Апрель 2025

Новая эпоха IT-безопасности

КУРСИВ | GUIDE

5 важнейших стратегий,
обеспечивающих безопасность бизнес-данных

Практика безопасной разработки(devsecops)

Риск-ориентированный подход к ИБ

как не потерять данные клиентов из ваших мобильных приложений?

Как пентест соответствует целям бизнеса?

План реагирования на киберинциденты – простой документ или сложныйплейбук?

сторонние риски, связанные с цепочкой поставщиков

Евгений Питолин

Управляющий директор DataStar,
сопредседатель комитета
по информационной безопасности
Альянса Qaztech.

Больше безопасности

Человекоцентричность и риск-ориентированный подход – ключевые термины для понимания кибербезопасности 2025 года.

Перед вами специальный обзор **Kursiv | Business Guide**, посвященный Cyber & Digital Security – крупнейшему ивенту в области кибербезопасности в РК, который пройдет 2 и 3 апреля в Астане. Темы и материалы выпуска пересекаются с программой ивента, а размышления экспертов подтолкнут вас к действиям после того, как мероприятие подойдет к концу.

Риск-ориентированный подход к информационной безопасности, при том, что он наращивает популярность в Казахстане, по-прежнему недооценивается бизнесом. При этом особенно печально осознавать, что речь зачастую идет о компаниях, которые можно назвать небольшими, но лишь по количеству сотрудников и подходу к защите, тогда как по составу абонентской базы, количеству денег и данных они вполне соответствуют крупной корпорации.В первую очередь злой рок настигает в подобных компаниях системы, связанные с базами контрактов, управлением человеческими ресурсами, общением с клиентами и выставлением счетов.

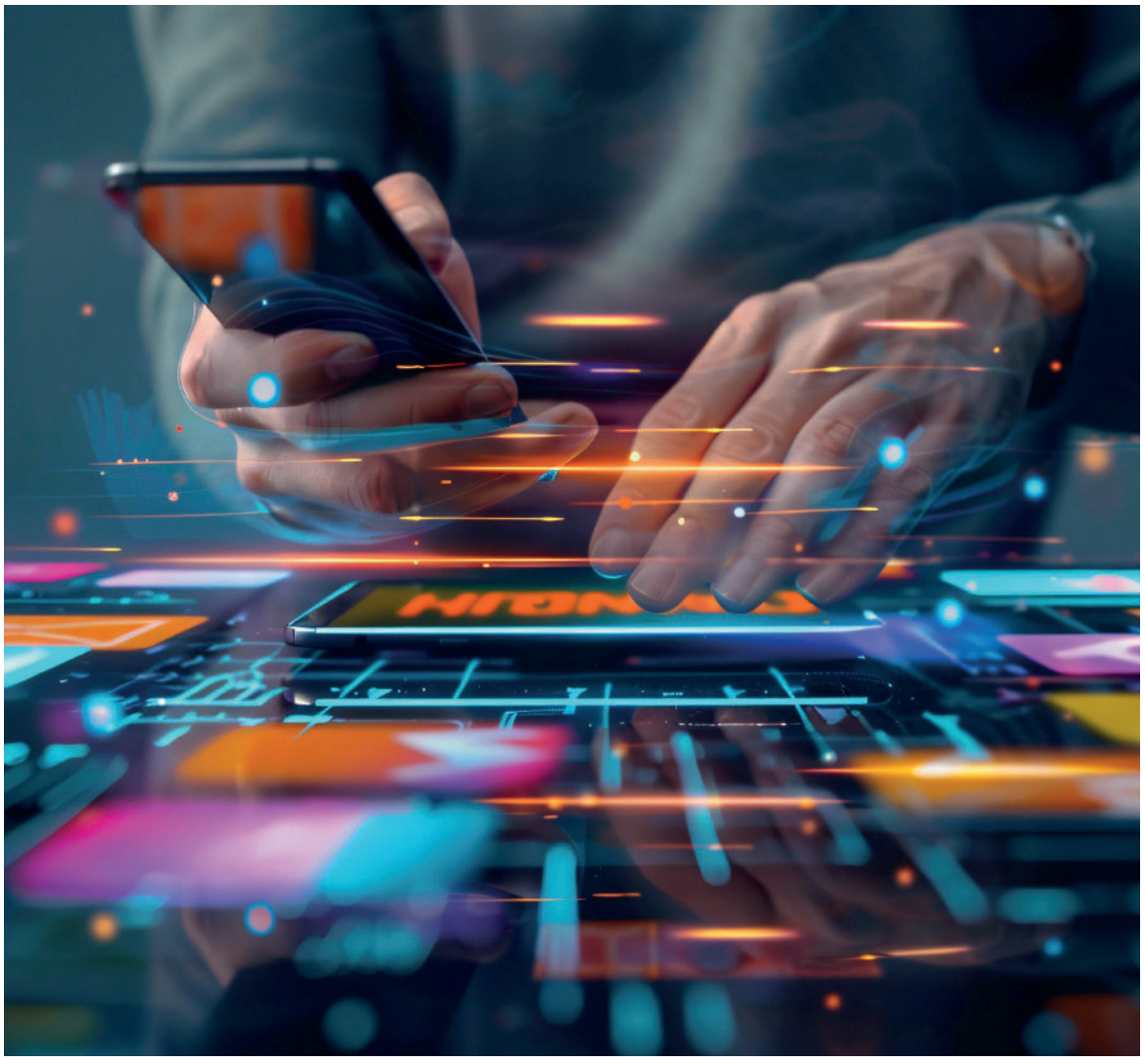
HR, ИТ и ИБ необходимо больше места за общим столом переговоров при обсуждении безопасности и ее влияния на бизнес. Это наименьшее, что руководителям стоит сделать для своего бизнеса в 2025 году.

