FINSOC

Этот offensive, offensive, offensive мир, или Смертные грехи админов

finsoc.online

whoami

Николай Беляков

В банковской сфере с 2003 года.
Руковожу московским офисом «Фродекс»
Отвечаю за развитие направлений аудита и тестирование на проникновение

FINSOC

О чём поговорим?

- Что в мире творится?
- Что у нас?
- Регулирование ИБ в финсекторе.
- Практика проведения оценок соответствия.
- Анализ защищённости (пентест).
- Мониторинг. Стоит ли строить самостоятельно?

FINSOC

А что вообще в мире делается?

- А что вообще в мире делается?

- Стабильности нет. Террористы опять захватили самолёт.

Словарь Ожегова:

Терроризм — Политика и практика террора.
Синонимами слова «террор» (лат. terror — страх, ужас) являются слова «насилие», *«запугивание», «устрашение»*.

Венесуэла

8 марта 2019 года в Венесуэле случился крупнейший блэкаут.

Министр информации Венесуэлы Хорхе Родригес утверждает, что причиной масштабного блэкаута стала **кибератака** с территории США, направленная **на автоматическую систему контроля ГЭС** "Гури".

..Врачи просто ничего не могли поделать. В кромешной тьме, нарушаемой только лучами пары фонариков и зыбким светом экранов смартфонов, медицинские работники беспомощно смотрели, как пациент умирал у них на глазах.

Еще одна проблема - сохранность продуктов и медикаментов, которые должны храниться в охлажденном виде. Чтобы сберечь еду и лекарства при неработающих холодильниках, венесуэльцы, в частности, вынуждены искать сухой лед.

Также сообщается, что по вечерам люди боятся выходить из домов на тёмные улицы.

Garmin — случай «попроще»

24 июля 2020 года отключились сервисы Garmin Connect для носимой электроники Garmin. Не работали сайт Garmin.com, колл-центр компании, онлайн-чат и даже часть производственной линии в Тайване.

Вину возложили на шифровальщик **WastedLocker**. В самой компании подтвердили факт инцидента, но не раскрыли его детали.

Злоумышленники получили сведения о геоданных клиентов Garmin, которые хранились на её серверах. Чья-то рыбацкая лодка вряд ли интересна, а вот маршруты перемещения яхт ~~замечательных людей~~ сильных мира сего, особенно факты того, что в одно и то же время их скромные суда оказались в одном и том же месте — это уже сродни разведданным.

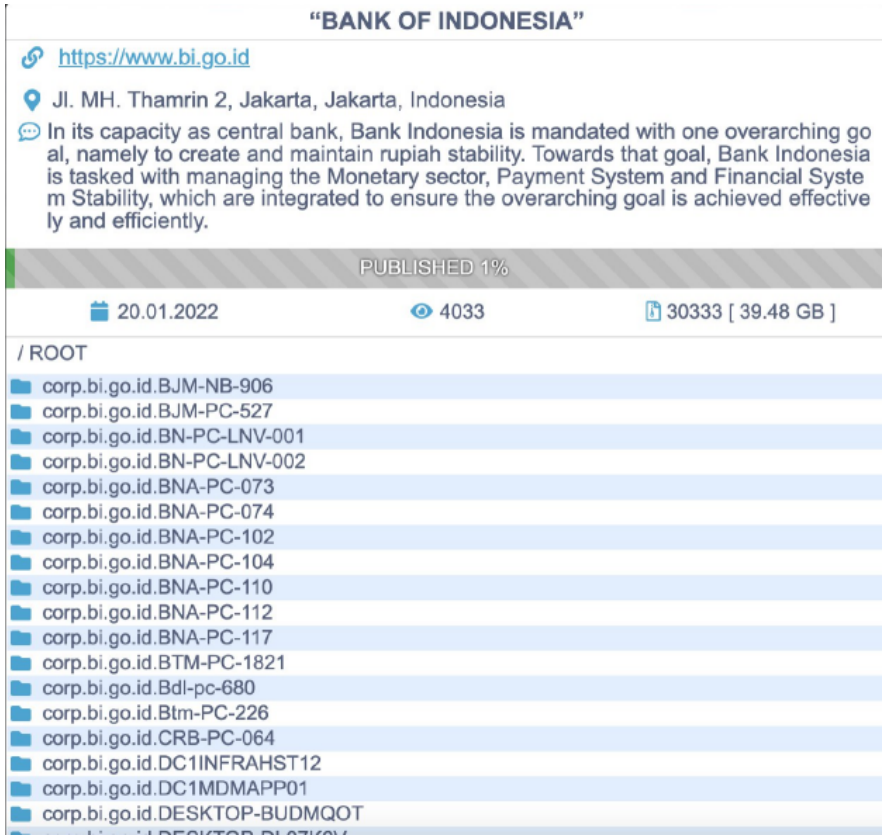
Garmin – плательщик-пионер. Этот случай открыл эру ransomware.

Что могло утечь в части военных контрактов, нам никогда не расскажут.

