Русалин Ю.В. Исследования систем информационной безопасности удаленного мониторинга // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 12(38) с. 5–10

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ИССЛЕДОВАНИЯ СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УДАЛЕННОГО МОНИТОРИНГА

Русалин Ю.В.
ФГБОУ ВО "ТЮМЕНСКИЙ ИНДУСТРИАЛЬНЫЙ УНИВЕРСИТЕТ", Тюмень, Россия (625000, Тюменская область, город Тюмень, ул. Володарского, д. 38), e-mail: Rusalin.yurij@yandex.ru

В данной статье отмечается важность мониторинга работы сотрудников как инструмента управления деятельностью предприятия. Описывается методология проведения сравнительного анализа существующих решений. Излагается проблематика предметной области, включающая указания наиболее критичных недостатков и существенных уязвимостей в области обеспечения информационной безопасности пользовательских данных.

Ключевые слова: Защита информации, автоматизация, киберугрозы, безопасность, автоматизация безопасности.

RESEARCH OF INFORMATION SECURITY SYSTEMS REMOTE MONITORING

Rusalin Yu.V.
TYUMEN INDUSTRIAL UNIVERSITY, Tyumen, Russia (625000, Tyumen, Volodarskogo st. 38), e-mail: Rusalin.yurij@yandex.ru

This article notes the importance of monitoring the work of employees as a tool for managing the activities of an enterprise. The methodology for conducting a comparative analysis of existing solutions is described. The problems of the subject area are outlined, including indications of the most critical shortcomings and significant vulnerabilities in the field of ensuring information security of user data.

Keywords: Information security, automation, cyber threats, security, security automation.

В настоящее время процесс всеобщей модернизации системы информационной безопасности удаленного мониторинга предполагает интенсивную интеграцию информационно-коммуникационных технологий. Системы информационной безопасности удаленного мониторинга позволяют осуществлять контроль и предпринимать соответствующие меры по восстановлению информационной безопасности предприятия без необходимости непосредственно присутствовать на предприятии.

На многих предприятиях имеет место множество обращений пользователей по различным вопросам, ввиду чего львиная доля времени тратится на учет подобных обращений, т.е. заявок. Соответственно, все это ведет к появлению простоев в работе предприятия. Пользователи начинают высказывать недовольство начальству по поводу того, что их заявки долго не рассматриваются. Все это определяет актуальность обеспечения

эффективного функционирования систем информационной безопасности удаленного мониторинга на предприятии.

В настоящее время практически во всех направлениях деятельности предприятий крайне остро стоит вопрос конкурентной борьбы. Существует множество инструментов для ведения успешной борьбы на конкурентном рынке, однако, без эффективной команды никакая конкуренция не сможет долго выдерживаться. Чаще всего для качественной реализации какого-либо проекта руководству предприятия нужно заручиться поддержки собственного персонала, хотя бы какой-то его частью. Это необходимо для того, чтобы в случае сопротивления изменениям персонала, «доверенные» лица руководства могли «изнутри» способствовать устранению подобных сопротивлений. Кроме того, «приближенные люди» могут самостоятельно вести проект, т.е. осуществлять соответствующие изменения, однако, все это зависит от сложности проекта. Для подобных целей и требуется формировать команду проекта, благоприятствующую реализации процесса стратегических изменений на предприятии.

Необходимо отметить, что большинство существующих информационных инфраструктур на различных предприятиях независимо от сферы их деятельности обладают определенными общими атрибутами. В настоящее время множество организаций пользуются современными сетями для оптимизации производительности и сокращения издержек ввиду роста уровня интеграции внешней сетей, сетей бизнеса. Но данные стратегии нередко ведут к появлению определенного рода уязвимостей, существенным образом снижающих уровень информационной безопасности организации. Кроме того, эти стратегии могут подвергнуть важнейшие системы управления киберугрозам. Одним из ключевых достоинств систем информационной безопасности удаленного мониторинга представляется возможность расширения функций управления и контроля ввиду применения функционала удаленного доступа [8, с.35]. В компании, занимающейся инновационной деятельностью и реализацией различных информационных услуг, Service Desk является обязательным подразделением, без которого не может обойтись ни один отдел компании. Работает данный отдел круглосуточно, поскольку даже минимальный простой технического оборудования компании способен нанести существенный урон как финансового, так и материального характера. Все это может причинить вред также и репутации организации, что крайне важно в контексте наличия на конкурентном рынке многих игроков.