Немного о цифровых продуктах: как не потерять данные клиентов из ваших мобильных приложений?

Как мы уже писали в этом выпуске, нельзя просто так взять и предотвратить утечку данных. Превентивный подход к утечкам – это и частые оценки третьей стороной собственной безопасности, и правильное шифрование данных, и информирование о возникающих угрозах. Как это все применить, чтобы защитить информацию пользователей и не допустить нарушений безопасности в мобильных приложениях?

Как случается утечка данных из мобильного приложения?

Нарушение правил хранения данных в мобильном приложении происходит, когда несанкционированные лица получают доступ к конфиденциальной информации, хранящейся, передаваемой и обрабатываемой мобильным приложением. Эти нарушения происходят из-за слабой аутентификации, уязвимостей безопасности, злонамеренных атак и незашифрованных данных. Нарушение правил хранения данных может привести к краже личных данных и финансовым потерям. В пику стереотипу., хакеры не всегда реализуют уязвимости удаленно. Доступ к физическим активам жертвы вручную или на близком расстоянии является одним из распространенных способов их возникновения.



Способы предотвращения утечки данных в мобильных приложениях

Зашифруйте все данные внутри приложения

Правильное шифрование защищает все данные вашего приложения и предотвращает утечку данных. Шифрование превращает конфиденциальную информацию в нечитаемый код, гарантируя, что хакеры не смогут понять ее, даже если перехватят.

Внедрите надежные протоколы шифрования

Вам понадобится сквозное шифрование для защиты хранимых и передаваемых данных. Используйте безопасные ключи и часто обновляйте методы шифрования, чтобы защитить свое приложение от новых угроз и несанкционированного доступа.

Избегайте кэширования данных

Многие приложения автоматически сохраняют данные для улучшения пользовательского опыта. К веб-данным, таким как истории транзакций, файлы cookie и данные, вводимые в формы, можно легко получить доступ через кэшированную информацию. Чтобы справиться с этим, отключите кэширование конфиденциальных данных, используйте безопасное хранилище и внедрите автоматическую очистку кэша.

Киберпреступники часто эксплуатируют незащищенные сети, используя их для перехвата данных с помощью различных атак, таких как «человек посередине». Вот почему мониторинг доступа к сети необходим для предотвращения утечки данных мобильных приложений.

Александр Пушкин,
руководитель SOC, PS Cloud Services

Мониторинг доступа к сети

Используйте инструменты мониторинга сети в режиме реального времени для выявления подозрительного поведения и обнаружения несанкционированного доступа. Ограничьте доступ вашего приложения к доверенным серверам, чтобы повысить безопасность и защитить пользовательские данные от взлома.

Запускайте регулярно пентесты мобильных приложений

Благодаря тестированию безопасности мобильных приложений вы можете выявить и устранить уязвимости до того, как ими воспользуются хакеры. Эти тесты имитируют реальные кибератаки и оценивают слабые места в аутентификации вашего приложения, сетевой связи и хранении данных. Частые тесты на проникновение гарантируют соответствие вашего приложения стандартам безопасности и позволяют разработчикам вовремя устранять любые уязвимости. Таким образом вы снизите риски взломов и защитите конфиденциальные данные.

Дмитрий Кан, Engine,ER Lab.

Изучайте сторонние риски, связанные с цепочкой поставщиков Большинство приложений полагаются на сторонние облачные сервисы, интерфейсы прикладного программирования (API) и комплекты разработки программного обеспечения (SDK). Если вы не обратите внимания, они могут легко создать уязвимости безопасности в вашем приложении.

Убедитесь, что сторонние поставщики соответствуют необходимым стандартам безопасности. Чтобы защитить данные вашего приложения, установите приоритет безопасности API, ограничьте доступ третьих лиц к конфиденциальной информации и отслеживайте интеграции с партнерами Вашего приложения.

Дивный новый мир IT-безопасности

Одним из главных сюрпризов прошлого года на рынке безопасности в РК – больше не надо пугать компании злыми хакерами и пентестом, утечки данных и кибератаки каждый день попадают в заголовки новостей, поэтому директора организаций начинают понимать, что проактивная защита важна для непрерывности бизнеса. Тестирование на проникновение - контролируемая симуляция реальных атак, в этом контексте сервисы пентеста помогают выявить лазейки в безопасности до того, как злоумышленники смогут ими воспользоваться.