Банк Индонезии

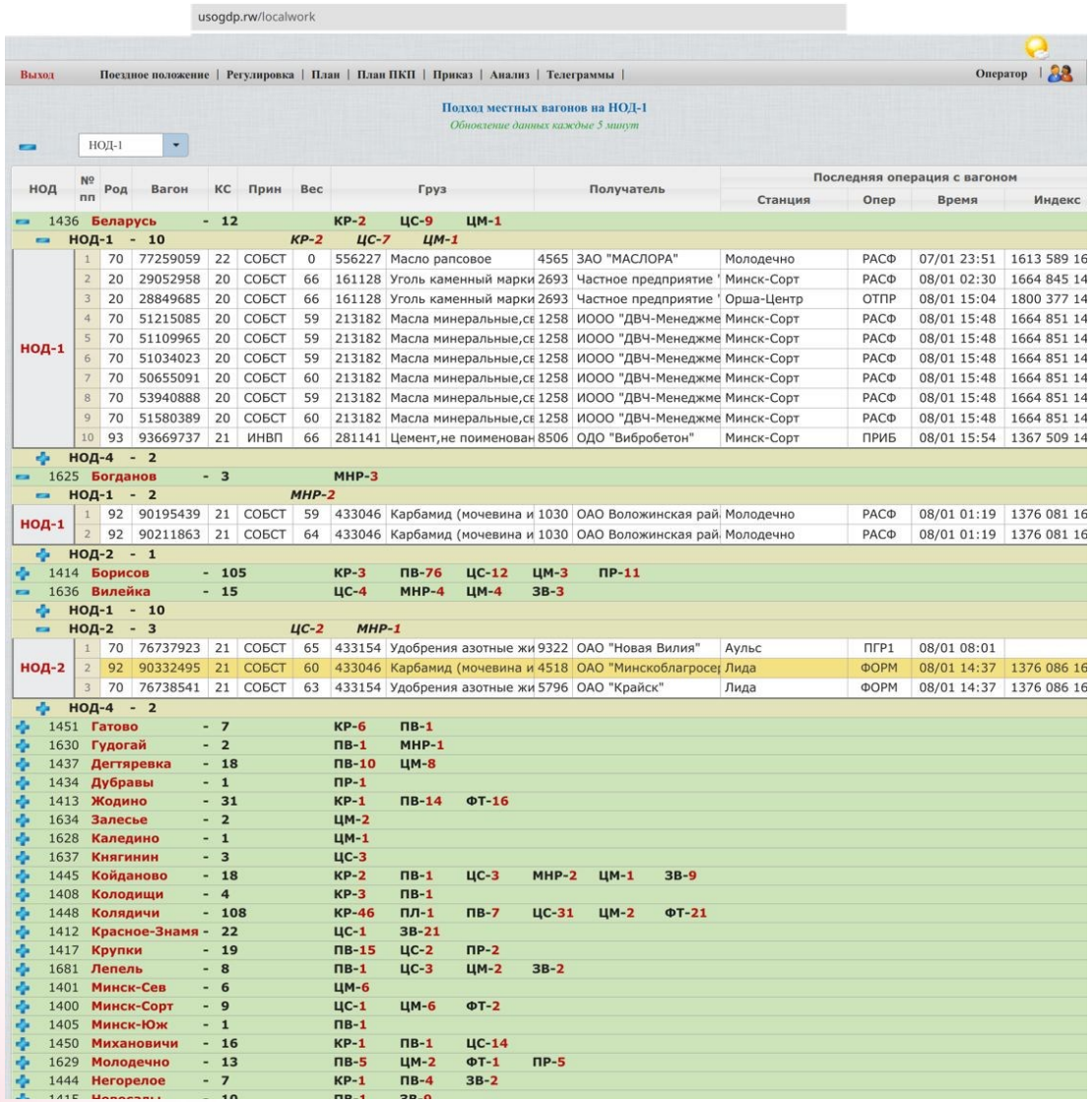
BANK INDONESIA
BANK SENTRAL REPUBLIK INDONESIA

Декабрь 2021 года.
Центральный банк Республики подтвердил декабрьский инцидент, связанный с атакой ransomware. На тот момент общественности были представлены образцы украденных файлов в качестве доказательства.



Представитель банка сообщил, что атака программы-вымогателя не повлияла на услуги, а представитель киберагентства Индонезии (BSSN) заявил, что утечки важных данных не было.
Это станет понятно, когда 39,5 ГБ или более чем 33 тысячи файлов будут на 100% вывалены в паблик. На момент добавления жертвы в DLS список включал 17 тысяч или 13,88 ГБ файлов. Похоже, что разгневанные результатами переговоров **Conti** решили увеличить объём утечки вдвое.

Восточный фронт - БелЖД



usogdp.rw/localwork

Выход | Поездное положение | Регулировка | План | План ПКП | Приказ | Анализ | Телеграммы | Оператор

