Проблемы ИБ в Архангельске и Архангельской области

Общероссийские тенденции в ИБ

- Рост атак на серверы государственных учреждений. Основная цель — компрометация данных.
- Чаще всего используется вредоносное ПО или с методы социальной инженерии.
- Вредоносное ПО как правило многофункциональное.
- Рост преступлений, связанных с хищением денежных средств с банковских карт граждан.

Общероссийские тенденции в ИБ

В 96% организаций отсутствует процесс обновления ПО

Более 70% организаций не фильтрует почту

В 80% организаций сети несегментированы

Число преступлений в сфере информационных технологий за первое полугодие 2020г. выросло на 91,7%

Хищение денежных средств с банковских карт

За период пандемии обзвонов увеличилось на **200%**

Более чем в **70%** случаев жертва сама переводит деньги злоумышленникам

В **80%** звонков используются технологии подмены телефонных номеров

Средний чек хищений в результате обзвонов составляет порядка **20 000** руб

Что было сделано организациях

В 95 % организаций установлено антивирусное ПО

В 60% организаций назначены ответственные за ИБ

Выполнены настройки ОС для снижения атак - в 40% организаций

Что не сделано организациях

Фрагментарно реализуются меры обеспечения ИБ — во ВСЕХ организациях

Отсутствие сегментации сетей — во ВСЕХ организациях

Безопасность сетевого периметра не реализуется — во ВСЕХ организациях

Неполная реализация мер обеспечения безопасности ПДн при их обработке в ИСПДн — во ВСЕХ организациях

Выявленные проблемы — уязвимости

До сих пор присутствуют:

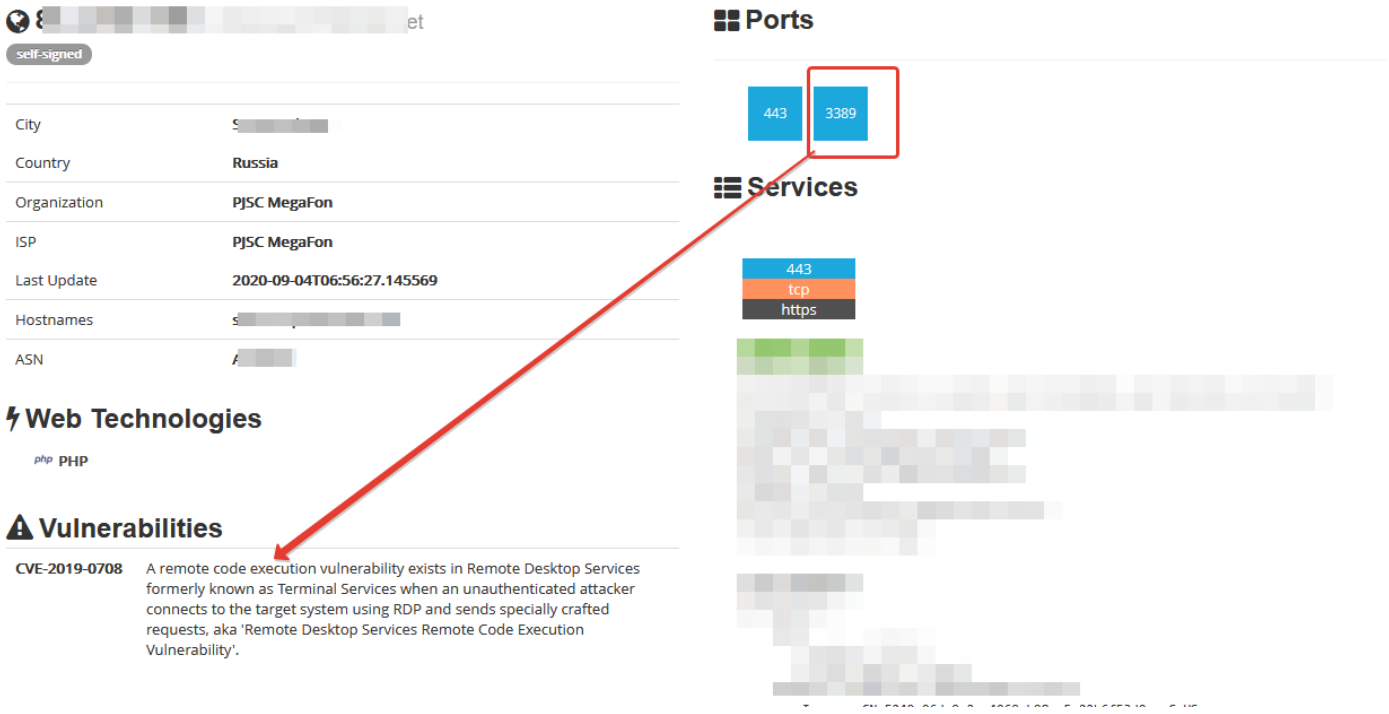
- MS17-013
- MS17-010
- CVE-2017-11882

Офисные пакеты не настроены — во ВСЕХ организациях.

Устаревшее ПО — во ВСЕХ организациях.

Уровень опасности	Найдено	Всего
Критический	30	1236
Высокий	532	3238
Средний	343	2866
Низкий	34	240
Всего	939	7580

Выявленные проблемы — уязвимости



Выявленные проблемы — сайты

Типичные уязвимости:

- Утечки идентификационных данных.
- Утечки метаданных.
- При беглом анализе - XSS, IDOR, Directory indexing

На сайтах образовательных организаций опубликованы документы, содержащие ПДн, которые потом **индексируются поисковой системой**.

Самый старый документ — от **2016 г**.

КИИ и ПДН - что реализовано в организациях

- Назначение ответственного за ЗИ.
- Проведение классификации ИСПДн.
- Обеспечение проведения процедуры получения согласия на обработку персональных данных.

Пути решения проблем

Усилить подготовку профильных специалистов ИБ.

Внедрять процедуры обеспечения ИБ как комплексного процесса, привязанного к обеспечению безопасности персональных данных.