Так или иначе, опытные киберпреступники постоянно совершенствуют свою тактику, тщательная оценка рисков становится как никогда важной. Заблаговременно выявляя уязвимости, эти оценки позволяют организациям активно укреплять свою защиту. Независимо от того, защищает ли конфиденциальные данные клиентов или обеспечивает соблюдение требований, тестирование на проникновение играет ключевую роль в поддержании доверия и защите критически важных активов.

Олжас Сатиев,
основатель TSARKA GROUP

Пентест имеет решающее значение для превентивного выявления уязвимостей. Но есть важное но: структурированный подход от разведки до анализа выявляет слабые места, которые автоматизированные инструменты могут не заметить. Однако, если компания не строит пентест как итеративный процесс, а проводит его исключительно как разовое мероприятие, меры безопасности никогда не будут достаточными для меняющегося ландшафта угроз.

Как пентест соответствует целям бизнеса?

Основные цели тестирования на проникновение - выявление недостатков безопасности, измерение эффективности существующих средств защиты и обеспечение готовности организации реагировать на инциденты.

Отраслевые игроки, задающие стандарт качества такого сервиса в РК, нацеливают пентесты на несколько уровней ИТ-среды, таких как

- сетевая инфраструктура
- веб - и мобильные приложения
- средства контроля физической безопасности
- роль человеческого фактора в безопасности организации

Однако, весь 2024 год на рынке появлялись игроки, использующие доступность автоматизированных инструментов (в том числе опенсорс) для легкого входа в индустрию. И хотя это способствует популярности инструмента защиты – но стандартам качества и ожиданиям серьезного бизнеса уже не соответствует.

Бизнесу рекомендуется детальная оценка квалификации пентестеров, к примеру, способность методов проникновения на основе полученных результатов по мере их продвижения, проверка в ручном режиме сценариев кибератак, которые автоматизированные инструменты могут упустить из виду. Этот более детальный подход предлагает более глубокое понимание общего состояния безопасности организации, позволяя руководителям расставлять приоритеты и активно устранять наиболее важные угрозы.

Цифровые продукты и инфраструктура поддержки: что поможет обеспечить стабильность бизнеса?

Любое веб-представительство цифрового продукта давно уже выходит за рамки эстетики и функциональности. Защита веб-сайта от киберугроз и обеспечение беспрепятственного взаимодействия с пользователем - жизненно важный аспект коммерческого функционала инфраструктуры цифрового продукта.

Интернет-среда стала мишенью для хакеров и злоумышленников, стремящихся использовать уязвимости веб-сайтов. Компании, предлагающие дизайн веб-сайтов, далеко не всегда уделяют первоочередное внимание безопасности для защиты конфиденциальных данных. Киберугрозы, включая утечку данных, вредоносное ПО и фишинговые атаки, могут поставить под угрозу информацию клиентов и нарушить бизнес-операции. Малые и средние предприятия особенно уязвимы, поскольку им часто не хватает надежных мер безопасности – их цифровые представительства делаются на бесплатных движках или онлайн-сервисах, часто не обновляющихся и не учитывающих всю палитру современных угроз;

Неочевидный для тех сотен компаний, что полегли в неравной борьбе за пятилетку, вывод - услуги по безопасной веб-разработке чрезвычайно необходимы компаниям, стремящимся защитить свои данные, клиентов и репутацию. Найти веб-дизайнера на рынке РК можно за пару минут, найти надежного поставщика промышленного веб-дизайна – за пару недель. А что с безопасностью?

Евгений Питолин
Управляющий директор DataStar

Инвестиции в безопасную веб-разработку снижают эти риски за счет внедрения надежных протоколов безопасности с нуля. Такой упреждающий подход гарантирует, что предприятия смогут защитить свои цифровые активы и сохранить доверие клиентов. Безопасный веб-сайт нужно строить на нескольких уровнях защиты, и от архитектуры, плана и начальных этапов разработки до финального сервисного обслуживания безопасность должна быть приоритетом.

Какие фундаментальные принципы способствуют хорошо защищенному веб-сайту:

1. Практика безопасной разработки(devsecops)

ДевСекОпс гарантирует, что разработчики пишут kol без уязвимостей, которыми могут воспользоваться хакеры. Это включает в себя очистку вводимых пользователем данных, предотвращение SQL-инъекций и реализацию протоколов аутентификации. Следуя передовым практикам, разработчики снижают вероятность появления лазеек в системе безопасности, которыми можно воспользоваться в дальнейшем.

2. Сертификация SSL и шифрование данных.

Сертификат SSL (Secure Sockets Layer) шифрует данные, которыми обмениваются сайт и его пользователи, защищая конфиденциальную информацию, такую как пароли и данные кредитной карты. Без SSL-шифрования браузеры помечают сайты как «небезопасные», что снижает надежность и доверие клиентов. Внедрение шифрования имеет важное значение для безопасной веб-разработки.

3. Регулярные проверки безопасности и обновления.

