Dr.WEB®
с 1992 года

У вас - компьютерный инцидент.

Что делать и куда бежать?

www.антивирус.рф
www.drweb.ru

Dr.WEB®
Сделано в России

ЗАЩИТИ СОЗДАННОЕ

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ВКИ
(вирусозависимые компьютерные инциденты)

	ГИС/МИС	КИИ*	ГОСТАЙНА
Лишение свободы	5-10 лет	2-10 лет	До 3 лет
Лишение права занимать определенные должности или заниматься определенной деятельностью	✓	✓	✓
Статья УК РФ	**274.1**		**284**

** Любая ГИС — объект КИИ.*

Ответственность установлена для юридических лиц. ИП приравнены к юрлицам.

 www.drweb.ru | антивирус.рф

Dr.WEB®
с 1992 года

«Накажут» и рублем

Июль 2020 — Garmin — $10 млн.

Июль 2020 — Carlson Wagonlit Travel — $4,5 млн.

Это только суммы выкупа. Величину производственных и репутационных потерь знают только пострадавшие.

Что бьет по бизнесу больней: простой или утечка данных клиентов?

Dr.WEB®
с 1992 года

Прежде чем говорить о процедурах реагирования на инциденты КИ

Проблема № 1

Факт инцидента нужно заметить
(именно заметить, а не установить –
это важное отличие)

Dr.WEB®
с 1992 года

- Используются ли у вас автоматизированные системы, позволяющие выявлять инциденты?

  Современные вредоносные программы рассчитаны на незаметную работу.

- Определена ли у вас процедура, позволяющая оперативно реагировать на инциденты?

  Администратор может быть в отпуске или на обеде, телефон безопасника может разрядиться, а время-то идет.

Проблема №2

Как отличить обычный инцидент безопасности от компьютерного преступления?

Вирус может попасть случайно или в результате целенаправленной атаки, и действия, которые нужно предпринять в этих случаях, – совершенно разные…

Dr.WEB®
с 1992 года

«В результате вирусной атаки часть моих данных была заархивирована и запаролена».

Как вы думаете, какова причина инцидента?

Dr.WEB®
с 1992 года

«Вероятнее всего произошел несанкционированный вход через подбор/похищение пароля одной из учетных записей, по RDP (или через терминальную сессию). Злоумышленник запустил легальную программу для сжатия данных, добавил данные в архивы, вручную был введен пароль на архив из длинной последовательности символов».

Результат анализа инцидента специалистами «Доктор Веб»

Dr.WEB®
с 1992 года

Готовы ли ваши сотрудники
в любой момент решить,
что нечто, замеченное вами, –
именно инцидент,
требующий расследования?

Dr.WEB®
с 1992 года

Умеют ли ваши сотрудники:

- идентифицировать и собирать данные, которые могут **исчезнуть** в короткий промежуток времени - временные файлы, cookies…;
- анализировать **сетевые подключения** и активность системы на предмет аномалий;
- анализировать **процессы**;
- анализировать **память**, что также важно для расследования – память большая, а вредоносные данные невелики и легко теряются в шестнадцатеричном дампе.

И это не все места, где прячутся улики!

Dr.WEB®
с 1992 года

Важно определить:

- когда началась атака

В **марте 2019 года** в компанию «Доктор Веб» обратился клиент из государственного учреждения Республики Казахстан по вопросу наличия вредоносного ПО на одном из компьютеров корпоративной сети. Это обращение послужило поводом к началу расследования… в ходе которого было установлено, что сетевая инфраструктура учреждения была скомпрометирована как минимум с **декабря 2017 года**. https://news.drweb.ru/show/?i=13907&c=0&p=0

Dr.WEB®
с 1992 года

Важно определить:

- через какую систему произошло вторжение
- какое программное обеспечение использовалось

Весной 2019 года в службу технической поддержки «Доктор Веб» обратился корпоративный клиент с жалобой на проблемы в работе сервера.
Нагрузка на вычислительные мощности была очень высокой и возникала словно из ниоткуда.

Как вы думаете, какова причина инцидента?

Dr.WEB®
с 1992 года

Выяснив, какое ПО связано с активностью трояна,
мы обратились к его разработчику, который передал нам для анализа НЖМД **руководителя** (!) своей разработки.

