www.deletron.ru

КИБЕРБЕЗОПАСНОСТЬ СИСТЕМ TCO

Вызовы информационной безопасности
в сегменте технических средств охраны

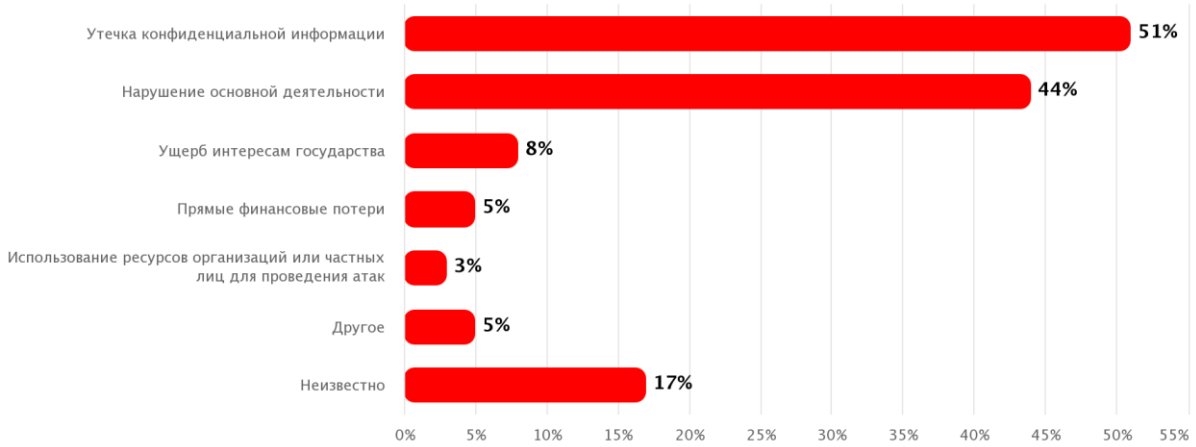
DELETRON®

ТРЕНДЫ В КИБЕРАТАКАХ 1/2

DELETRON

КОЛИЧЕСТВО УСПЕШНЫХ КИБЕРАТАК НА ОРГАНИЗАЦИИ

УЩЕРБ И ПОСЛЕДСТВИЯ КИБЕРАТАК



ПОСЛЕДСТВИЯ КИБЕРАТАК (МИР)

$2,8 млн
средний финансовый ущерб от кибератак в промышленности

РЕЗОНАНСНЫЕ ИНЦИДЕНТЫ ИБ 2024 В РФ

CDEK

Остановка работы на 5 дней.
Ущерб до 1 млрд руб.

