Расследование киберпреступлений

расследование и предотвращение киберпреступлений в режиме 24/7

Широкое распространение и внедрение компьютеров во все сферы жизни общества привело к тому, что изменился сам характер многих преступлений, появились их новые виды. Преступные группы и сообщества также начали активно использовать в своей деятельности новые информационные технологии. Для достижения, прежде всего, корыстных целей преступники стали активно применять компьютеры и специальную технику, создавать системы конспирации и скрытой связи в рамках системного подхода при планирования своих действий. Одновременно наблюдается резкое нарастание криминального профессионализма - количества дерзких по замыслу и квалифицированных по исполнению преступлений.

Регулярно на современном рынке компании подвергаются кибератакам. С ростом уровня информатизации бизнеса многократно увеличивается уровень возможных финансовых потерь и рисков, а для киберпреступников растет привлекательность получения противозаконного заработка.

Ключевым фактором стремительной эволюции и развития преступности в области высоких технологий является слабая юридическая база в сфере квалификации действий и преследования хакеров в правовом поле. Это приводит к ощущению безнаказанности для «виртуальных» мошенников. Из-за неразвитой правоприменительной практики в области расследования преступлений ИБ такие инциденты зачастую предпочитают скрывать, что дополнительно стимулирует активность киберпреступников.

Основываясь на большом опыте разбора, реагирования и предотвращения инцидентов в области информационной безопасности, имея штат высококвалифицированных специалистов, мы готовы предложить комплекс услуг по расследованию киберпреступлений.

Основные этапы расследования компьютерных преступлений

- Установление факта неправомерного доступа к информации в компьютерной системе или сети;
- Установление места несанкционированного проникновения в компьютерную систему или сеть;
- Установление времени совершения преступления;
- Установление надежности средств защиты компьютерной информации;
- Установление способа несанкционированного доступа;
- Установление лиц, совершивших неправомерный доступ, их виновности и мотивов преступления;
- Сбор доказательной базы;
- Выявление обстоятельств, способствовавших преступлению;
- Установление вредных последствий преступления;
- Разработка и предоставление рекомендаций по минимизации рисков.

Состав услуги

- Срочная круглосуточная консультация ведущих специалистов;
- Оперативные меры реагирования на инцидент информационной безопасности;
- Устранение критичных уязвимостей;
- Восстановление затронутых в инциденте бизнес-процессов;
- Разработка и внедрение плана по расследованию инцидента;
- Описание наиболее вероятных механизмов и сценариев атаки;
- Оформление цифровых свидетельств и экспертных заключений, которые могут потребоваться при обращении клиента в правоохранительные органы;
- Рекомендации по улучшению мер защиты информации;
- Предоставление детального отчета;
- Разработка политик и процедур реагирования на инциденты ИБ;
- Обучение персонала процедурам реагирования на инциденты ИБ;
- Внедрение систем мониторинга и активного противодействия.

Преимущества сотрудничества

- Оперативное реагирование (свершившийся инцидент ИБ, попытка осуществления инцидента ИБ, подозрение на инцидент ИБ);
- Обширный опыт наших сотрудников в вопросах обеспечения ИБ, как с точки зрения атакующей стороны (отдел анализа защищенности), так и с точки зрения защиты (отдел разработки систем обеспечения ИБ);
- Обучение персонала применению принципов безопасной работы с информационными системами, а также оперативному реагированию на инциденты, повышение осведомленности в вопросах обеспечения ИБ;
- Снижение количества корпоративных рисков, связанных с инцидентами ИБ.