Проблемные вопросы комплексной безопасности информации промышленного предприятия

Директор Дирекции по экономической безопасности
АО «ДИАЙПИ», Группа ТМК
Севостьянов Александр, 2024

Кратко о ситуации

Более 600 организаций и предприятий под санкциями

Более 36 кредитных организаций в SDN листе Минфина США

Запрет экспорта на территорию РФ оборудования и компонентов: некоторые категории транзисторов, полупроводников и электронных приборов, изготовленных на их основе; оборудование для производства полупроводников; электронное оборудование для промышленности; некоторые химические элементы и электронные платы; фото- и видеотехника, включая цифровые камеры, перископы и камеры для подводной съемки; электротрансформаторы и т.д.

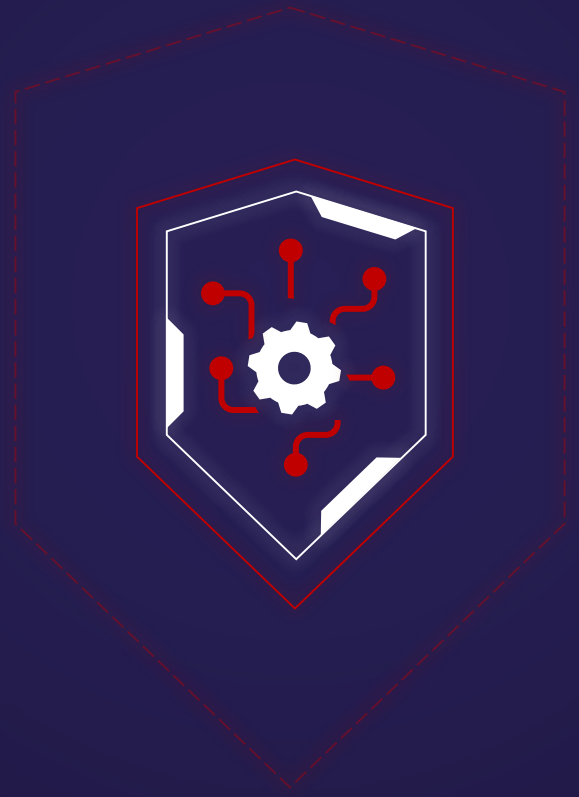
О тенденциях. 2023 год

1. Более 170 тагетированных атак на Российские Компании в день

2. Масштабные утечки данных (Компании ритейла, электронной коммерции, страхование. Более 200 млн. строк и более 200 новых БД) – !

3. Крупные атаки на приложения Microsoft

4. Увеличение доли атак шифровальщиков (более 13%)



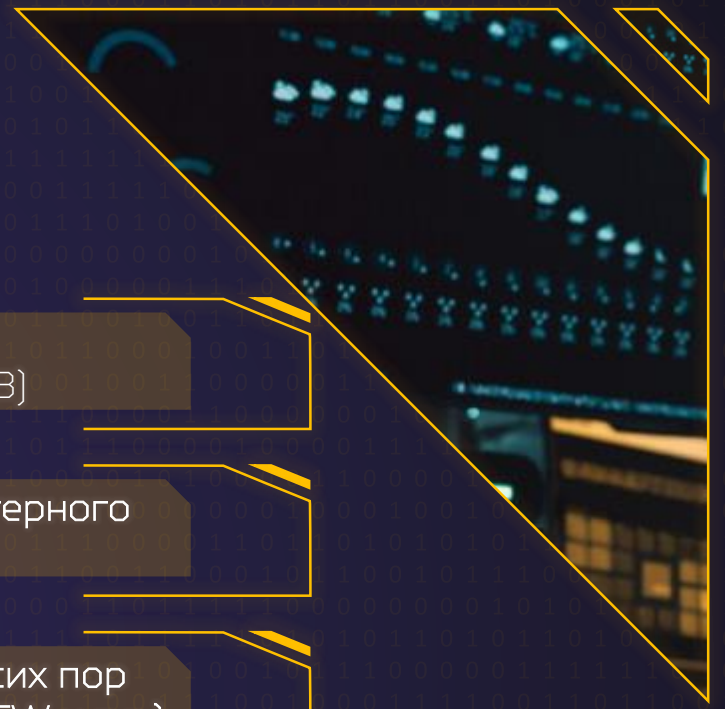
5. Концентрация атак на АРМ, сетевое и серверное оборудование