Подход местных вагонов на НОД-1

Обновление данных каждые 5 минут

НОД-1

НОД	№ пп	Род	Вагон	КС	Прин	Вес	Груз		Получатель		Последняя операция с вагоном: Станция	Опер	Время	Индекс
1436 Беларусь - 12							КР-2 ЦС-9 ЦМ-1							
НОД-1 - 10							*КР-2 ЦС-7 ЦМ-1*							
НОД-1	1	70	77259059	22	СОБСТ	0	556227	Масло рапсовое	4565	ЗАО "МАСЛОРА"	Молодечно	РАСФ	07/01 23:51	1613 589 16
	2	20	29052958	20	СОБСТ	66	161128	Уголь каменный марки	2693	Частное предприятие '	Минск-Сорт	РАСФ	08/01 02:30	1664 845 14
	3	20	28849685	20	СОБСТ	66	161128	Уголь каменный марки	2693	Частное предприятие '	Орша-Центр	ОТПР	08/01 15:04	1800 377 14
	4	70	51215085	20	СОБСТ	59	213182	Масла минеральные,се	1258	ИООО "ДВЧ-Менеджме	Минск-Сорт	РАСФ	08/01 15:48	1664 851 14
	5	70	51109965	20	СОБСТ	59	213182	Масла минеральные,се	1258	ИООО "ДВЧ-Менеджме	Минск-Сорт	РАСФ	08/01 15:48	1664 851 14
	6	70	51034023	20	СОБСТ	59	213182	Масла минеральные,се	1258	ИООО "ДВЧ-Менеджме	Минск-Сорт	РАСФ	08/01 15:48	1664 851 14
	7	70	50655091	20	СОБСТ	60	213182	Масла минеральные,се	1258	ИООО "ДВЧ-Менеджме	Минск-Сорт	РАСФ	08/01 15:48	1664 851 14
	8	70	53940888	20	СОБСТ	59	213182	Масла минеральные,се	1258	ИООО "ДВЧ-Менеджме	Минск-Сорт	РАСФ	08/01 15:48	1664 851 14
	9	70	51580389	20	СОБСТ	60	213182	Масла минеральные,се	1258	ИООО "ДВЧ-Менеджме	Минск-Сорт	РАСФ	08/01 15:48	1664 851 14
	10	93	93669737	21	ИНВП	66	281141	Цемент,не поименован	8506	ОДО "Вибробетон"	Минск-Сорт	ПРИБ	08/01 15:54	1367 509 14
НОД-4 - 2														
1625 Богданов - 3							МНР-3							
НОД-1 - 2							*МНР-2*							
НОД-1	1	92	90195439	21	СОБСТ	59	433046	Карбамид (мочевина и	1030	ОАО Воложинская рай	Молодечно	РАСФ	08/01 01:19	1376 081 16
	2	92	90211863	21	СОБСТ	64	433046	Карбамид (мочевина и	1030	ОАО Воложинская рай	Молодечно	РАСФ	08/01 01:19	1376 081 16
НОД-2 - 1														
1414 Борисов - 105							КР-3 ПВ-76 ЦС-12 ЦМ-3 ПР-11							
1636 Вилейка - 15							ЦС-4 МНР-4 ЦМ-4 ЗВ-3							
НОД-1 - 10														
НОД-2 - 3							*ЦС-2 МНР-1*							
НОД-2	1	70	76737923	21	СОБСТ	65	433154	Удобрения азотные жи	9322	ОАО "Новая Вилия"	Аульс	ПГР1	08/01 08:01	
	2	92	90332495	21	СОБСТ	60	433046	Карбамид (мочевина и	4518	ОАО "Минскоблагросер	Лида	ФОРМ	08/01 14:37	1376 086 16
	3	70	76738541	21	СОБСТ	63	433154	Удобрения азотные жи	5796	ОАО "Крайск"	Лида	ФОРМ	08/01 14:37	1376 086 16
НОД-4 - 2														
1451 Гатово - 7							КР-6 ПВ-1							
1630 Гудогай - 2							ПВ-1 МНР-1							
1437 Дегтяревка - 18							ПВ-10 ЦМ-8							
1434 Дубравы - 1							ПР-1							
1413 Жодино - 31							КР-1 ПВ-14 ФТ-16							
1634 Залесье - 2							ЦМ-2							
1628 Каледино - 1							ЦМ-1							
1637 Княгинин - 3							ЦС-3							
1445 Койданово - 18							КР-2 ПВ-1 ЦС-3 МНР-2 ЦМ-1 ЗВ-9							
1408 Колодищи - 4							КР-3 ПВ-1							
1448 Колядичи - 108							КР-46 ПЛ-1 ПВ-7 ЦС-31 ЦМ-2 ФТ-21							
1412 Красное-Знамя - 22							ЦС-1 ЗВ-21							
1417 Крупки - 19							ПВ-15 ЦС-2 ПР-2							
1681 Лепель - 8							ПВ-1 ЦС-3 ЦМ-2 ЗВ-2							
1401 Минск-Сев - 6							ЦМ-6							
1400 Минск-Сорт - 9							ЦС-1 ЦМ-6 ФТ-2							
1405 Минск-Юж - 1							ПВ-1							
1450 Михановичи - 16							КР-1 ПВ-1 ЦС-14							
1629 Молодечно - 13							ПВ-5 ЦМ-2 ФТ-1 ПР-5							
1444 Негорелое - 7							КР-1 ПВ-4 ЗВ-2							

24 января 2022 года.
Телеграм-канал «Кибер-партизаны».

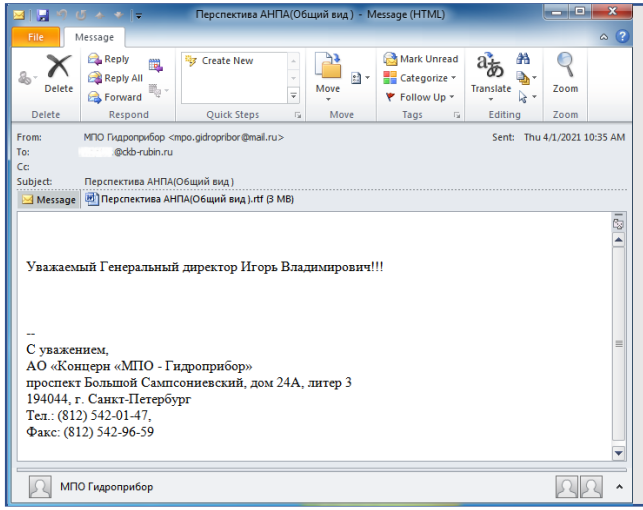
Комментарий хакеров:

"В рамках киберкампании "Пекло" мы зашифровали основную часть серверов, баз данных и рабочих станций БелЖД с целью замедлить и нарушить работу дороги. Бекапы уничтожены/ Кибератаке подверглись десятки баз данных, в том числе АС-След, АС-УСОГДП, SAP, АС-Пред, pass.rw.by, управа, ИРЦ и др"
"У нас ключи шифрования, и мы готовы при определенных условиях вернуть системы БелЖД в штатный режим".