Веб-безопасность — это не одноразовая задача. Хакеры постоянно разрабатывают новые методы использования уязвимостей, поэтому регулярные проверки безопасности необходимы. Частые обновления плагинов сайта и основной структуры веб-сайта помогают исправить недостатки безопасности до того, как они станут проблемой. Проведение оценок уязвимостей гарантирует, что веб-сайт останется защищенным от возникающих угроз.

4. Строгая аутентификация пользователя

Реализация многофакторной аутентификации (MFA) добавляет дополнительный уровень безопасности, требуя нескольких этапов проверки для входа пользователей. Применение политики надежных паролей и ограничение доступа к конфиденциальным областям дополнительно предотвращает несанкционированный доступ к веб-сайту. Механизмы аутентификации пользователей помогают предприятиям защитить как свои внутренние данные, так и информацию своих клиентов.

5. Безопасный хостинг и защита сервера

Выбор надежного хостинг-провайдера со встроенными функциями безопасности имеет решающее значение. Безопасные среды хостинга включают сканирование на наличие вредоносных программ, защиту от DdoS, встроенный WAF и решения для резервного копирования. Меры безопасности на стороне сервера, такие как контроль доступа и системы обнаружения вторжений, также помогают предотвратить несанкционированный доступ и атаки.

6. Улучшение пользовательского опыта с помощью безопасной веб-разработки

Помимо безопасности, хорошо разработанный сайт обеспечивает плавную навигацию, высокую скорость загрузки и доступность. Безопасные платформы также лучше оцениваются в поисковых системах, поскольку они отдают приоритет строгим мерам безопасности. Интеграция безопасности в разработку гарантирует визуально привлекательный, функциональный и безопасный цифровой опыт.

Учитывая растущий спрос на высокопроизводительные веб-сайты, профессиональные услуги по веб-разработке также могут помочь бизнесу оставаться конкурентоспособным. Хорошо защищенный веб-сайт повышает удобство работы пользователей, укрепляет доверие к бренду и укрепляет доверие клиентов, обеспечивая успех бизнеса.

5 важнейших стратегий, обеспечивающих безопасность бизнес-данных

IBM опубликовала ежегодный отчет о стоимости утечки данных, свидетельствующий о том, что средняя стоимость утечки данных в 2024 году достигла рекордного уровня в 4,88 млн. долларов США, что на 10% больше, чем в 2023 году, поскольку взломы становятся все более разрушительными. Еще более тревожно то, что злоумышленники теперь взламывают системы в среднем всего за 3 дня, в то время как компаниям обычно требуется более 200 дней, чтобы обнаружить эти нарушения.

А есть ли хорошие новости, спросит грустный читатель?

Пожалуй, да. Эксперты форума Cyber and Digital Security сформулировали для вас пять наиболее важных подходов, которые используют успешные организации для создания эффективной цифровой крепости вокруг своих самых ценных цифровых активов.

1. Внедрение передовых решений прокси-сервиса для безопасного удаленного доступа.

Современное рабочее место выходит далеко за рамки традиционных офисных стен. Поскольку модели удаленной и гибридной работы становятся стандартом, обеспечение доступа к конфиденциальным ресурсам компании представляет собой беспрецедентную проблему. Именно здесь сложные прокси-решения оказываются неоценимыми. Расширенные прокси-сервисы создают безопасный способ коммуникации между членами вашей команды и критически важными бизнес-системами. В отличие от базовых VPN, высокопроизводительные прокси-решения предлагают несколько явных преимуществ:

Во-первых, они создают зашифрованные туннели, которые защищают конфиденциальные данные от перехвата, что особенно важно, когда сотрудники подключаются через общедоступные сети в кафе, аэропортах или коворкингах. Это шифрование работает аналогично бронированному транспортному средству, перевозящему ценный груз: внешние наблюдатели могут видеть движение, но не могут получить доступ к тому, что находится внутри.

Во-вторых, самые быстрые на сегодняшний день прокси-сервисы поддерживают детальный контроль доступа, который ограничивает доступность данных на основе ролей пользователей, географического местоположения и профилей безопасности устройства. Это означает, что ваш финансовый аналитик в столице может получить доступ к финансовым прогнозам, будучи заблокированным для инженерных спецификаций, и одновременно предотвращая любые попытки доступа из регионов с высоким уровнем риска, где ваша компания не работает.

В-третьих, расширенные прокси-серверы обеспечивают подробную регистрацию активности, создавая контрольные журналы, которые оказываются неоценимыми во время инцидентов безопасности. Эта возможность превращает ваш прокси-сервер из простого инструмента защиты в активный интеллектуальный актив безопасности.

Организации, внедряющие выделенные прокси-решения, сообщают о на 60% меньше инцидентов безопасности, связанных с удаленным доступом, по сравнению с теми, которые полагаются исключительно на традиционные VPN.

2. Внедрение комплексного процесса проверки поставщиков (KYB).

