PRO iP VIDEO

Тема доклада:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ПРОЕКТАХ ВИДЕОНАБЛЮДЕНИЯ

Дмитрий Борощук
независимый эксперт в области ситуационной безопасности

ЭВОЛЮЦИЯ ФИЗИЧЕСКИХ ИНТЕРФЕЙСОВ

RS-232

RS-485/422

ПИТАНИЕ

ВИДЕО

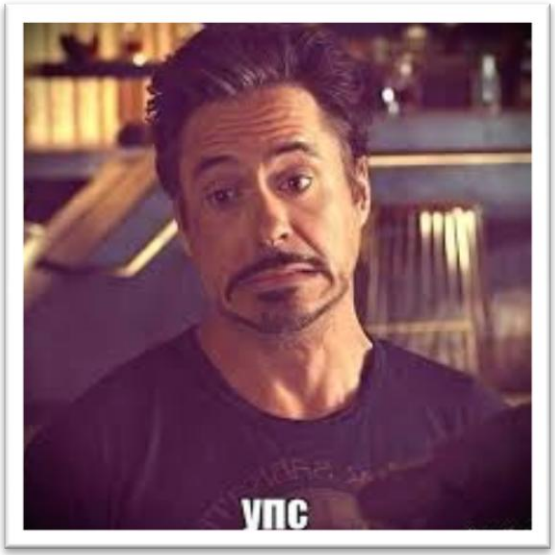
ETHERNET PoE TCP/IP

ИСТОРИЯ ПЕРВАЯ. «ЗАЩИТА ОТ ДУРАКА». ЛОКАЛЬНАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

ИСТОРИЯ ПЕРВАЯ. «ЗАЩИТА ОТ ДУРАКА». ЛОКАЛЬНАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

ПРОБЛЕМЫ И УГРОЗЫ

- Полный или частичный вывод из строя системы
- Умышленное или случайное удаление/изменение информации
- Сложности в оперативном управление системой
- Задержки при передачи видеоизображения
- Невозможность оперативного проведения простых ремонтных работ без привлечения стороннего специалиста
- Физический доступ к сетевому оборудованию



ИСТОРИЯ ПЕРВАЯ. «ЗАЩИТА ОТ ДУРАКА». ЛОКАЛЬНАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

ПРИНЦИПЫ ПОСТРОЕНИЯ

- Разумная достаточность (STAND ALONE или платформенное решение)
- Оптимизация в составе оборудования (минимизация элементов системы)
- Создание закрытой самостоятельной экосистемы (локализация всех элементов)
- Резервированное питание для всех компонентов системы
- Разделение DVR/NVR/сервер оборудования и АРМ
- Оборудование сетевого сегмента – одного производителя для лучшей интеграции
- Упрощение элементов пользовательского интерфейса
- Разделение прав доступа
- Физическая защита оборудования

ИСТОРИЯ ПЕРВАЯ. «ЗАЩИТА ОТ ДУРАКА». ЛОКАЛЬНАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

МЕТОДИКА ПОДБОРА ОБОРУДОВАНИЯ

DVR/NVR

Интегрированные решения с встроенными Ethernet PoE. (Power on Ethernet) для подключения и питания видеокамер. Для маленьких систем начального уровня

МАРШРУТИРИЗАТОР

Раздача PoE питания на портах (Passive PoE)

Встроенный Firewall и NAT (правила фильтрации по ip/mac/url)

Поддержка туннельных протоколов (PPTP/PPoE/IPsec/SSTP/L2TP/IP2IP/EoIP)

Встроенный VPN сервер

ИСТОРИЯ ПЕРВАЯ. «ЗАЩИТА ОТ ДУРАКА». ЛОКАЛЬНАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ.

БЕСПРОВОДНЫЕ МОСТЫ

Многодиапазонность 900МГц/1800МГц/2.4ГГц/5ГГц

Встроенный контроль состояния радиоэфира

Поддержка туннельных протоколов (PPTP/PPoE/IPsec/SSTP/L2TP/IP2IP/EoIP)

ИСТОРИЯ ВТОРАЯ. «ВЕЗДЕ КАК ДОМА». СЕТЕВАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

ИСТОРИЯ ВТОРАЯ. «ВЕЗДЕ КАК ДОМА». СЕТЕВАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

ПРОБЛЕМЫ И УГРОЗЫ:

- Полный/частичный вывод из строя системы.
- Утечка информации
- Вектор атаки для проникновения в сеть
- Манипулирование потоком с камер
- Манипулирование АРМ / сервером.
- MITM и Spoofing – атаки
- DDOS- атаки
- Ваше оборудование будет майнить криптовалюту! Не Вам! ☹

ИСТОРИЯ ВТОРАЯ. «ВЕЗДЕ КАК ДОМА». СЕТЕВАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