Не важны декларируемые лозунги.
Фактически, речь идёт о диверсии.

ЦКБ «Рубин» - привет от китайских друзей

30 апреля 2021 компания Cybereason выпустила отчёт, в котором описала результаты отслеживания циркулирующего в дикой природе вредоноса RoyalRoad aka 8.t Dropper.



В качестве фишинговой приманки использовалось письмо генеральному директору ЦКБ «Рубин» Игорю Вильниту от имени АО "Концерн "МПО - Гидроприбор". Сама **приманка составлена грамотно**, правда адрес отправителя находится на mail .ru (хотя это как раз неудивительно...).

К письму был приложен файл "Перспектива АНПА(Общий вид).rtf", который содержал изображение АНПА и RoyalRoad в виде полезной нагрузки.

С большой долей вероятности, атакующие заранее подломили "Гидроприбор" либо близкое к нему учреждение, чтобы добыть правдоподобно выглядящую фишинговую приманку.

В качестве полезной нагрузки 8.t Dropper доставлял недокументированный ранее авторский бэкдор PortDoor, который представляет собой полноценный кибершпионский RAT.

Атрибуция, проведенная исследователями, указывает на китайские APT - используемая в приманке кодировка ранее была замечена у APT Tonto и APT TA428. Первая группа, как считается, работает под крышей Технического разведывательного Департамента НОАК (Unit 65017) в китайском городе Шэньян и в 2018 году уже была замечена в фишинговых атаках на Концерн Автоматика, входящий в Ростех.

https://www.cybereason.com/blog/portdoor-new-chinese-apt-backdoor-attack-targets-russian-defense-sector

Никогда такого не было и вот опять!

Хакерская группировка **MoneyTaker** смогла успешно атаковать российский банк через его рабочее место в ЦБ. До этого подобная атака была в 2018 году. У банка не из первой сотни смогли украсть более полумиллиарда рублей. Название банка не раскрывается.

Атака началась в **июне 2020** через компрометацию **аффилированной с банком компании**, **предположительно** за счёт эксплуатации уязвимости CVE-2018-13379 в межсетевом экране Fortinet FortiGate-200E. Финальная стадия стартовала в **январе 2021**.

В течение месяца атакующие получили доступ к сети банка. В последующие **шесть месяцев** они исследовали сеть.

В ходе атаки злоумышленники использовали ПО Mimikatz, встроенные утилиты в ОС Windows – WinRM и WMI, ПО RStudio, ПО для удаленного доступа DameWare, фреймворк Metasploit для удаленного исполнения команд, утилиты nbtstat, netstat, tasklist, PsExec и другие. *Были обнаружены следы использования бэкдора «DoublePulsar», разработанного группировкой Equation Group*.

Да поможет нам ГОСТ!

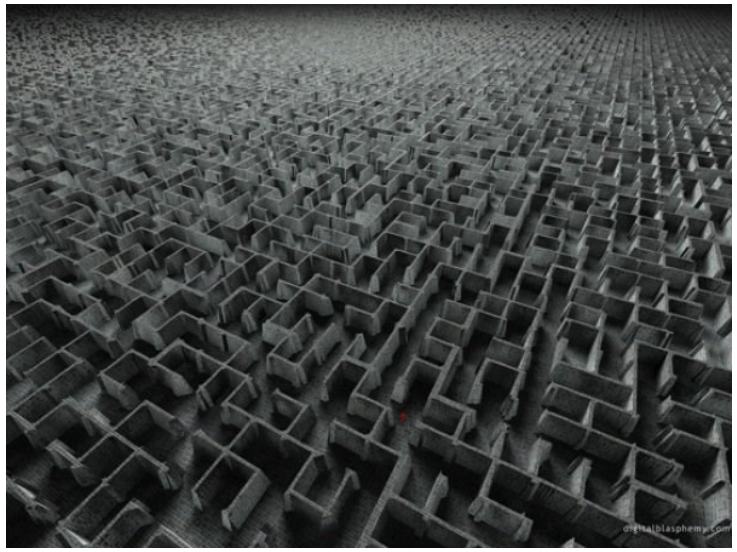
Платёжная инфраструктура любого государства – критически важный аспект функционирования его экономики.

> *Развитие и укрепление банковской системы Российской Федерации, развитие и обеспечение стабильности финансового рынка Российской Федерации и национальной платежной системы являются целями деятельности Банка России. Одним из основных условий реализации этих целей является обеспечение необходимого и достаточного уровня защиты информации в кредитных организациях, некредитных финансовых организациях РФ, а также субъектах национальной платежной системы (далее при совместном упоминании - финансовые организации).*

Главная «проблема» ГОСТ 57580.1-2017 – это то, что он технический. Допускается реализация организационной меры путём применения технической, но не наоборот, как это было раньше.

Сложности в понимании самого ГОСТ «на местах» и деловой подход ряда вендоров, порождают обратный перекос:
«Посоветуйте нам <*класс решения*>, чтобы выполнить требования ГОСТ-а».