Инфраструктура безопасности настолько сильна, насколько сильно ее самое слабое звено, и все чаще эти уязвимости возникают через отношения с третьими сторонами. Атаки в цепочке поставок, когда злоумышленники компрометируют доверенных поставщиков, чтобы получить доступ к их клиентам, за последние годы увеличились на 300%. В результате процессы проверки «Знай свой бизнес» (KYB) превратились из проверки для галочки в критически важные меры безопасности.

Эффективные процедуры KYB включают в себя:

• Тщательная первоначальная проверка потенциальных поставщиков, включая проверку сертификатов безопасности (например, SOC 2, ISO 27001), результатов тестирования на проникновение и документированных процедур реагирования на инциденты. Этот процесс напоминает проверку анкетных данных, которую проводят банки перед выдачей кредитов, включая регулярную переоценку методов обеспечения безопасности поставщиков посредством анкетирования, оценок на местах и проверки обновленной документации по безопасности. Важно установить четкие требования безопасности в контрактах с поставщиками, включая сроки уведомления о нарушениях.

• Непрерывный мониторинг доступа поставщиков, ограничение подключений только к системам и данным, необходимым для предоставления услуг, а также внедрение протоколов оперативного доступа, которые предоставляют временные разрешения при необходимости.

Олег Биль,
7 Hills of Kazakhstan

Организации с зрелыми программами KYB обнаруживают сторонние проблемы безопасности до 70% быстрее, чем организации без структурированных процессов проверки, что значительно снижает потенциальный ущерб от компрометации, связанной с поставщиками. Жаль, что пока таких организаций в РК – единицы, но мы верим в их рост.

3. Разворачивание многофакторной аутентификации во всех системах.

Несмотря на десятилетия обучения по вопросам безопасности, уязвимости, связанные с паролями, остаются удивительно распространенными. Более 80% взломов связаны с кражей или компрометацией учетных данных, что делает защиту паролем одной только крайне недостаточной. Многофакторная аутентификация (MFA) устраняет эту уязвимость, требуя дополнительной проверки помимо паролей.

Эффективная реализация MFA включает в себя:

• Требование как минимум двух факторов проверки во всех бизнес-системах, в идеале сочетание того, что знает пользователь (пароль), того, что у него есть (мобильное устройство или ключ безопасности), и того, чем он является (биометрическая проверка, например отпечатки пальцев или распознавание лиц).

• Внедрение аутентификации на основе рисков, которая корректирует требования безопасности в зависимости от контекстуальных факторов. Например, директору по маркетингу, имеющему доступ к данным кампании из своего офиса в рабочее время, может потребоваться только базовая проверка, в то время как та же попытка доступа в 3 часа ночи из незнакомого места вызовет дополнительные проверки безопасности.

• Использование устойчивых к фишингу методов аутентификации, таких как ключи безопасности FIDO2, которые проверяют легитимность веб-сайта перед передачей учетных данных, что делает их невосприимчивыми к сложным фишинговым атакам, которые могут обойти традиционный MFA.

По данным исследования безопасности Microsoft, организации, внедряющие комплексный MFA, сообщают о снижении количества инцидентов, связанных с компрометацией учетных записей, до 99,9%. Это делает MFA, возможно, наиболее эффективной мерой безопасности по сравнению со стоимостью реализации.

4. Используйте сквозное шифрование для всех передач данных.

Передаваемые данные представляют собой особую уязвимость, особенно когда информация передается между облачными средами, филиалами и удаленными работниками. Сквозное шифрование гарантирует, что даже если передача данных будет перехвачена, содержимое останется нерасшифрованным для неавторизованных сторон.

Комплексные стратегии шифрования включают в себя:

• Внедрение Transport Layer Security (TLS) 1.3 в качестве минимального стандарта для всех веб-сервисов и приложений гарантирует, что данные, передаваемые через Интернет, остаются зашифрованными.

• Использование шифрования для особо конфиденциальной информации, такой как финансовые данные, медицинские записи или интеллектуальная собственность, гарантирует, что определенные элементы данных останутся зашифрованными даже во время обработки в различных системах.

• Внедрение надежных методов управления ключами, включая регулярную ротацию ключей, безопасное хранение ключей шифрования отдельно от данных, которые они защищают, и процедуры восстановления, которые обеспечивают баланс между безопасностью и требованиями непрерывности бизнеса.

5. Проведение нового формата тренингов по безопасности - иммерсивные тренинги

Технические средства контроля обеспечивают необходимую защиту, но человеческое суждение остается и самой большой уязвимостью, и самой сильной защитой. Традиционное обучение безопасности часто терпит неудачу, поскольку оно рассматривает безопасность как абстрактную концепцию, а не практический навык.

Организации, инвестирующие в иммерсивное обучение безопасности, страдают на 70% меньше от успешных атак социальной инженерии, а их сотрудники значительно быстрее сообщают о подозрительных действиях, что кардинально сокращает время реагирования на инциденты.

Евгений Питолин
Управляющий директор DataStar

Даурен Салипов,
основатель и CEO MSSP.Global

Создайте позитивную культуру безопасности, признавая и поощряя поведение, заботящееся о безопасности, а не просто наказывая за ошибки. Такой подход превращает сотрудников из потенциальных уязвимостей в активных агентов безопасности.