Именно там мы нашли исходники эксплойтов
(ПО, использующего уязвимости
в легальных программах во вредоносных целях).
Заражение начиналось с RCE-уязвимости
в легальном продукте.
https://antifraud.drweb.ru/expertise/examples/legal_program_as_a_channel_for_penetration/

Важно определить:

- в какой последовательности совершалась атака;
- какая именно система пострадала в результате инцидента;
- какой именно сервис был скомпрометирован;
- какие именно данные были скомпрометированы;
- какова была конечная цель атаки.

Dr.WEB®
с 1992 года

Проблема №3

Отсутствие опыта сбора доказательств вредит

- Системные администраторы, не осознавая **необходимости** процедур, **требующихся** для привлечения к ответственности виновников инцидента, хотят максимально быстро устранить уязвимость в системе.

Ваш системный администратор знает процедуру реагирования на КИ?
Он соблюдает ее неукоснительно?
У вас есть такая процедура?☺

Dr.WEB®
с 1992 года

Сформирован ли список адресатов тревожных звонков?

Знают ли ваши сотрудники, в какую компанию следует обращаться при возникновении инцидентов **разных типов**?

«*Несанкционированный вход в компьютер с удалением ВАЖНОЙ ИНФОРМАЦИИ – файлов 10 Гб*»

Как вы думаете, какова причина инцидента?

Dr.WEB®
с 1992 года

«Проблема с жестким диском или файловой подсистемой».

Результат анализа инцидента специалистами «Доктор Веб»

Почему клиент обратился в антивирусную компанию и потерял время?

Dr.WEB®
с 1992 года

Определите подразделения, которые, возможно, будут участвовать в реагировании на инциденты:

- Менеджмент
- Подразделение информационной безопасности
- IT-подразделение
- Юридический отдел
- PR-служба
- Отдел кадров
- Управление непрерывностью бизнеса
- Подразделения физической и объектовой безопасности

NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide

Ваши сотрудники знают, как обязаны действовать?
Каковы их задачи и способы их решения?

Dr.WEB®
с 1992 года

Внешними сторонами, с которыми может возникнуть необходимость взаимодействия, могут быть:

- СМИ
- Интернет/сервис-провайдер
- Надзорные органы
- Поставщики ПО и услуг
- Пользователи
- и др.

NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide

Ваши сопрудники знают контактные данные профильных подразделений в этих организациях?

Dr.WEB®
с 1992 года

Коммуникации членов команды реагирования на инциденты

- **Контактная информация** для членов команды и других сотрудников внутри и за пределами организации.
- **Информация по эскалации** инцидентов.
- **Механизм отчетности** по инциденту (например, номера телефонов, адреса электронной почты, онлайн-формы и системы мгновенного обмена сообщениями, которые пользователи могут использовать для сообщения о предполагаемых инцидентах; по крайней мере один механизм должен позволять людям сообщать о таких случаях анонимно).
- **Система управления проблемами** для отслеживания информации об инцидентах, их статусе и т. д.
- **Смартфоны** для членов команды для связи как в рабочее, так и нерабочее время.

NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide

Dr.WEB®
с 1992 года

Ваши *удаленные* сотрудники знают,
у кого они **обязаны запросить помощь**
в случае компьютерного инцидента?

Dr.WEB®
с 1992 года

Ерундовый вопрос?
А если директор в отпуске?

Статья 144 Уголовно-процессуального кодекса РФ отводит на т. н. доследственную проверку 10 дней с момента подачи заявления.
Статья 145 УПК разрешает следователю принять решение об отказе в возбуждении уголовного дела или о направлении материалов проверки по подследственности.

Dr.WEB®
с 1992 года

Крайне важно определить, кто будет заниматься первичным анализом инцидента.

Правоохранительные органы зачастую не обладают опытом проведения расследования компьютерных преступлений, не имеют необходимого оборудования, опытных специалистов в области анализа компьютерных данных (или их необходимого количества) – в результате даже явного преступления для осуждения преступника не хватает доказательств.

Необходимо заранее озаботиться поиском контактов нужных специалистов и компаний, специализирующихся на расследованиях и экспертизе КИ.

Dr.WEB®
с 1992 года

- Сотрудник службы информационной безопасности не может постоянно отслеживать правовые решения по компьютерным преступлениям, от которых зависит, как именно необходимо настроить систему журналирования в ИС и выстроить процедуру реагирования на инциденты ИБ, отвечающие реальной проблематике и обеспечивающие правовой сбор доказательств.
- Для проведения расследования требуется специальное оборудование и программное обеспечение.
- Расследование инцидента информационной безопасности может занимать несколько месяцев – сотрудник, проводящий расследование, будет оторван от текущей работы.
- Если инцидент произошел по вине службы информационной безопасности, то стоит ли ждать объективной оценки происходящего?
- Служба безопасности не может расследовать внешние инциденты.

