Организация Объединенных Наций по промышленному развитию

Distr.: General
20 September 2024
Russian
Original: English

Совет по промышленному развитию
Пятьдесят вторая сессия
Вена, 25–27 ноября 2024 года
Пункт 4 (f) предварительной повестки дня
Общее управление рисками

Обновленная информация об общем управлении рисками

Доклад Генерального директора

В своем заключении 2016/8 Комитет по программным и бюджетным вопросам «предложил Генеральному директору представить Совету по промышленному развитию и Комитету по программным и бюджетным вопросам на их следующих сессиях доклады об общей стратегии ЮНИДО по управлению рисками и предложить всеобъемлющие меры для того, чтобы преодолеть финансовые и административные последствия выхода государств-членов из Организации, в том числе чтобы переломить тенденцию к выходу».

В настоящем документе представлена обновленная информация к докладу, представленному на сороковой сессии Комитета (IDB.52/9-PBC.40/9), и отмечается создание новой специализированной Группы по управлению рисками и обеспечению соответствия требованиям в рамках Директората корпоративных услуг и операций, включая дополнительные функции, связанные с кибербезопасностью.

I. Введение

1. В результате принятия скорректированной структуры Секретариата ЮНИДО 2024 года (DGB/2024/03) ЮНИДО создала Группу по управлению рисками и обеспечению соответствия требованиям. Новая Группа оказывает поддержку директору-управляющему Директората корпоративных услуг и операций в качестве назначенного координатора ЮНИДО по общеорганизационному управлению рисками (ОУР) в целях дальнейшей разработки, координации и внедрения рамок УОР и информационной безопасности ЮНИДО. Группа также оказывает активную поддержку старшему руководству в формировании надежной культуры риска. Помимо функций управления рисками и обеспечения соответствия требованиям мандат Группы касается управления кибербезопасностью.

2. В настоящем документе освещаются действия, предпринимаемые ЮНИДО для выявления и уменьшения угрозы возникновения рисков в сфере кибербезопасности.

II. Система обеспечения кибербезопасности и ее совершенствование

3. Во исполнение рекомендаций Объединенной инспекционной группы (ОИГ), содержащейся в ее докладе, озаглавленном «Кибербезопасность в организациях системы Организации Объединенных Наций» (JIU/REP/2021/3) ЮНИДО представляет всеобъемлющий обзор принятых мер, связанных с ее системой кибербезопасности. В обзоре, содержащемся в документе зала заседаний IDB.52/CRP.14, описываются критические элементы и действия, предпринимаемые для защиты Организации от киберугроз и внедрения надежных методов обеспечения безопасности.

4. ЮНИДО добилась существенного прогресса в укреплении своей системы кибербезопасности, приведя ее в соответствие с рекомендациями Внешнего ревизора, ОИГ и передовой отраслевой практикой. Организация создала прочную основу кибербезопасности, определив структуру управления и создав систему управления информационной безопасностью (в соответствии с ISO 27001) на основе Политики информационной безопасности ЮНИДО (DGB/2023/01), а также Административной инструкции по процессу управления рисками в сфере информационной безопасности (AI/2024/01), в которой описывается процесс, позволяющий обеспечить выявление, оценку, устранение и смягчение рисков в сфере информационной безопасности эффективным, своевременным и структурированным образом.

5. По мере осуществления своей деятельности ЮНИДО крайне важно последовательно применять упреждающий подход в вопросах кибербезопасности. Это предполагает постоянную переоценку рисков, расширение технических возможностей и формирование культуры осведомленности о кибербезопасности в рамках всей Организации. Благодаря таким усилиям ЮНИДО не только будет иметь возможность противостоять новым киберугрозам и защищать свои информационные активы, но и будет поддерживать свою более широкую миссию, демонстрируя устойчивость и уверенность.