Эффективные программы повышения безопасности включают в себя:

• Модели реальных атак с помощью контролируемых фишинговых упражнений, тестов социальной инженерии и оценок физической безопасности. Эти симуляции превращают безопасность из теоретических знаний в практический опыт.

• Обучение с учетом рисков, связанных с конкретной ролью, гарантируя, что руководители пройдут целенаправленное обучение по китобойным атакам (целевой фишинг ценных лиц), команды разработчиков изучат методы безопасного кодирования, а финансовый персонал пройдет специализированное обучение по попыткам финансового мошенничества.

Реализация этих пяти важнейших стратегий — передовых прокси-решений, комплексной проверки KYB, многофакторной аутентификации, сквозного шифрования и иммерсивного обучения вопросам безопасности — создает несколько уровней защиты ваших ценных бизнес-данных. Помните, что эффективная безопасность напоминает хорошо спроектированную крепость, а не одну стену. Каждый защитный уровень компенсирует потенциальные слабости других, создавая эшелонированную защиту, которая значительно улучшает общий уровень безопасности. Систематически реализуя эти стратегии, ваша организация может значительно снизить свою уязвимость к утечкам данных, демонстрируя при этом клиентам, партнерам и регулирующим органам свою приверженность защите конфиденциальной информации в современных сложных условиях угроз..

Что-то уже случилось: план реагирования на киберинциденты

Павел Жуйков,
управляющий партнер
Geos Research Group

План реагирования на киберинциденты — это простой документ (или сложный плейбук – зависит от масштаба вашей организации), который помогает команде действовать быстро и синхронно в момент атаки. Опыт показывает, что именно здесь команды чаще всего недорабатывают, теряя время на согласование действий, поиск ответственных и разрозненные решения.

План реагирования на киберинциденты состоит из следующих этапов

- Подготовка
- Выявление / Анализ происходящего
- Попытка реагирования / сдерживания
- Устранение причин
- Восстановление
- Полученные уроки

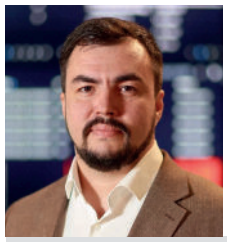
Любая организация, серьезно относящаяся к своей кибербезопасности, должна уделять приоритетное внимание разработке и поддержанию подобного плана реагирования на киберинциденты. Этот план служит важной основой для эффективного управления и смягчения последствий киберугроз и атак.

Участники форума Cyber and Digital Security поделились своими видениями о том, каким должен быть такой план:

Клим Гольцман,
ASTEL

План должен быть кратким, четким и точным.

Все заинтересованные стороны внутри компании (C-Level и подчиненные) могут быстро принимать решения и все указанные шаги. Важно: В нем не должно быть сложного жаргона, долгих схем, фокус - на конкретной ИТ-инфраструктуре вашего бизнеса, самых критических активах (ВАЖНО ОЦЕНИТЬ ЗАРАНЕЕ!) и конкретном контексте угроз.



Александр Пушкин,
руководитель SOC,
PS Cloud Services

План реагирования на киберинциденты должен быть не только всеобъемлющим, но и динамичным.

Это означает, что его необходимо регулярно тестировать с помощью киберштабных учений и обновлять по результатам учений (А Вы уже запланировали такие?). Его также следует регулярно совершенствовать, чтобы он соответствовал текущему ландшафту киберугроз в РК и Вашей отрасли. Постоянно развивая и адаптируя план реагирования на киберинциденты, вы можете повысить устойчивость своей организации к киберугрозам и защитить критически важные активы и информацию.

Но как создать этот план, из чего эффективную стратегию реагирования на кибератаки?

Давайте подробно рассмотрим каждый этап, чтобы понять, как они в совокупности способствуют устойчивости кибербезопасности.

Подготовка

Назгуль Таимова,
директор Elcore Kazakhstan

Важно утвердить права и обязанности людей в структуре компании, которые определяют эти шаги, ЗАРАНЕЕ!

Этап подготовки в структуре реагирования на инциденты в основном сосредоточен на том, как дать все права структуре (ИБ-департаменту), который согласует политику организации в отношении защиты личной информации и конфиденциальных данных с ее тактиками бизнеса и политиками безопасности персонала. Это предполагает тщательную оценку и интеграцию этих политик с существующей технологической инфраструктурой вашего бизнеса.

Этап подготовки также включает разработку четких бумажных и электронных протоколов и руководств, определяющих, как управлять конфиденциальными данными и защищать их, гарантируя, что все сотрудники знают свои роли и обязанности в обеспечении кибербезопасности. Кроме того, этот этап может включать в себя проведение регулярных учебных занятий по реагированию на киберинциденты и учений по моделированию кибератак, чтобы гарантировать, что все хорошо подготовлены к быстрым и эффективным действиям в случае киберинцидента.

Выявление / анализ

Даурен Салипов,
основатель и CEO MSSP.Global

Важно действовать быстро и решительно!