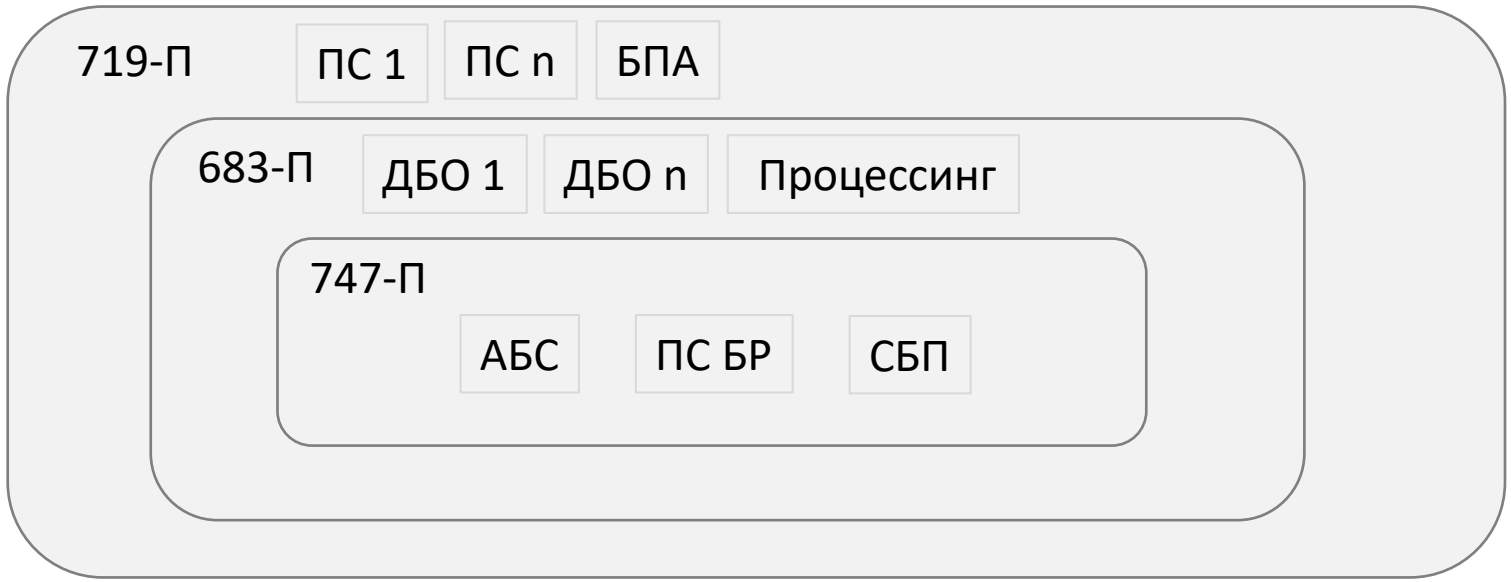
Лабиринты ГОСТа



Любой ГОСТ является добровольным к применению, если иное не определено нормативными актами.

В случае с ГОСТ 57580.1-2017 «слегка переборщили»: 747-П, 683-П, 719-П, 321 приказ...

Положений много, а банк один. Где границы отдельно взятого положения? Какие системы к чему относятся? Сколько аудитов необходимо проводить: один аудит на все положения или на каждое отдельно?



Риски – наше всё!

С 1 января 2022 годя банки обязаны соответствовать положению Банка России от 8 апреля 2020 года №716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе». Приведение в соответствие главе 7 «Управление риском информационной безопасности» и главе 8 «Управление риском информационных систем» создали не мало трудностей для соответствующих подразделений.

В настоящий момент в стадии утверждения находятся ГОСТ-а:

- «Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения».
- «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер».

Это значит, что ближайшее время будет выпущено положение, делающее эти ГОСТы обязательными и порядок оценки соответствия. Так или иначе, Банк России подводит к риск-ориентированному подходу управления ИБ.

Проблемы? Как же без них?

- Неправильная сегментация сети. Например, промышленные и тестовые серверы в одном сегменте.
- Используются групповые, общие и стандартные учетные записи и пароли.
- Нет защиты виртуализации.
- Отсутствие систем предотвращения утечек информации.
- Не обеспечивается централизованный сбор информации о событиях безопасности.
- Нет контроля отсутствия (выявление) аномальной сетевой активности.
- Нет управления уязвимостями защиты информации (не применяются сканеры уязвимостей, не производится автоматическое обновление ПО).
- Не проводятся тестирования на проникновение.

Если коротко, то большинство организаций имеют плохое техническое обеспечение и обеспечение кадрами.

Пришёл, увидел, всё взломал

Одним из требований Банка России в области ИБ является ежегодное проведение тестирования на проникновение.

В организации прошёл аудит соответствия ГОСТ Р 57580.1-2017 и получен достаточный уровень соответствия. Говорит ли это о высоком уровне практической безопасности?

Если коротко, то нет.

Основные причины:

- пароли (слабые, по умолчанию, легко добываемые);
- неиспользуемые протоколы;
- неправильная конфигурация оборудования;
- ошибки топологии сети;
- социальная инженерия;
- уязвимости.

И снова о паролях

Вроде бы уже всё давно всем известно, тем не менее.

1. Пароли по умолчанию – no comments.
2. Примитивные либо словарные пароли.

qwe-123, Qq12345678, zaq1234 – классика примитивизма.

«pfvtxfntkmysq,fyr_4» - сложный? – «замечательныйбанк_4».

3. <сезон><год>, работа<месяц> и т.п.
4. Конфиги с паролями в открытом виде.
5. Текстовые файлы с паролями («хитрые» создают 1.docx).

«Самый хороший собеседник тот, кто умеет слушать».