Без осуществления конкретных мер безопасности функции удаленного доступа способны формировать комфортные возможности для киберпреступников, которые стремятся нанести ущерб важным процессам того или иного предприятия, оказать негативное влияние на жизни людей, социум, экономику, а также окружающую среду.

Так или иначе на данный момент существует достаточно много подобных систем, каждая из которых имеет присущие только ей преимущества и недостатки [2, с.75].

Аутентификация представляет собой процесс идентификации человека, основанный на имени пользователя и пароле. Однако аутентификация представляет собой лишь небольшую составляющую общего процесса обеспечения информационной безопасности. Львиная доля крупных компаний тратит внушительные финансовые объемы на обеспечение кибербезопасности, отличаясь как раз этим от мелких компаний. Кроме того, всем организациях нужно понять, что обучение персонала взаимодействию с системой информационной безопасности удаленного доступа является небходимой задачей

организации, и тем быстрее оно будет осуществлено, тем скорее повысится общий уровень информационной безопасности организации [3, с.512].

Раньше соединение для удаленного доступа реализовывалось благодаря действию традиционных технологий коммутируемого доступа. Такие технологи были довольно дорогими ввиду того, что компания покупала выделенный канал в аренду в телефонной сети общего пользования.

В частности, Пинола М. осуществляет анализ удаленного рабочего стола, который представляет собой один из методов удаленного доступа. Данный метод дает возможность пользователю получить удаленный доступ к другому компьютеру и осуществлять им управление из удаленного места, как если бы удаленный компьютер являлся локальным [6].

Также целесообразно рассмотреть виртуальную частную сеть – VPN – представляющую собой расширение локальной сети при помощи создания туннеля между конечными точками благодаря технологиями Secure Socket Layer, Open VPN и пр.VPN дает возможность удаленному пользователю стать частью корпоративной сети, предоставляя ему доступ к соответствующим ресурсами корпорации. Чаще всего в VPN применяется протокол туннелирования уровня 2 (L2TP), дающий возможность поставщикам услуг дать клиентам удаленный коммутируемый доступ к VPN. Для защиты данных через Интернет данные шифруются и инкапсулируются благодаря технологии IP Security. Гарантируется, что данные, которые проходят через туннель, не перехватятся атаками хакеров. При помощи указанных мер информационной безопасности, которые имеют место в случае использования VPN-подключений, предприятия в некотором роде полагаются на надежность VPN для оптимизации производительности, т.к. персонал может получать доступ к ресурсам из любого места за пределами рабочего помещения. VPN-соединение включает следующие варианты: клиент-сайт и сайт-сайт. Первый вариант включает корпоративную сеть и удаленного пользователя, второй – как минимум две корпоративные сети. Прочие методы включают глобальную сеть (WAN), цифровую сеть с интегрированными услугами (ISDN), а также цифровую абонентскую линию (xDSL) [1, с.410].

Определенные VPN-приложения обладают протоколами туннелирования без шифрования. Отмечается, что другие приложения VPN не туннелируют трафик IPv6 и DNS через туннельный интерфейс ввиду отсутствия поддержки IPv6, ошибочных настроек разработчиков. Отсутствие эффективного шифрования, утечка трафика способны упростить онлайн-мониторинг, реализуемый промежуточными устройствами на пути, такими, как коммерческие точки доступа Wi-Fi, которые аккумулируют данные пользователей, а также агентствами по наблюдению [4, с.920].