6. В докладе Внешнего ревизора по счетам ЮНИДО за финансовый год с 1 января по 31 декабря 2023 года (IDB.52/4-PBC.40/4), представленном на сороковой сессии Комитета по программным и бюджетным вопросам, Внешний ревизор подтвердил прогресс ЮНИДО в области кибербезопасности, отметив выполнение всех пяти рекомендаций, касающихся создания специальной функции по кибербезопасности, разработки Системы управления информационной безопасностью и внедрения процесса выявления и устранения факторов уязвимости. Были также рассмотрены и устранены критические технические параметры уязвимости, выявленные Внешним ревизором, а тест на проникновение в систему безопасности 2023 года, проведенный ЮНИДО при поддержке специализированных внешних компаний, позволил выявить дополнительные проблемы, которые были включены в рабочий план в отношении услуг по цифровизации, инновациям и оптимизации технического сотрудничества. Оценка рисков в сфере информационной безопасности, проведенная в 2023 году, также позволила определить ключевые активы и риски, что привело к разработке всеобъемлющего плана устранения рисков в сфере информационной безопасности на 2023–2024 годы, включающего 35 мероприятий, из которых 15 завершены, а остальные находятся в стадии осуществления. Общий обзор этих мероприятий представлен в приложении к настоящему документу. Результаты подтверждают эффективность функции кибербезопасности ЮНИДО в плане упреждающего выявления и управления рисками, а также повышения безопасности и устойчивости Организации.

7. Настоящий документ дополняется документом зала заседаний IDB.52/CRP.14, в котором описываются процессы, способствующие повышению киберустойчивости Организации.

III. Меры, которые надлежит принять Совету

8. Совет, возможно, пожелает принять к сведению информацию, содержащуюся в настоящем документе.

Приложение

Ход выполнения мероприятий, предусмотренных в плане устранения рисков в сфере информационной безопасности на 2023–2024 годы

Завершенные мероприятия

1. Тестирование на проникновение: привлечен внешний подрядчик для проведения тщательного тестирования на проникновение с целью имитации злоумышленника с внутренним доступом. Это привело к уточнению элементов управления и включению новых мероприятий в план устранения рисков.

2. Внедрение современного метода аутентификации для обмена в интернете: внедрение современного метода аутентификации для Exchange Online для повышения безопасности электронной почты.

3. Вывод из эксплуатации системы обмена файлами xFiles: успешно выведена из эксплуатации устаревшая система обмена файлами ЮНИДО и внедрено современное решение для обмена на основе Microsoft 365 (OneDrive), что сократило диапазон для совершения атак.

4. Улучшение аутентификации для Microsoft Teams: внедрение многофакторной аутентификации для Teams в целях снижения рисков хищения учетных данных.

5. Улучшение регламента в отношении паролей: разработка и внедрение новых процедур, охватывающих комплексные регламенты в отношении паролей, установление правил и мониторинг соответствия.

6. Улучшение аутентификации, поведения пользователей и безопасности: переход на единый вход (SSO) на основе Microsoft 365 Azure AD, улучшение мониторинга, устойчивости и доступности.

7. Внедрение многофакторной аутентификации для облачных систем: включение многофакторной аутентификации для всех служб, использующих облачную аутентификацию для усиления безопасности.

8. Средства и процесс выявления и устранения факторов уязвимости: внедрение средств выявления и устранения факторов уязвимости, охватывающего критически важные ресурсы, такие как общедоступные системы, критически важные серверы и рабочие станции администраторов. Также были разработаны дополнительный процесс и процедура в соответствии с рекомендациями внешнего аудитора и передовой практикой.

9. Улучшение контроля соответствия: улучшение контроля соответствия ключевых элементов обеспечения кибербезопасности в соответствии с минимальными базовыми показателями ООН и передовой практикой Microsoft.

10. Повышение безопасности систем Microsoft 365: внедрение бесшовного единого входа для выбранных систем Microsoft 365, улучшение опыта пользователей и повышение безопасности.

11. Внутренние системы специализированного обучения для администраторов информационных технологий (ИТ): проведено внутреннее перекрестное обучение для администраторов ИТ и разработаны специализированные курсы для привилегированных пользователей.

12. Проверка хранилища файлов в отделениях на местах: завершена проверка разрешений и проведена оценка миграции общих ресурсов отделений на местах в Teams для повышения безопасности.