Этот этап планирования реагирования на инцидент направлен на определение того, подверглись ли вы взлому или была ли скомпрометирована какая-либо из ваших систем. В случае, если нарушение действительно обнаружено, следует сосредоточиться на ответах на такие вопросы, как:

- Кто обнаружил нарушение?
- Какова степень нарушения?
- Как это влияет на работу?

На этапе анализа вы должны оценить текущее состояние подотчетных активов, актуальные в момент атаки риски, принятые уже меры безопасности, чтобы установить базовый уровень для нормальной деятельности. Этот этап включает в себя непрерывный мониторинг в моменте, анализ угроз и оценку рисков для превентивного обнаружения аномалий. Эффективная идентификация атакуджщих группировок (Threat Intel) помогает минимизировать время реагирования и снизить потенциальный ущерб от киберугроз. На этом этапе также важно все документировать.

Сдерживание.

Олжас Сатиев,
основатель TSARKA GROUP

Важно действовать АКТИВНО
и привлекать все возможные ресурсы,
включая сторонние организации- партнеров

На этом этапе плана реагирования необходимо подумать о том, что можно сделать, чтобы сдержать последствия нарушени:

- Какие системы можно перевести в автономный режим, отключив от любого внешнего доступа? Какие системы надо изолировать?
- Какова краткосрочная и долгосрочная стратегия борьбы с последствиями нападения?
- Кто и как блокирует найденную вредоносную активность?
- Что с резервными копиями?
- Что с настройками привилегированного доступа?
- Применены ли все соответствующие обновления безопасности?

Устранение.

Клим Гольцман,
ASTEL

Важно действовать ИНТЕЛЛЕКТУАЛЬНО
И СПОКОЙНО!

Фаза устранения в плане реагирования на киберинциденты является критически важным этапом, который фокусируется на тщательном понимании основной причины нарушения и ее быстром и эффективном устранении в режиме реального времени.

Процесс реагирования на инциденты на этом этапе включает в себя ряд тщательных действий, таких как:

- Исправление уязвимостей в системе для предотвращения дальнейшей эксплуатации (апдейт прошивок, корректировка настроек)
- Удаление любого вредоносного программного обеспечения, которое могло быть установлено
- Обновление старых версий программного обеспечения, чтобы обеспечить их защиту от известных угроз.
- Детальное изучение всей ИТ-инфраструктуры для выявления любых других потенциальных уязвимостей, которые могут быть использованы в будущем.
- Сотрудничество с экспертами по кибербезопасности для внедрения передовых мер безопасности и протоколов, которые могут улучшить общий уровень безопасности организации.

Олег Биль,
7 Hills of Kazakhstan

На этом этапе необходимо сделать все необходимое, чтобы все следы вредоносного вмешательства были полностью удалены из ваших систем. Крайне важно выполнять эти действия с точностью и осторожностью, чтобы не потерять ценные данные в процессе, поскольку их целостность имеет первостепенное значение.

Восстановление. Извлеченные уроки.

Павел Жуйков,
управляющий партнер
Geos Research Group

Важно действовать УВЕРЕННО
и с упором на СТРАТЕГИЮ!

Команда должна в сжатые сроки не только устранить брешь в системе, но и обеспечить устойчивость к будущим атакам. Это не финальный шаг, а начало перехода к более зрелому уровню кибербезопасности. Решающее значение имеет то, как мы справляемся с нарушением и какие уроки извлекаем из этого.

На этом этапе крайне важно

- собрать всех членов группы реагирования (не позднее, чем через 2 недели после происшествия)
- вернуться к документации, созданной на этапе 2.
- оценить, что произошло, почему это произошло и что было сделано для сдерживания ситуации.
- обсудить, можно ли было что-то сделать по-другому. Были ли какие-либо пробелы в плане реагирования на инциденты? Был ли какой-то отдел или заинтересованная сторона, которая могла бы отреагировать быстрее или иначе?

Аналитика и прогнозы от наших экспертов. Какие действия важны для укрепления киберзащиты в 2025 году?

Генеративный ИИ в 2025 году принесет преобразующие возможности, но повысит риски кибербезопасности, включая случайное раскрытие данных и неправильное использование новых моделей ИИ.

Олжас Сатиев,
основатель TSARKA GROUP

Важно обеспечить безопасность агентов ИИ, на рабочих местах, внедрить управление данными в коллаборации с ИИ и развернуть платформы безопасности для ИИ-систем. Совместные усилия поставщиков средств безопасности, поставщиков ИИ и самих предприятий будут иметь ключевое значение для противодействия автоматизированным масштабируемым атакам на системы ИИ

Несмотря на широкое внедрение облачных технологий, большинство команд DevSecOps полагаются на локальные инструменты оповещения, что приводит к пропущенным угрозам и пустой трате ресурсов на ложные срабатывания. Чтобы уменьшить количество облачных атак, организации должны интегрировать облачные данные в режиме реального времени в SOC, обеспечивая последовательное обнаружение угроз, более быстрое реагирование и снижение рисков существенных нарушений в 2025 году и в последующий период.