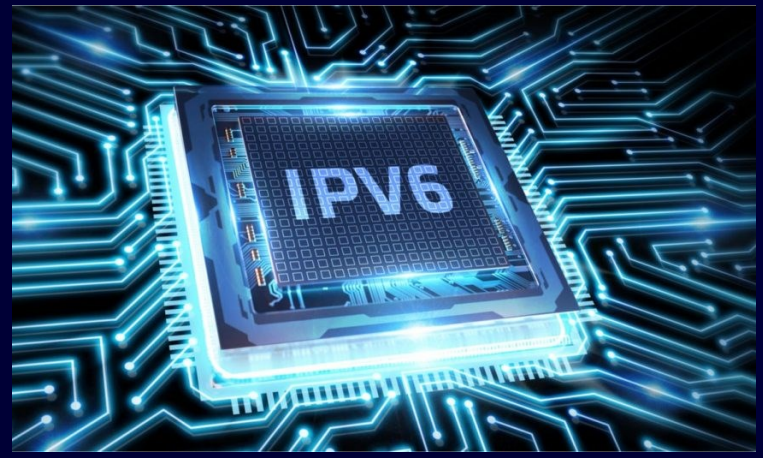
От «голого» TCP/IP до легального доступа в доме от нескольких минут до, максимум пара дней при почти полном отсутствии следов.

При тотальной проверке хешей домена на словарные пароли, от 30% до 60% - словарные пароли.

Протоколы

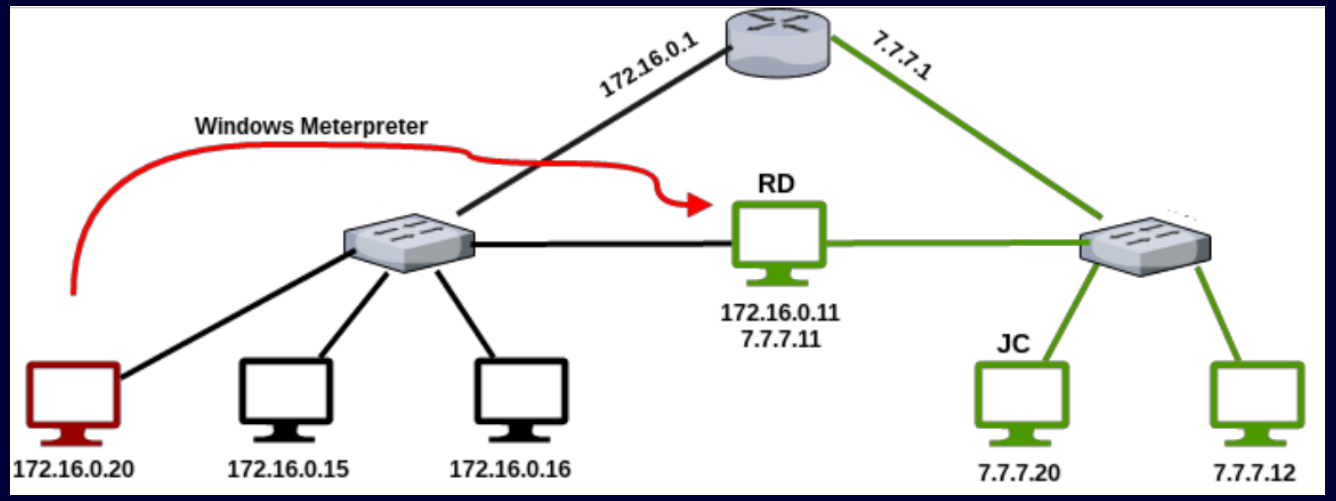
```
root@kali:~# responder -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.3.9

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CRTL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
```

- Включены неиспользуемые протоколы – LLMNR, MDNS, WPAD…
- Используется SMBv1
- Отключена подпись в SMB.
- SNMP v1 – Security is Not My Problem.
- IPv6 – приоритет над IPv4.



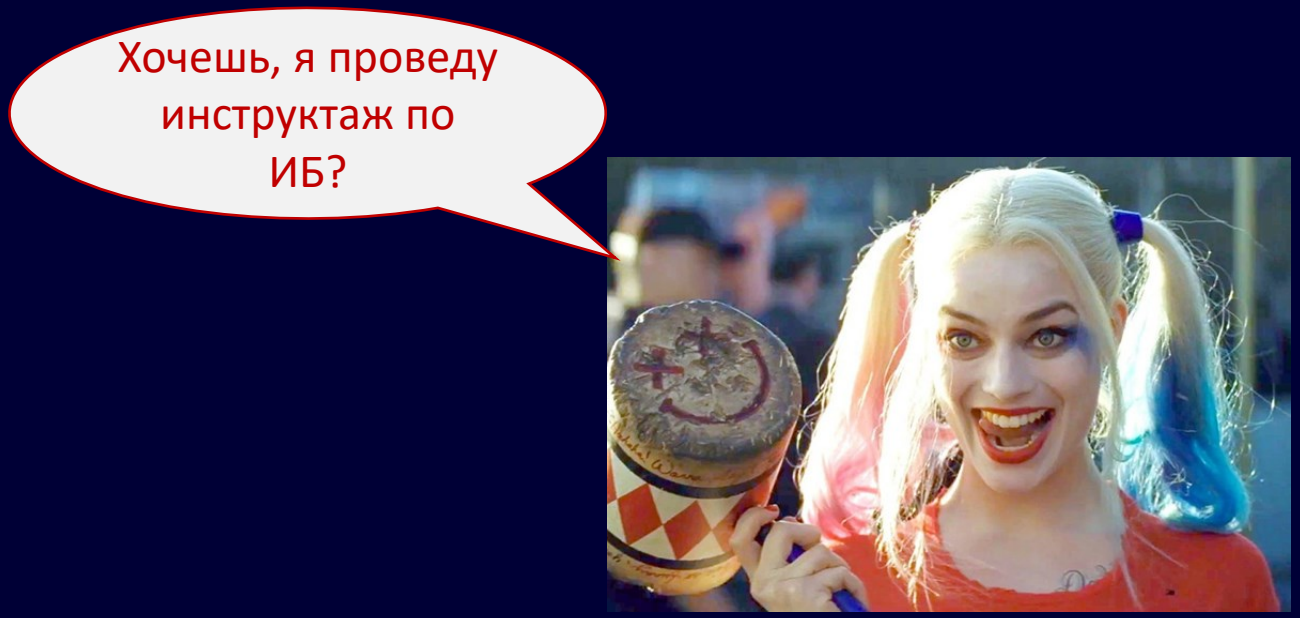
Топология сети

- Нет либо плохая сегментация сети
- «Двуногие» серверы – плохая идея
- Немаршрутизируемые сети – это не защита
- Нет фильтрации между сегментами.



