7. Unreal Engine: from gaming to ground-breaking cures. URL: https://www.pharmaceutical-technology.com/features/unreal-engine-gaming-ground-breaking-cures/

8. Air Canada uses VR to showcase its top-flight business class service. URL: https://www.unrealengine.com/en-US/spotlights/air-canada-uses-vr-to-showcase-its-top-flight-business-class-service .

9. Игровые движки теперь не только для игр. URL: https://ru.hexlet.io/blog/posts/igrovye-dvizhki-teper-ne-tolko-dlya-igr

10. Get Unity Certified. URL: https://unity.com/products/unity-certifications/vr-developer

11. C# vs C++. Complete comparison between Unity and Unreal programming languages. URL: https://circuitstream.com/blog/c-vs-c-complete-comparison-between-unity-and-unreal-programming-languages/

Ключові слова: віртуальна реальність, доповнена реальність, XR-розробник, ігрові рушії.

Ключевые слова: виртуальная реальность, дополненная реальность, XR-разработчик, игровые движки.

Keywords: virtual reality, augmented reality, XR-developer, gaming engines.

Науковий керівник: *к.т.н., доц. Трофименко О. Г.*

Баланюк Никита Сергеевич

Национальний университет «Одесская юридическая академия»,

студент 3-го курса факультета кибербезопасности и информационных технологий

КИБЕРБЕЗОПАСНОСТЬ НА УДАЛЕННОЙ РАБОТЕ

В последнее время переход на удаленную работу сопутствуется с нововведениями и проблемами. В частности, организация информационной

безопасности должна была претерпеть изменения в связи с переносом рабочей среды в домашние офисы. А значит существует необходимость в более высоком уровне информационной безопасности и ее более технологичной технической составляющей. Но основные задачи остались неизменными: доступность конфиденциальность и целостность информации, а сейчас с учетом удаленности сотрудников.

1. Угрозы безопасности для дистанционных работников.

Работники находятся в зоне рисков по разным причинам. Устанавливаемое ПО может быть зараженным, незащищенные соединения, вредоносные веб-ресурсы. Никто не отменял простейший фишинг во время перехода на сайт компании для входа в среду разработки или кейлоггер скачанный вместе с ПО из интернета. Необходимость в современных и гибких решениях, как никогда необходима в связи последними событиями в мире. Пандемия стала катализатор для активизации всевозможных хакерских групп, улучшенная инфраструктура и технические возможности позволят им сильнее влиять своими действиями на современный мир. Мобильные устройства остаются самыми желанными целями т.к. каждый из нас держит огромный объем информации о себе в телефоне. В 2021 году программы-вымогатели атаковали каждую 61 организацию в мире каждую неделю. Злоумышленники нацелены на компании, которые могут позволить себе уплату выкупа. Планируется что в 2022 году атаки с вымогателями станут только изощреннее. Хакеры будут все чаще использовать инструменты проникновения для настройки атак в реальном времени, а также для работы в сетях жертв [1].

2. Необходимость в защищенном виртуальном рабочем месте для удаленного сотрудника (VDI).

Для защиты работника первичной необходимостью является защищенное рабочее место. Самым простым способом является перенос приложения, не изменяя процедур и изоляция людей. Или менять подход, если к примеру человек застрял в другой стране без доступа к своему рабочему устройству. Единая идентификация применяется для гибкости работы и мобильности сотрудника. Дает возможность подключения и идентификацию с любого устройства и доступ

ко всем необходимым материалам. Это все реализуется с помощью VDI, они запускаются в центре обработки данных (ЦОД). В этом случае ЦОД не подвергается опасности, т.к. мы запускаем свой VDI и просто передаем картинку. И в этом случае вы получаете возможность обезопасить себя от различного рода зловредов, которые могут находиться на ваших конечных устройствах. Существуют также виртуальные офисы, такое предоставляют отдельные компании вместе с набором необходимых инструментов. На практике легче и безопаснее заказать такую услугу.

3. Безопасная среда для разработки.

Для защиты ЦОД в большинстве компаний используется виртуализирование, которое придает ей гибкость и доступность. Такая технология дает доступ к общему облаку, а также дает возможность развертки сразу на нескольких серверах. Что делает ее уязвимой для атак. Для обеспечения безопасности используют сетевые экраны или фаерволы. Также используется ПО для мониторинга и настройки политик безопасности. Также существуют права доступа и при крайней план восстановления системы при потере доступа к облачным сервисам. Также можно использовать микросегментацию. Этот подход помогает разделить защиту на сегменты на уровне рабочих нагрузок. А значит позволяет создать защиту для каждого приложения и не дать больше нужного уровня доступа чем необходимо и распределить нагрузку. Механизм адаптивный и динамичный благодаря его политикам, которые также могут генерироваться автоматически. Может создаваться на основе межсетевых экранов или на основе защиты конечного хоста что подходит лучше. Защитить устройства пользователя. В большинстве случаев компания не может предоставить своим сотрудникам оборудование поэтому они используют свое. Необходимо идентифицировать как само устройство, так и его пользователя. MDM-системы дают возможность управления любыми устройствами сотрудников, это решение позволяет мониторить действия сотрудника и предотвращать возможные атаки, но обеспечивают безопасность только на самом устройстве.

4. Защита каналов связи.

Использование интернет в качестве канала связи на данный момент зачастую является единственно возможным решением. При этом необходимо понимать, что сеть интернет не защищает своих пользователей от перехвата и компрометации сеансов связи.

1) Применяемые меры.
2) Построение виртуальных сетей связи с помощью средств VPN.
3) Защищенные протоколы передачи данных.
4) Криптографическая защита информации, передаваемой посредством сети Интернет.
5) Настройка алгоритмов шифрования.
6) Контроль за целостностью документов.
7) Динамическая аутентификация пользователей.
8) Примером этой технологии является SMS-рассылка одноразовых паролей.
9) Применение электронного сертификата.
10) Электронный сертификат подтверждает принадлежность ключа владельцу, используется при создании ЭЦП [2].

Список использованной литературы:

1. Информационный портал TADVISER Статья:Главные тенденции в защите информации веб-сайт. URL: https://www.tadviser.ru/index.php/Статья:Главные_тенденции_в_защите_информации (дата звернення: 11.05.2021)

2. Информационный портал TADVISER Интервью TAdviser: Александр Василенко, VMware – о формуле эффективности для «удаленки»веб-сайт. URL: https://www.tadviser.ru/index.php/ Статья: Безопасный доступ с любого устройства к любому приложению в любом облаке – формула эффективности VMware для удаленки (дата звернення: 11.05.2021)

Ключові слова: пристрій, безпека, доступ.

Ключевые слова: устройство, безопасность, доступ.