Киберугрозы существуют...

За последние годы кибератаки стали более скоординированными и продуманными. Во внимание киберпреступников попадают как учетные записи пользователей, так и целые организации и регионы Для предотвращения возможного экономического ущерба, а также урона для репутации и основной деятельности организации уже недостаточно оптимизировать работу информационных технологий. Активные шаги по повышению уровня защиты от кибератак должны предпринимать высшее руководство, юрисконсульты и советы директоров организаций.

... и их количество растет

Мировой масштаб. Индивидуальный подход к клиенту

По всему миру у нас работают более 900 сертифицированных специалистов по безопасности в области информационных систем (CISSP), 1 500 сертифицированных аудиторов информационных систем (CISA), 150 сертифицированных менеджеров информационных систем (CISM), 65 сертифицированных специалистов по защите информации (CIPP) и более 100 сертифицированных специалистов по этичному хакингу (CEH).

Подразделение «Делойта» по проведению анализа киберугроз поможет вам выбрать комплексное решение по управлению информационной безопасностью.

Благодаря индивидуальному подходу, применяемому при обнаружении киберугроз, учитывающему специфику вашего бизнеса, вы сможете с большей уверенностью прогнозировать и предотвращать случаи нарушения безопасности, а также повышать устойчивость организации к воздействию угроз и снижать уровень уязвимости к атакам киберпреступников.

Контакты

Денис Липов
Директор
Тел.: +7 (495) 787 06 00
Доб. 3071
dlipov@deloitte.ru

Анатолий Остроглазов
Старший менеджер
Тел.: +7 (495) 787 06 00
Доб. 2389
aostroglazov@deloitte.ru

deloitte.ru

Deloitte.

Защищен ли ваш бизнес?
Услуги по управлению информационной безопасностью для минимизации киберрисков

Киберугрозы — не вымысел, а реальность

В последнее время технологические составляющие становятся более сложными, а доступ к информационным технологиям растет. В связи с этим все организации как малого, так и крупного размера, ведущие свою деятельность во всех секторах экономики, сталкиваются с растущим числом киберугроз. Проведение детального анализа угроз позволит минимизировать последствия нарушений системы безопасности и защититься от операционных, финансовых и репутационных рисков.

Некоторые случаи нарушения безопасности могут привести к серьезными негативным последствиям для организации. Улучшение способности определять угрозы и реагировать на них позволяет минимизировать потери и в более сжатые сроки возвращаться в обычный режим ведения бизнеса.

Расширенный анализ уязвимостей в сфере кибербезопасности
Киберпреступники постоянно ищут новые уязвимые и слабые стороны, начиная от доступной в сети информации и заканчивая ошибками конфигурации и пробелами в осведомленности сотрудников, которые приводят к незащищенности данных. Проведите тестирование сетевых ресурсов на уязвимость и повысьте уровень безопасности, используя решения «Делойта» по проведению диагностики кибератак и самые современные методы тестирования приложений и сетей на возможность вторжения.

Предотвращение потери данных и внутренних угроз
Специалисты подразделения «Делойта» по проведению анализа киберугроз помогут вам выявить внутренние угрозы и угрозы в отношении важных данных организации. Современное технологическое обеспечение для выявления угроз, а также мировой опыт в области информационной безопасности позволяют нам представить комплексное решение по управлению внутренними киберрисками.

Результат:

- Внедрение процессов предотвращения кибератак
- Устранение известных уязвимостей в корпоративной сети
- Повышение уровня осведомленности пользователей об информационной безопасности
- Усиление внутреннего контроля над информационной безопасностью в организации

Анализ рисков и оценка текущих угроз	Построение программы по предотвращению угроз	Внедрение процессов противодействия киберугрозам	Контроль за эффективностью мер информационной безопасности
• Анализ бизнес-процессов и процессов управления информационной безопасностью • Построение карты киберугроз в организации • Проведение оценки уязвимостей компонентов сети и систем	• Описание мероприятий по противодействию киберугрозам • Выбор оптимального решения и приоритизация устранения недостатков информационной безопасности • Согласование плана проведения мероприятий	• Внедрение мероприятий, контрольных процедур в бизнес-процессы организации • Написание регламентирующих документов	• Проведение тестирования контрольных процедур по информационной безопасности • Проведение обучающих семинаров и разработка программы по повышению осведомленности сотрудников в области информационной безопасности

Услуги, которые мы оказываем

Управление информационной безопасностью:
- разработка стратегии;
- проведение аудита на соответствие стандартам и нормам законодательства (ISO 270001, СТО БР, 382-П и т. д.);
- разработка политик/регламентов;
- проведение тренингов и повышение осведомленности сотрудников.

Тестирование информационной безопасности (анализ уязвимостей, тестирование на проникновение, OWASP TOP10):
- тестирование безопасности инфраструктуры;
- тестирование настроек безопасности и настроек сетевого оборудования;
- тестирование исходного кода веб-приложений;
- тестирование безопасности веб-приложений;
- тестирование безопасности Wi-Fi;
- тестирование настроек конфигураций управления мобильными устройствами (Mobile device management);
- тестирование мобильных приложений (Android, iOS);
- тестирование физической безопасности;
- социальная инженерия (фишинг);
- тестирование парольных настроек.

Управление уязвимостями:
- анализ угроз информационной безопасности, оценка и оптимизация процессов и контрольных процедур кибербезопасности, в том числе обнаружение угроз, оценка рисков, устранение уязвимостей и построение эффективного внутреннего взаимодействия.

Процесс управления доступом и учетными записями (Identity& Access management):
- создание единого и актуального каталога персональной информации пользователей в привязке к учетным записям;
- тестирование процессов управления доступом;
- анализ и оптимизация процессов аутентификации и идентификации пользователей в системах.

Проведение финансовых расследований в сфере безопасности и анализ причин случаев нарушения информационной безопасности:
- проведение расследований причин кибератак, выявление фактов, указывающих на сговор, передачу критичной информации третьим лицам, способствующей подготовке и проведению кибератак; разработка рекомендаций по дальнейшему управлению киберугрозами;
- проведение расследований инцидентов кибербезопасности, выяснение причин и обеспечение неповторения инцидентов после принятия ответных мер и ликвидации ущерба. Анализ основных причин может охватывать не только сами случаи нарушения безопасности, но и ошибки в процессах и управлении, не позволившие предупредить такие случаи;
- анализ финансовых транзакций на предмет выявления подозрительных операций, а также сфальсифицированных платежных поручений;
- проведение аудита, выявление признаков и фактов нарушения законодательства в области противодействия отмыванию доходов и финансированию терроризма.