Социальная инженерия

- Опыт применения социальной инженерии показывает слабую подготовку пользователей
- Больше половины пользователей перешли по ссылке в фишинговом письме и оставили свои учётные данные
- Некоторые вступали в переписку



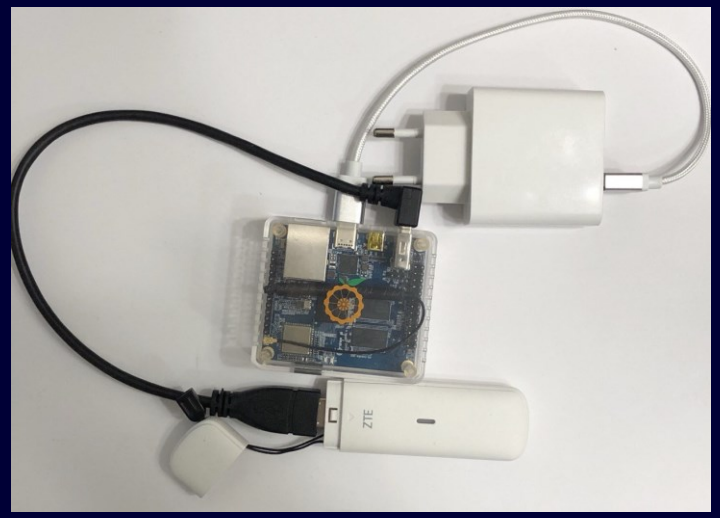
Социальная инженерия

Hitachi ID провели опрос среди руководителей IT и безопасности и их подчинённых в 100 крупных компаниях (более 5000 работников).

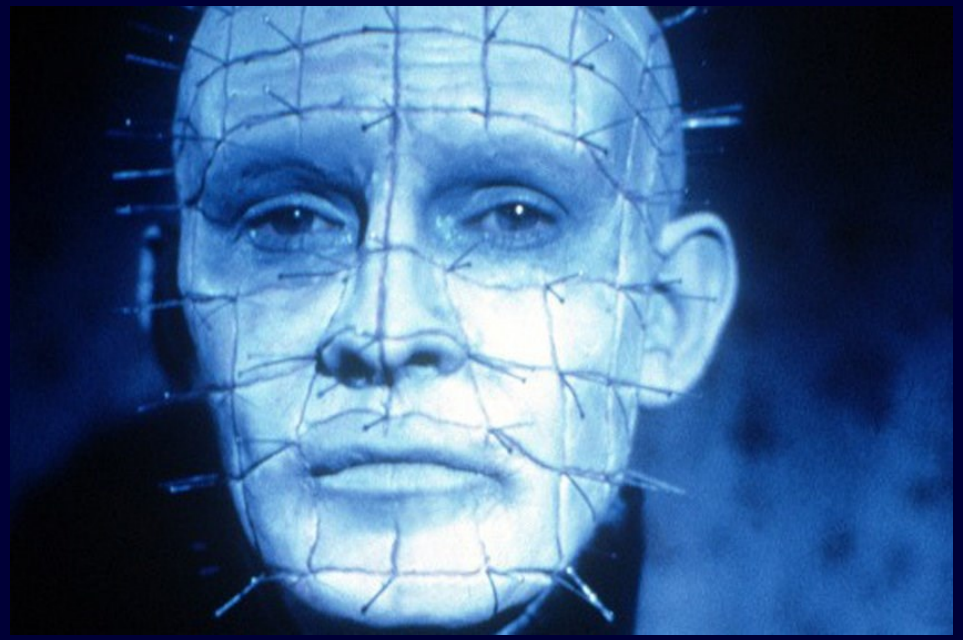
65% респондентов получали от злоумышленников предложение содействовать в вымогательских атака. Это на 17% больше, чем в ноябре 2021 года.

В атакованном банке так и не была обнаружена точка входа в сеть. Почему? Варианта два: либо надёжно затёрли следы, либо точку входа просто вынесли из сети до начала активной фазы операции.

Пример сетевого импланта – 55x65 мм, который может скрытно разместить кто угодно, имеющий доступ в контролируемую зону. Большинство небольших сетей не увидят «гостя» и не отреагируют. Ради доли от 500 млн. можно и на работу устроиться в атакуемую компанию.



Ошибки АДминов



- Администрируют АРМ и серверы под доменным администратором
- Один и тот же локальный админ для АРМ и серверов
- Скрипты с паролями открытым текстом
- Бросают RDP-сессии от имени доменного админа
- Бакап и другие службы с правами доменного админа
- Игнорируют события антивируса и т.п.

А что же СЗИ?

- Во многих случаях средств мониторинга просто нет
- Настройка СЗИ – «как прибили, так и держится»
- Неполное покрытие
- Некому сопровождать
- Используют «лекарства» off-label

И что делать?