13. Улучшение процессов и регламентов безопасности: улучшены процессы и регламенты, связанные с правами доступа, разделением обязанностей и безопасными конфигурациями, что сокращает отклонения от стандартных практик.

14. Оптимизация процессов информационной безопасности: приняты и адаптированы современные передовые практики в области информационной безопасности для оптимизации осведомленности сотрудников Организации в вопросах безопасности.

15. Проверка безопасности Teams: проведена проверка настроек безопасности и разрешений в Teams.

Текущие мероприятия

16. Проверка учетных записей на основе принципов необходимости ознакомления и наименьших привилегий: продолжение проверки привилегированных и служебных учетных записей, прав доступа к файлам и применения таких мер, как решение по паролю местного администратора.

17. Внедрение защиты учетных данных: для повышения безопасности и снижения риска компрометации учетных данных проводится установка функции безопасности Credential Guard на серверах и конечных точках.

18. Внедрение новейших регламентов паролей в ЮНИДО: обновление регламентов паролей и привилегированного доступа на основе обновленных процедур регламента паролей.

19. Улучшения управления исправлениями: текущие усилия направлены на совершенствование управления исправлениями и процессов восстановления.

20. Улучшение безопасности SAP: реализуются меры по реализации рекомендаций по результатам ревизии и улучшению гигиены безопасности в системе SAP.

21. Улучшение системы сетевой защиты: внедряются усовершенствования, включая реализацию принципа нулевого доверия и полный обзор архитектуры системы сетевой защиты, управления и регламентов безопасности.

22. Замена инструмента управления паролями для ИТ-администраторов: осуществляется процесс замены устаревшего инструмента управления паролями для ИТ-администраторов.

23. Оценка зрелости системы нулевого доверия: проводится комплексная оценка зрелости системы нулевого доверия для планирования будущих улучшений.

24. Вывод из эксплуатации/замена устаревших систем: постоянные усилия по выводу из эксплуатации и замене устаревших систем для сокращения диапазона для совершения атак.

25. Улучшение процесса реагирования на инциденты безопасности: проводится совершенствование процессов и инструментов реагирования на инциденты как с использованием внутренних, так и внешних ресурсов.

26. Контролирование ключевых элементов управления для SAP: осуществляется внедрение системы контроля соответствия для ключевых элементов управления в SAP и вспомогательных процессов в соответствии с рекомендациями внешнего ревизора.

27. Разделение обязанностей в ИТ для системы общеорганизационного планирования ресурсов: продолжается усиление разделения обязанностей в ИТ для SAP, насколько позволяют ресурсы и в соответствии с рекомендациями внешнего ревизора.

28. Персонализированные учетные записи для администраторов: продолжается внедрение персонализированных и отдельных учетных записей для ИТ-администраторов в различных системах.

29. Экспериментальное применение аутентификации без пароля: проводятся оценка и экспериментальное применение инновационных методов аутентификации без пароля для повышения безопасности при упрощении доступа.

30. Обзор поставщиков интернет-услуг в отделениях на местах: проводится обзор качества и пропускной способности интернет-услуг в отделениях на местах.

31. Расширение сотрудничества с внешними партнерами: проводится изучение возможностей сотрудничества с внешними партнерами для получения специализированных знаний и потребностей в сфере безопасности.

32. Разработка дорожной карты нулевого доверия: ведется разработка дорожной карты нулевого доверия, соответствующей приоритетам деятельности и профилям рисков.

33. Многофакторная аутентификация для всех общедоступных служб: ведется внедрение многофакторной аутентификации для всего внешнего и привилегированного доступа.

34. Совершенствование управления активами и систем обнаружения: ведутся работы по улучшению инструментов управления активами и систем обнаружения, включая расширение номенклатуры серверов и уточнение процедур развертывания исправлений.

35. Рассмотрение центра аварийного восстановления: ведется планирование вторичного центра аварийного восстановления и резервного копирования данных для обеспечения бесперебойного функционирования организации.