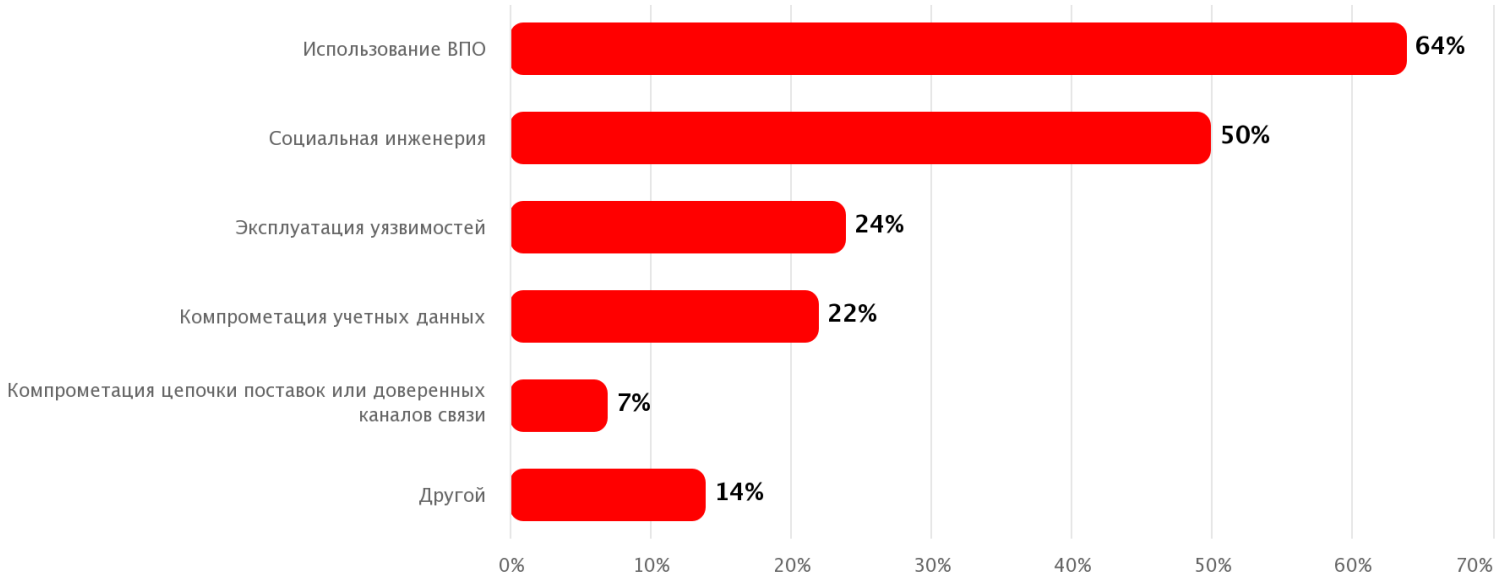
Верный универсам

Остановка работы на 3 дня.
Потери около 660 млн руб.

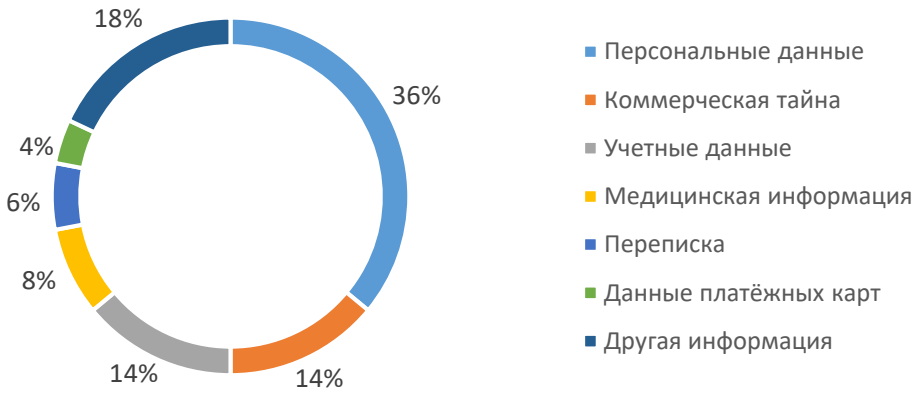
ТРЕНДЫ В КИБЕРАТАКАХ 2/2

DELETRON

КАК АТАКУЮТ?