- Инвентаризация активов и контроль покрытия СЗИ.
- Построить систему управления уязвимостями (непропатченный фаервол может сильно вырасти в цене)
- Систематический анализ защищённости (шире, чем просто пентест) и устранение недостатков по результатам
- Построить комплексную систему мониторинга (ходить по канату над пропастью с завязанными глазами можно, но не долго)

Многие считают, что для организации мониторинга достаточно приобрести SIEM. Как показывает практика, в большинстве случаев это будет просто очередная система, в которой что-то там происходит.

Центр кибербезопасности для банков

FINSOC

Реализует комплексный подход в решении задач обеспечения безопасности как самой финансовой организации, так и безопасности ее клиентов, опираясь на более чем 10-летний опыт

Направления деятельности

1. Создание новых технологий и продуктов противодействия мошенничеству и анализа на соответствие требованиям ПОД/ФТ, внедрение решений, консалтинг, обучение.

2. Консалтинг по соблюдению требований регуляторов и выстраивания процессов выявления и реагирования на инциденты информационной безопасности.

3. Создание новых технологий и продуктов кибербезопасности, предоставление сервиса мониторинга и реагирования на инциденты, расследование инцидентов, эксплуатация систем информационной безопасности.

FINSOC Аудит

Аудит защищенности и оценка соответствия требованиям

На основании наших отчетов и индивидуальных рекомендаций, полученных в результате проведения аудита, финансовая организация осуществляет процесс устранения недостатков в системе защиты информации и несоответствия в области compliance, минимизирует риски реализации угроз, обеспечивает необходимый уровень защищенности, и, как следствие, избегает не только санкций со стороны регуляторов, но и нарушения бизнес-процессов, разглашения конфиденциальных данных, репутационных и финансовых потерь

Оценка соответствия требованиям

- аудит соответствия ГОСТ Р 57580.1-2017, положениям ЦБ РФ 747-П, 683-П, 684-П, 719-П, 152-ФЗ «О персональных данных»
- оценка соответствия единой биометрической системы Приказу № 321
- аудит безопасности SWIFT — Customer Security Programme (CSP)
- управление рисками в соответствии с положениями ЦБ РФ 716-П, 590-П, 611-П и указанными ЦБ РФ 3624-У, 4927-У

Технический аудит защищенности

- тестирование на проникновение (penetration testing) по методам «белого», «черного» или «серого» ящика
- аудит программного кода
- аудит безопасности веб-приложений: сайтов, систем ДБО, порталов и т.д.

FINSOC Центр мониторинга

Мониторинг событий информационной безопасности и реагирование на инциденты

Обязательным условием для выстраивания полноценной системы защиты информации является мониторинг за событиями ИБ и реагирование на инциденты. Располагая собственным центром ИБ SOC «Сокол» (является центром ГосСОПКА), который объединяет в себе квалифицированный персонал, передовые технические средства и процессы, мы берем решение данной задачи на себя и сохраняем ценные ресурсы клиентов.

Мы обеспечим

оперативное выявление проблем (инцидентов) в ИТ-инфраструктуре

выявление злонамеренных (несанкционированных) действий

уведомление ответственных лиц

непрерывный инструментальный аудит ИТ-инфраструктуры

постоянную актуализацию данных и выявление проблемных мест

соответствие требованиям законодательства в части мониторинга ИБ

техническое расследование инцидентов

подключение объекта КИИ к ГосСОПКА

FINSOC Антифрод и ПОД/ФТ

Защита денежных средств организации и её клиентов

Атакам мошенников подвергаются не только финансовые организации, но и их клиенты, активно использующие банковские продукты и различные платежные каналы (ДБО, СБП, АБС). Для противодействия кибермошенничеству банки должны выполнять требования Федерального закона "О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств" № 167-ФЗ

Кроме того, организации финансового сектора должны останавливать сомнительные операции, выполняя требования Федерального закона "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" № 115-ФЗ, а также выявлять клиентов, фигурирующих в различных санкционных списках и контролировать операции с ними

Наши решения обеспечивают сохранность денежных средств и выполнение требований регуляторов

Противодействие мошенничеству

- FraudWall – современная система обнаружения мошеннических платежей («Антифрод-система»)
- ICFraud – система мониторинга состояния клиентского окружения
- FraudTrack – сервис, предоставляющий банку информацию обо всех проблемах на стороне клиента
- FraudInform – автоматизированная система голосового подтверждения подозрительных платежей

Противодействие ОД/ФТ

- **FraudWall AML** – система противодействия отмыванию (легализации) доходов и финансированию терроризма
- **FraudWall AML List** – модуль проверки юридических и физических лиц по санкционным спискам и перечням публичных должностных лиц

FINSOC Поставки оборудования

Поставка средств защиты информации и оборудования для ИТ-инфраструктуры

Предоставляя возможность построения полноценной системы защиты информации, противостоящей в соответствии с законодательством Российской Федерации угрозам неправомерного доступа, изменения, удаления и распространения конфиденциальных данных, мы обеспечиваем поставку средств защиты информации от ключевых российских производителей, а также грамотную техническую поддержку и информационное сопровождение

Нашим клиентам мы предлагаем

проектирование, внедрение, техническую поддержку и сопровождение ИТ-инфраструктуры

средства вычислительной техники

телекоммуникационное, периферийное и сетевое оборудование

системы хранения данных, источники бесперебойного питания, расходные материалы

инфраструктурное ПО

внедрение и техническую поддержку систем электронной очереди, видеонаблюдения, систем контроля и управления доступом

FINSOC

+7 (495) 967-65-19

promo@frodex.ru

finsoc.online