В 2024 году 65% нарушений были связаны с облачными данными, что подчеркивает серьезный пробел в облачной безопасности.

Назгуль Таимова,
директор Elcore Kazakhstan

Защита в режиме реального времени и проверенный подход к обеспечению безопасности персонала имеют решающее значение для обеспечения устойчивости.

Евгений Питолин
Управляющий директор DataStar

Сложность искусственного интеллекта и злоупотребление им растут по мере снижения затрат, что приводит к всплеску мошенничества с использованием МО и атак на физические устройства. Организации сталкиваются с растущими рисками социальной инженерии на основе искусственного интеллекта и новых взломов персональных устройств. По мере снижения вычислительных затрат вырисовываются автономные операции и обнаруженные ИИ эксплойты нулевого дня. Хотя полностью вредоносное ПО с искусственным интеллектом не пришло в РК, отрасль должна подготовиться уже сейчас.

Нехватка навыков в области безопасности ИИ вызывает лично у меня растущую обеспокоенность.

Даурен Салипов,
основатель и CEO MSSP.Global

Сложность искусственного интеллекта и злоупотребление им растут по мере снижения затрат, что приводит к всплеску мошенничества с использованием МО и атак на физические устройства. Организации сталкиваются с растущими рисками социальной инженерии на основе искусственного интеллекта и новых взломов персональных устройств. По мере снижения вычислительных затрат вырисовываются автономные операции и обнаруженные ИИ эксплойты нулевого дня. Хотя полностью вредоносное ПО с искусственным интеллектом не пришло в РК, отрасль должна подготовиться уже сейчас.

В 2025 году безопасность приложений перейдет от выявления уязвимостей к интеллектуальной приоритизации и автоматизированному устранению уязвимостей.

Батыржан Шакманов,
CyberX

Это позволит разработчикам устранять критические риски в своих рабочих процессах. При более ограниченном бюджете организации будут использовать интегрированные платформы для повышения эффективности и экономичности. Традиционные инструменты, отключенные от SDLC, исчезнут, в то время как возможности искусственного интеллекта станут важными, расширяя возможности команд безопасности и защищая приложения на базе искусственного интеллекта.DevSecOps переводит безопасность с реактивного процесса на проактивные действия, внедряя ее на ранних этапах разработки. Сотрудничество между командами по кибербезопасности, разработками и бизнесом требует анализа данных и общих приоритетов. Заблаговременно устраняя векторы атак и согласовывая безопасность с бизнес-целями, организации могут повысить устойчивость и сделать кибербезопасность фундаментальным бизнес-требованием.

Alper Cem Yılmaz,
Основатель Crypttech

В 2025 году угрозы кибербезопасности будут распространяться на API, облачные настройки, цепочки поставок и блокчейн.

Эксплойты API будут нацелены на теневые API и проблем авторизации на уровне объектов (BOLA). Неправильные настройки облака в гибридных блоках инфраструктуры будут терять конфиденциальные данные. Атаки на цепочки поставок будут усиливаться из-за «отравленных» API и неконтролируемых обновлений (а точнее, их отсутствия) программного обеспечения. Для компаний в РК важно будет автоматизировать облачный мониторинг, укрепить цепочки поставок и использовать средства защиты искусственного интеллекта.

IT-директор: будущее профессии

В условиях продолжающихся утечек данных, новых векторов атак и сложных экономических условий, 2024 год сумел сильно расстроить директоров по информационной безопасности. Геополитика, искусственный интеллект, новые инструменты атак – попытки взлома становяться все более изощренными и осуществляются с большей скоростью, в куда большем масштабе, чем когда-либо прежде.

Роль CISO в понимании проблематики, в распределении прав доступа, в надзоре за рисками и митигации штрафов от регулятора выходит все чаще в топовый список вопросов на уровне совета директоров. Мировые исследования (к примеру, Исследование Datos Insights) показывает, что и бюджеты / зарплаты CISO выходят в мире на второй, а то и первый план. Это казахстанским CISO пока только снится, но инструменты киберуправления, рисков и соблюдения требований (GRC), позволяющие осуществить комплаенс и повысить качество корпоративного управления в 25 году. И даже – запустить подобные продукты на базе казахстанских разработчиков.

О чем стоило думать вчера: крупнейшие запланированные в бюджете инвестиции в киберзащиту ориентированы на 90% на он-премис инфраструктуру. Большинство компаний повышают уровень использования технологий в мультиоблачной среде, отсюда мораль -

необходимо усовершенствовать инструменты для надзора за киберрисками в облаках на уровне совета директоров «снизу», пока это решение не пришло «сверху» без комфортного коридора изменений.

О чем будут думать лидеры борьбы с киберрисками Казахстана в 2025 году?

- больше беспокоиться об использовании искусственного интеллекта
- спасать учетки клиентов через фшинг-тренинги и тестирование гна социальную инженерию
- защищать бизнес-приложения и инфраструктуру клиентского канала
- повышать выявление уровня мошенничества и уровня устойчивости потребителей.
- Определять новые векторы атак для рисков корпоративных данных