6. Масштабный фишинг, социальная инженерия на физических лиц (работников)

7. Уход с рынка иностранных решений в области КИБ

8. Атакуют специалисты спец. служб иностранных государств

ОТРАСЛЕВАЯ СПЕЦИФИКА: ПРОМЫШЛЕННОСТЬ И МЕТАЛЛУРГИЯ



- Почти все Предприятия промышленности – субъекты КИИ и операторы персональных данных (187-ФЗ, Указ Президента № 250, 152-ФЗ, 149-ФЗ)
- Значительная доля промышленного программного обеспечения, компьютерного оборудования иностранного производства
- Необходимость перехода на СЗИ и ОС отечественного производства, до сих пор уступающих иностранным аналогам по ряду классов средств защиты (NGFW и т.д.)
- Острая нехватка квалифицированного персонала в области ИБ и КИБ
- Риски параллельного импорта (экономические, информационные и правовые)
- Нахождение в состоянии «постоянно под атакой» (особенно в компаниях подсанкционных списков)

Особенности атак

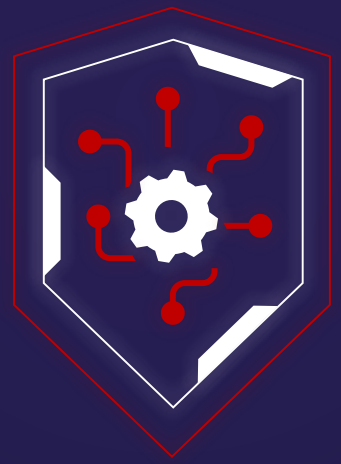
1. Атаки на операторов связи, предоставляющих услуги Предприятиям по передачи данных
2. Атаки на ЦОДы, где Предприятие может держать инфраструктуру (облака)
3. Использование внутреннего нарушителя, как источника начала атаки (подкуп привилегированных пользователей)
4. Сценарий атаки на моментальное уничтожение инфраструктуры и данных
5. Проникновение через в АСУТП через КСПД

Основные вектора атак

Основные методы атак

Шпионское ПО

- Install exe



Шифровальщики

- e-mail

ВПО для удаленного управления

- привет любителям AnyDesk

Как и от чего защититься

От чего защищаемся

- Риски нанесения ущерба АСУТП в следствии компьютерных атак через подрядчика (включая остановку производственной деятельности)

Что глобально делать

- Удаленка под контролем через PAM
- Подписание NDA
- Качественная проверка юр.лица на благонадежность;
- Проверка модели исполнения работ (удаленка; офис; локация)
- Выдача служебной техники исполнителю
- Сегментация сети
- Разделение КСПД от ПСПД

УГРОЗА

Несанкционированный доступ к ИТ-инфраструктуре по ТКС

Как и от чего защититься

От чего защищаемся

- Риски нанесения ущерба субъекту Пдн. – оборотные штрафы!
- Риски нанесения ущерба от утраты секретов производства вследствие промышленного шпионажа

УГРОЗА

Нарушение конфиденциальности информации ограниченного доступа

Что глобально делать

- Локализация критических информационных систем внутри ИТ-периметра Предприятий (ИСПДн., СУБД с НИР/НИОКР; разработка; ДБО; АСУТП), т.е. уходим из «облаков»
- Установление режима КТ согласно ст.10 98-ФЗ
- Внедрение DCAP- систем!

Как и от чего защититься

От чего защищаемся

- Нанесение ущерба работнику – то есть – риски нанесения ущерба Предприятию вследствие НСД к его данным (атака через персонал и его устройства по модели BYOD)

Что глобально делать

- Оптимизация привилегированных пользователей
- Регулярное информирование персонала
- Исключение из корп. коммуникаций иностранных мессенджеров
- Минимизация доступа к критичным данным с личных устройств, а в сегменте АСУТП – только корпоративные!
- Запрет администрирования ИС и оборудования АСУТП «из дома»

УГРОЗА

Компрометация персонала через фишинг

ТМК

Благодарю за внимание!