Dr.WEB®
с 1992 года

А у вас есть юрист, разбирающийся в тонкостях уголовного права?

Dr.WEB®
с 1992 года

Система расследования инцидентов безопасности (а расследование компьютерных преступлений является частным случаем расследования инцидентов ИБ) — неотъемлемая часть системы информационной безопасности компании.
И этого, кстати, требуют многие стандарты.

Без наличия постоянно действующих систем аудита и расследования инцидентов функционирование системы IT-безопасности невозможно, так как в этом случае **компания обречена** на постоянное повторение этих инцидентов.

Dr.WEB®
с 1992 года

У вас проводятся compliance-проверки (тесты на соответствие):

- ИБ-процедурам компании?
- Требованиям регуляторов?

Dr.WEB®
с 1992 года

Какие действия персонала затрудняют или делают невозможным сбор доказательств?

Типичные ошибки

Никогда и ни при каких условиях нельзя работать на скомпрометированном компьютере: он – объект исследования специалиста.

До передачи экспертам компьютер желательно даже не включать.

Допуск к компьютеру его владельца (пользователя) должен быть исключен.

Dr.WEB®
с 1992 года

Эти действия уничтожат следы злоумышленников

Если есть острая необходимость включить скомпрометированный компьютер, на нем **запрещено**:

- исполнять любые операции, не обеспечив необходимых мер защиты (например, защиты от модификации или создания резервной копии);
- производить загрузку с использованием его собственной операционной системы;
- переустанавливать операционную систему;
- удалять с диска какие-либо файлы или программы;
- обновлять антивирус или запускать сканирование. Если сканирование запущено, категорически запрещено применять действия по лечению/удалению вредоносных объектов.

Dr.WEB®
с 1992 года

- Для исключения возможности опровержения в суде идентичности предъявленного на процессе программного обеспечения тому, которое находилось на ПК на момент изъятия, компьютер, не включая, следует **опечатать в присутствии понятых**.
- До начала экспертизы необходимо снять копию с жесткого магнитного диска или иного носителя – вещественного доказательства – **с помощью спецоборудования.**

Под давлением защиты некорректно собранные электронные доказательства могут быть не приняты во внимание судом. Чтобы исключить это, необходимо строго придерживаться УПК, а также стандартизированных приемов и методик их изъятия. Это – задача специалистов.

Dr.WEB®
с 1992 года

Вы готовы к тому, что любой компьютер и любое устройство компании могут быть изъяты на экспертизу на длительный срок?

Обнаружение, осмотр и изъятие компьютеров и компьютерной информации в процессе следственных действий могут совершаться при следственном осмотре (ст. 190 КПК), при обыске (ст. 178 КПК), выемке (ст. 179 КПК), воспроизведении обстоятельств и обстановки происшествия (ст.194 КПК).

Dr.WEB®
с 1992 года

Пока все еще хорошо и спокойно, задумайтесь, что будет с вашей организацией, если:

- троянская программа зашифрует ваши базы данных, компьютер директора или бухгалтера;
- персональные данные сотрудников или клиентов будут выложены в сеть;
- содержимое конфиденциальной переписки с контрагентами попадет чужие руки;
- в результате несанкционированного доступа на компьютер бухгалтера произойдет списание с банковского счета организации крупной суммы денег;
- компьютеры вашей компании будут использованы для атаки на сайты государственных организаций;
- работа компании будет парализована в результате действий троянца?
- ……

Dr.WEB®
с 1992 года

Знают ли ваши сотрудники, что нужно делать, получив требование о выкупе зашифрованных данных?

- Кого вызывать в офис?
- Как писать заявление в компетентные органы?
- Как *правильно* снять доказательства?
- Сколько файлов нужно послать на экспертизу?
- Каких типов?
- …

Есть ли в вашей компании письменный список требований и все ли ознакомлены с ним под подпись?

Dr.WEB®
с 1992 года

Знает ли ваша компания стоимость 1 дня своего простоя?

Простоя 1 дня сотрудника?

Dr.WEB®
с 1992 года

Что может «Доктор Веб»

- **Dr.Web vxCube** — анализ файлов онлайн (песочница)
- **Dr.Web FixIt!** — утилита для удаленной **диагностики** инцидентов ИБ и у**странения их последствий.**
- Экспертиза ВКИ

Dr.WEB®
с 1992 года

А теперь о подарке