Эрнест Д. предлагает эффективные технологии для реализации необходимой поддержки сетевым администраторам при помощи интеграции безопасного приложения для удаленного системного администрирования, функционирующего на смартфонах Android. Это необходимо для помощи администраторам удаленно администрировать серверы, когда они не находятся в офисе, при помощи своих смартфонов [9, с.164]. Приложение для Android, которое создано в Eclipse, создает безопасное соединение с удаленным сервером, где запущено приложение PHP. Приложение разработано с принятием во внимание протокола удаленного буфера кадров (RFB). Данный протокол, однако, обладает определенными недостатками в безопасности, включая уязвимость к атаке «человек посередине» (MITM) с применением соответствующих инструментов. Ввиду этого в приложение для Android внесен самозаверяющий сертификат

Secure Socket Layer для реализации безопасного зашифрованного соединения. Эти соединения должны налаживаться между приложением Android и удаленным сервером для обеспечения сквозной защиты от атак [7, с.20].

Учитывая необходимость поддержания информационного обмена с другими локальными сетями, а также получения информации из Интернета, особое внимание уделяется защите от внешних атак. Реализация защиты от внешних атак осуществляется применением сертифицированных по требованиям безопасности информации межсетевых экранов и других специализированных средств, а также путем запрета использования информации из внутренней сети вне контура.

Что касается принципа функционирования систем удаленного мониторинга, то здесь записи в журнал вносятся ежедневно, причем в бумажном варианте приходится все данные вводить снова, т.е. отсутствует какой-либо единый шаблон для реализации данного процесса. Таким образом, время внесения одной записи в журнал составляет 40 минут, а с учетом количества заявок ежедневно, практически весь рабочий день уходит на осуществление данного процесса.

Кроме того, комплекс технических средств обеспечения информационной безопасности может позволить использовать постоянный централизованный антивирусный мониторинг на персональных компьютерах пользователей с помощью средств ПО Kaspersky endpoint security.

Чтобы найти определенную заявку, приходится поднимать архивы всей информации, а не отсортированной по какому-либо критерию. Львиную долю времени также занимает процесс формирования реестра заявок, требующихся исполнения. Очевидным становится факт, что без автоматизации процесса учета заявок пользователей не обойтись. Но и сама автоматизация должна не только облегчать сам процесс учета заявок, но и обеспечивать его безопасность, поскольку заявки присылаются от разных пользователей, и есть вероятность, что их содержание будет искажено или включать какой-либо вирус.

Преимущество системы удаленного мониторинга заключается не только в минимизации времени как на отдельную операцию, так и на процесс в совокупности, но и в оптимизации издержек на учет пользовательских заявок.

Все это приносит дополнительную прибыль предприятию, позволяя направить этот излишек на совершенствование деятельности организации – расширение ассортимента, внедрение новых технологий, диверсификацию услуг и пр.

Таким образом, нарастающая скорость развития информационных технологий значительным образом изменила принципы работы систем информационной безопасности удаленного мониторинга. Удаленная работа в настоящее время представляет собой важную составляющую функционирования многих предприятий. Кроме того, сейчас имеет место практика интеграции различных мобильных устройств в корпоративную сеть. Ввиду этого имеет место актуальная потребность интеграции и обеспечения соблюдения установленной политики безопасности и удаленной аутентификации конечных пользователей [5, с.1370]. Пользователь так или иначе представляет собой ключевой фактор риска для информационной безопасности предприятия, ввиду чего ему надо уделить пристальное внимание для смягчения последствий уязвимостей аутентификации пользователя. Помимо всего прочего, организациям надо улучшать уровень обучения и осведомленности о кибербезопасности, но одного лишь обучения мало для смягчения киберугроз. Организациям в обязательном порядке нужно осуществлять оценки информационной безопасности на постоянной основе,

мониторить сетевой трафик на предмет всяческих вредоносных действий и интегрировать развитые механизмы аутентификации пользователь. Например, в качестве решения для безопасности удаленного доступа пользователей можно применять двухфакторную аутентификацию. Удаленное устройство тоже должно быть аутентифицировано, даже если присутствует подлинный пользователь.

Создание технологии защиты регистрируемых данных, транслируемых через открытый коммуникационный канал к облачному хранилищу остается актуальной задачей и требует разработки новых математических методов, моделей и алгоритмов для реализации шифрования и расшифрования сообщений.

