытно внесённого программного кода.

Российские разработчики и производители средств идентификации и аутентификации расширяют номенклатуру их модификаций, отходя от традиционных форматов. Нам представляется перспективным использование Bluetooth-токенов, позволяющих аутентифицировать пользователей при обеспечении доступа к информационной среде организации посредством мобильных устройств, например посредством планшетов и смартфонов.

Заключение

Токены и универсальные идентификационные ID-карты сегодня внедряются практически во все сферы жизни: электронные удостоверения и пропуска, паспорта, водительские удостоверения и удостоверения личности, международные удостоверения студентов. Малазийская ID-карта MyID/MyKID кроме программы идентификации содержит медицинскую информацию, водительское удостоверение и т.д. [4]. В России универсальная электронная идентификация граждан вводится поэтапно и начнет действовать повсеместно с 2023 г. Все это, с одной стороны, ведет к росту спроса на компоненты систем идентификации, но, с другой, увеличение их выпуска может привести к снижению стоимости систем идентификации.

Использование прав конфиденциальности при подключении виртуальных машин к закрытым сегментам информационной среды организации подразумевает сравнение прав пользователя и, в случае их несоответствия, блокирует сеанс, отправляет электронное письмо сотруднику, отвечающему за информационную безопасность организации, и делает отметку в журнале событий.

Исходя из практики, выделяем категории лиц, потенциально представляющих угрозу безопасности информационной среды организации:

– злоумышленник, не являющийся сотрудником организации, представляющий угрозу работоспособности аппаратных компонентов сети и конфиденциальной информации. Профилактической мерой является автоматическая проверка внешних запросов на подключение к сегментам сети на соответствие уровню доступа в соответствии с разграничением прав доступа;

– пользователь, обладающий, в силу должностных обязанностей, доступом к тем или иным сегментам информационной среды посредством своего рабочего места. В качестве профилактической меры предлагаем проводить периодическую проверку соответствия уровня доступа к сети должностным обязанностям сотрудника, мониторинг его деятельности, особенно записей журнала событий о программных сбоях;

– системный администратор, контролирующий виртуальную среду организации и имеющий доступ к закрытым сегментам сети. Профилактической мерой может быть регулярный контроль состояния виртуальной среды вышестоящим лицом.

Лучшим способом защиты информационной среды организации в целом является ее разделение по тем или иным критериям и организация доступа к разным разделам в соответствии с политикой информационной [5]. Предполагается такое разделение информации, при котором, во-первых, минимизируется количество запросов со стороны пользователей к защищенной части информационной среды и, во-вторых, несанкционированный доступ одномоментно будет возможен лишь к части конфиденциальной информации, что позволит избежать значительного ущерба.

Исходя из практики, можем рекомендовать включить в инструкции администраторов, отвечающих за обеспечение безопасности информационной среды организации, следующие положения:

– осуществлять автоматизированный контроль соответствия использования токенов и смарт-карт рабочим местам сотрудников, к которым они приписаны,

и проверку пользовательских паролей при подключении виртуальных машин к защищенным сегментам сети;

– осуществлять настройку прав пользователей, их уровня доступа и конфиденциальности, исходя из особенностей функционирования виртуальных машин и удаленного доступа.

Список литературы

1. Мартемьянов Ю.Ф., Яковлев А.В., Яковлев А.В. Операционные системы. Концепции построения и обеспечения безопасности: учебное пособие для вузов. М.: Гор. линия-Телеком, 2010. 332 с.

2. Майкл Хотек. Методы достижения высокой отказоустойчивости // Windows & .NET Magazine/RE. 2003. № 12. [Электронный ресурс]. URL: http://www.rnivc.kis.ru/?id=420 (дата обращения: 18.12.2019).

3. Патрик Лоундс, Чарбел Немном, Леанардо Карвальо. Windows Server 2016 Hyper-V. Книга рецептов. 2-е изд., 2017. [Электронный ресурс]. URL: http://onreader.mdl.ru/windowsServer2016HyperVCookbook2nd/content/index.html (дата обращения: 18.12.2019).

4. Митрохин В.В., Аршинов И.В., Корчиганова А.О. Универсальная электронная карта: достигнутые результаты и проблемы дальнейшего внедрения // Современные проблемы науки и образования. 2014. № 6. [Электронный ресурс]. URL: http://www.science-education.ru/ru/article/view?id=15450 (дата обращения: 19.12.2019).

5. Киреенко А.Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения // Молодой ученый. 2012. № 3. С. 40–46. [Электронный ресурс]. URL: https://moluch.ru/archive/38/4365/ (дата обращения: 18.12.2019).