ОСНОВНЫЕ ЦЕЛИ АТАК

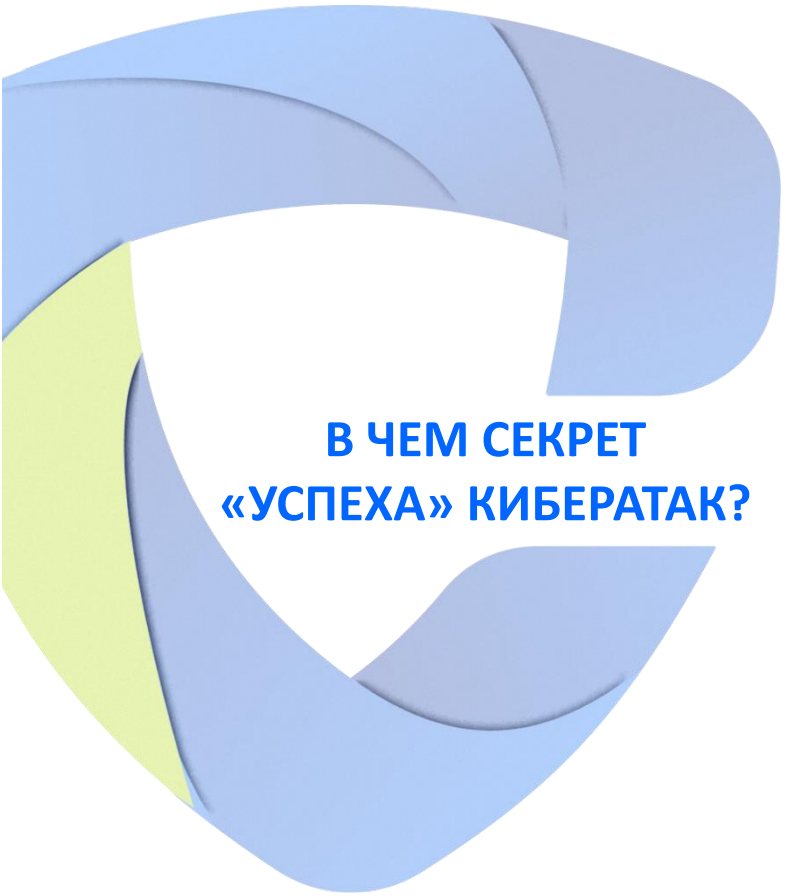


86% атак

с использованием социальной инженерии проводятся по электронной почте

Мессенджеры выходят на сцену

Распространение практики решения рабочих вопросов в общедоступных мессенджерах привело к резкому росту интереса злоумышленников к данному инструменту



В ЧЕМ СЕКРЕТ «УСПЕХА» КИБЕРАТАК?

- Проникновение «цифры» в «каждый дом»
- Простота реализации и доступность инструментов
- Эффективность социальной инженерия
- Непонимание ситуации и последствий
- Анонимность атакующих и чувство безнаказанности
- Несоблюдение цифровой гигиены

Более 50% успешных кибератак на организации происходят с «помощью» самих сотрудников

ПРОЯВЛЕНИЯ СОЦИНЖЕНЕРИИ В ПРОЦЕССАХ РЕЖИМА И ОХРАНЫ

DELETRON

01 Притворство «своим»
притвориться сотрудником или подрядчиком

02 Дружелюбие и общительность
проявить дружелюбие и завести беседу

03 Использование срочности или экстренной ситуации
создание ощущения неотложности или аварийной ситуации

04 Подмена личности
злоумышленник притворяется знакомым компании, кем-то, кого сотрудники могут знать и ожидать увидеть

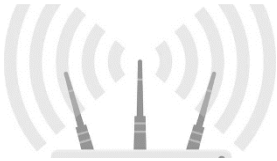
05 Создание доверительных отношений (повторные появления)
стать "своим" для сотрудников и охраны, чтобы впоследствии проникнуть в здание без проверок

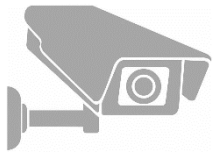
06 Следование за сотрудником
следовать за настоящим сотрудником, который открывает дверь с помощью пропуска или карты доступа

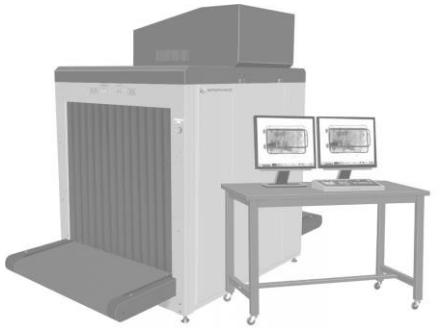
07 Ложное предложение помощи
социальный инженер может предложить свою помощь сотруднику компании, чтобы проникнуть в здание

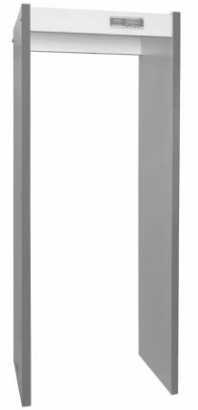
«ЗООПАРК» В ТСО

DELETRON

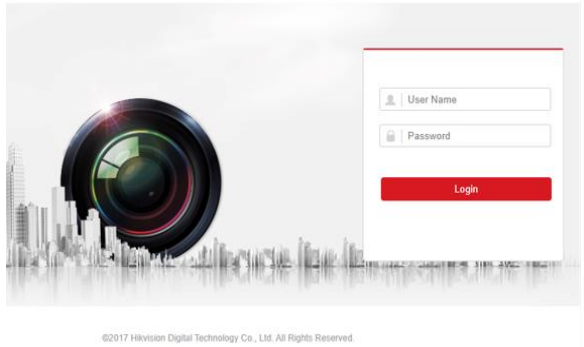








ВОЗМОЖНЫЕ ТОЧКИ ПРОНИКНОВЕНИЯ В СЕГМЕНТ ТСО



Пароли по умолчанию

Уязвимости в прошивках

Модификация прошивки

Перехват управления устройствами через интернет

КЕЙС - ИНСТРУМЕНТАЛЬНОЕ СКАНИРОВАНИЕ СЕГМЕНТА ТСО

DELETRON

4410
камер и серверов

TRASSIR HIKVISION LTV RVi

Количество обнаруженных уязвимостей по уровню критичности:

Критический	Высокий	Средний	Низкий
2	1	1	391

Уровень	Уязвимость	CVE	Описание	Рекомендации
Критический	Множественные уязвимости переполнения буфера в libupnp	CVE-2012-5958 CVE-2012-5959 CVE-2012-5960 CVE-2012-5961 CVE-2012-5962 CVE-2012-5963 CVE-2012-5964 CVE-2012-5965	Устаревшая версия libupnp подвержена множественным уязвимостям, позволяющим осуществить: - внедрение команд; - выполнение произвольного ко	Обновить до версии 1.6.21 или более актуальной.
Критический	Учетные данные по умолчанию		Возможно подключиться к устройству, используя учетные данные по умолчанию. Логин: "admin" Пароль: "12345"	Изменить пароль по умолчанию на устойчивый к взлому, в соответствии с политиками Компании.
Высокий	Уязвимости раскрытия информации на устройстве	CVE-2017-7925 CVE-2017-8229	Множественные устройства подвержены уязвимостям раскрытия информации и/или обхода пути. Уязвимый URL: http /current_config/passwd	Обновить до актуальной версии или настроить приватный доступ до уязвимого URL.
Средний	Обнаружено использование устаревшей (EoL) операционной системы		Операционная система (ОС) Ubuntu Linux 21.04, установленная на устройствах, является устаревшей (EoL) и не поддерживаемой производителем. Для таких ОС не будут выпускаться обновления, в том числе обновления безопасности.	Запланировать переход на актуальную поддерживаемую версию ОС (при наличии технической возможности). При отсутствии возможности рекомендуется усилить меры защиты, применяемые на хосте, например, использовать антивирусное программное обеспечение, ограничить доступ к хосту на сетевом уровне по белым спискам и пр.

CVE от 2012 года !!!

Directory of Video Surveillance Cybersecurity Vulnerabilities and Exploits

https://ipvm.com/reports/security-exploits

DELETRON

Обновляйте прошивки

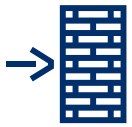
Устаревшие прошивки с большой вероятностью содержат уязвимости, которыми могут воспользоваться хакеры, чтобы перехватить управление камерой или внедриться на хранилище видеоданных.

Включайте шифрование

Шифрование трафика между камерой и сервером защищает от MiTM-атак и перехвата учётных данных

Включайте OSD

Если ваши камеры не справляются с шифрованием, включите на них простановку даты и времени на видеозапись. Тогда подменить картинку станет труднее.



Не выставляйте камеры в интернет, сегментируйте сеть

Подумайте, действительно ли вам требуется доступ к камерам видеонаблюдения через интернет. Если нет — пусть работают внутри локальной сети.

Фильтруйте IP-адреса

Ограничьте диапазон адресов, с которых можно подключиться к вашей системе видеонаблюдения. «Белые» списки и ACL ограничат свободу действий для злоумышленников.

Измените пароли по умолчанию

Пусть это будет первым действием при установке новых камер или монтаже системы.

Включите обязательную авторизацию

Даже если кажется, что на этапе настройки отсутствие авторизации упростит работу, включите её сразу.

Сканируйте на уязвимости

Периодическое сканирование сегментов на уязвимости позволит снизить риски атак

Повышайте осведомленность

Обучайте сотрудников, повышайте их киберкультуру

DELETRON

- **IP-камеры на пентестах. Используем видеокамеры не по назначению**

https://xakep.ru/2024/06/18/ip-cameras/

- **Более тысячи моделей IP-камер подвержены root-уязвимости**

https://www.opennet.ru/opennews/art.shtml?num=46175

- **Хакеры легко взламывают современные охранные системы**

http://kb-sb.ru/pub/19/773/

- **Бревно в глазу: какие уязвимости есть у систем видеонаблюдения**

https://habr.com/ru/companies/trendmicro/articles/465513/

- **Исследователь продемонстрировал удаленный взлом сигнализации SimpliSafe**

https://xakep.ru/2016/02/20/simplisafe-hack/

Спасибо за внимание !

ДЕЛЕТРОН

КОМПЛЕКСНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

+7 (499)-113-65-60

info@deletron.ru

www.deletron.ru