Список литературы

1. Авани П., Анкита Г. Обзор оценки эффективности VPN // Journal on Recent and Innovation Trends in Computing. – 2017. – Т. 5, - №5. – С.409 – 413.
2. Булдакова Т.И., Гриднев В.И., Кириллов К.И., Ланцберг А.В., Суятинов С.И. Программно-аналитический комплекс модельной обработки биосигналов // Биомедицинская радиоэлектроника. 2019. № 1. С. 71-78.
3. Вигнеш У., Аша С. Изменение политик безопасности в отношении BYOD // 2-й Международный симпозиум по большим данным и облачным вычислениям. – 2018. - №50. - С. 511 – 516.
4. Джоти К.К., Редди Д.Б. Исследование виртуальной частной сети (VPN), протоколов VPN и безопасности // Journal of Scientific Research in Computer Science, Engineering and Information Technology. – 2018. - № 3. – С. 919-932.
5. Ли С., Ню Ц., Хан М.Х., Ляо Дж. Усовершенствованная схема аутентификации удаленного пользователя по паролю на основе смарт-карты // Journal of Network and Computer Applications. – 2013. - №36. – С. 1365–1371.
6. Пинола М. Что такое удаленный доступ? [Электронный ресурс]. – Режим доступа: URL: https://www.lifewire.com/what-is-remote-access-2377975 (дата обращения: 7 сентября 2023).
7. Свапнонил Р., Чанчал К. Криптоанализ и улучшение протоколов аутентификации и обмена ключами на основе ECC // MDPI. – 2017. – Т. 9, - №1. – С. 1-25.
8. Суятинов С.И., Самочетова Н.С., Ланцберг А.В., Коблов А.В. Методика идентификации сложных систем // Вестник Саратовского государственного технического университета. 2017. Т. 4. № 1 (28). С. 31-38.
9. Эрнест Д. и др. Сравнительное исследование технологий удаленного доступа и реализации приложения для смартфона для удаленного системного администрирования на основе предлагаемого безопасного протокола RFB // Международный журнал науки и инженерных приложений. – 2015. – Т. – 4, - № 4. – С. 163-168.

References

1. Avani P., Ankita G. Review of VPN efficiency assessment // Journal on Recent and Innovation Trends in Computing. – 2017. – Vol. 5, - No.5. – pp.409-413.
2. Buldakova T.I., Gridnev V.I., Kirillov K.I., Lantsberg A.V., Suyatinov S.I. Software and analytical complex of model processing of biosignals // Biomedical radioelectronics. 2019. No. 1. pp. 71-78.

3. Vignesh U., Asha S. Changing security policies regarding BYOD // 2nd International Symposium on Big Data and Cloud Computing. - 2018. - No.50. - pp. 511 – 516.
4. Joti K.K., Reddy D.B. Virtual Private network (VPN) research, VPN protocols and security // Journal of Scientific Research in Computer Science, Engineering and Information Technology. - 2018. - No. 3. – pp. 919-932.
5. Li S., Nu C., Han M.H., Liao J. An improved authentication scheme for a remote user using a password based on a smart card // Journal of Network and Computer Applications. - 2013. – No.36. – pp. 1365-1371.
6. Pinola M. What is remote access? [electronic resource]. – Access mode: URL: https://www.lifewire.com/what-is-remote-access-2377975 (date of access: September 7, 2023).
7. Swapnonil R., Chanchal K. Cryptanalysis and improvement of authentication and key exchange protocols based on ECC // MDPI. – 2017. – Vol. 9, - No. 1. – pp. 1-25.
8. Suyatinov S.I., Samochetova N.S., Lanzberg A.V., Koblov A.V. Method of identification of complex systems // Bulletin of the Saratov State Technical University. 2017. Vol. 4. No. 1 (28). pp. 31-38.
9. Ernest D. et al. A comparative study of remote access technologies and the implementation of a smartphone application for remote system administration based on the proposed secure RFB protocol // International Journal of Science and Engineering Applications. – 2015. – Vol. – 4, - No. 4. – pp. 163-168.