ПРОБЛЕМЫ И УГРОЗЫ

ACTi: admin/123456 or Admin/123456
Amcrest: admin/admin
American Dynamics: admin/admin or admin/9999
Arecont Vision: none
AvertX: admin/1234
Avigilon: Previously admin/admin, changed to Administrator/<blank> in later firmware versions
Axis: Traditionally root/pass, n[illegible] require p[illegible]ord c[illegible]tion during [illegible]n (not that root/pass may be used fo[illegible]NVIF access but logg[illegible]the[illegible]quire[illegible]rod[illegible]assw[illegible] creation)
Basler: admin/admin
Bosch: None required, but new firmwares (6.0+) prompt users to create passwords on first login
Brickcom: admin/admin
Canon: root/camera
Cisco: No default password, requires creation during first log[illegible]
Dahua: Requires password creation on first login. Previously t[illegible]pro[illegible]s w[illegible]me[illegible] could be canceled; older models default to admin/admin
Digital Watchdog: admin/admin
DRS: admin/1234
DVTel: Admin/1234
DynaColor: Admin/1234
FLIR: admin/fliradmin
FLIR (Dahua OEM): admin/admin
FLIR (Quasar/Ariel): admin/admin
Foscam: admin/<blank>
GeoVision: admin/admin
Grandstream: admin/admin
Hanwha: admin/no default password, must be created during initia[illegible]
Hikvision: Firmware 5.3.0 and up requires unique password creatio[illegible]revi[illegible]y[illegible]min/[illegible]
Honeywell: admin/1234
IndigoVision (Ultra): none
IndigoVision (BX/GX): Admin/1234
Intellio: admin/admin
Interlogix admin/1234
IQinVision: root/system

IPX-DDK: root/admin or root/Admin
JVC: admin/jvc
Longse: admin/12345
Lorex: admin/admin
LTS: Requires unique password creation; previously admin/12345
March Networks: admin/<blank>
Mobotix: [illegible]
Panasonic: [illegible]Firmware 2[illegible]and [illegible]requires [illegible]/[illegible]on; previously admin/12345
Pelco: New firmwares require unique password creation; previously admin/admin
Pixord: admin/admin
Q-S[illegible]admin/a[illegible]or admin/123456
R[illegible]admin/[illegible]
Samsung [illegible]ctr[illegible]cs: [illegible]/[illegible]min/4321
S[illegible]old[illegible]d[illegible]n[illegible]1
Samsung (new): Previously admin/4321, but new firmwares require unique password creation
Sanyo: admin/admin
Scallop: admin/password
Se[illegible]360 (mini): admin/1234
[illegible]360 (pro): none
[illegible]admin/admin
Sp[illegible]admin/1234
Stardot: admin/admin
Starvedia: admin/<blank>
Sunell: admin/admin
[illegible]
[illegible]net[illegible]min/[illegible]
[illegible]iba: [illegible]/ikw[illegible]
VideoIQ: [illegible]ervis[illegible]is[illegible]
Vivotek: root/<blank>
Ubiquiti: ubnt/ubnt
Uniview: admin/123456
W-Box (Hikvision OEM, old): admin/wbox123
W-Box (Sunell OEM, new): admin/admin
Wodsee: admin/<blank>

СТАНДАРТНЫЕ ПАРОЛИ И ПОРТЫ

ИСТОРИЯ ВТОРАЯ. «ВЕЗДЕ КАК ДОМА». СЕТЕВАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

МЕТОДИКА ПОДБОРА ОБОРУДОВАНИЯ. МЕЖСЕТЕВЫЕ ЭКРАНЫ.

- Идентификация и контроль приложений по любому порту
- Идентификация и контроль попыток обхода защиты
- Управление неизвестным трафиком
- Сканирование с целью выявления вирусов и вредоносных программ во всех приложениях, по всем портам
- Обеспечение одинакового уровня визуализации и контроля приложений для всех пользователей и устройств
- Упрощение, а не усложнение системы безопасности сети благодаря добавлению функции контроля приложений
- Обеспечение той же пропускной способности и производительности при полностью включенной системе безопасности приложений

ИСТОРИЯ ВТОРАЯ. «ВЕЗДЕ КАК ДОМА». СЕТЕВАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

МЕТОДИКА ПОДБОРА ОБОРУДОВАНИЯ. МЕЖСЕТЕВЫЕ ЭКРАНЫ. НЕОБХОДИМЫЕ КОМПОНЕНТЫ

- Управление HotSpot (Гостевыми точками доступа)
- Управление полосой пропускания
- Интерфейсы VLAN
- VPN (IPSec,SSL,L2TP over IPSec)
- SSL/HTTPS inspections
- Журнал событий и мониторинга
- Настраиваемые зоны
- Система обнаружения вторжений (IntrusionDetection and Prevention)

ИСТОРИЯ ВТОРАЯ. «ВЕЗДЕ КАК ДОМА». СЕТЕВАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ

ЗАЩИЩАЕМСЯ:

- Идентификация пользователя. Определение полномочий.
- Используем аутентификацию устройств в сети
- Создаем отдельные сети VLAN
- Включаем фильтрацию ip-адресов на устройствах
- Используем VPN для подключения удаленных устройств
- Включаем HTTPS, SSL/TLC
- Отключаем камеры от сторонних встроенных сервисов.
- Отключаем DHCP. Принцип «Белого списка»
- Закрываем неиспользуемые порты
- Изменяем стандартные порты
- Используем аутентификацию устройств в сети
- Контроль активности сетевого окружения

СЕТЕВАЯ СИСТЕМА ВИДЕОНАБЛЮДЕНИЯ. ВЫВОДЫ

ПРОВЕРЯЙ!

- Установили ли вы, кто и как будет использовать систему? Необходимо конкретизировать роли администратора, оператора и наблюдателя
- Известно ли вам, что происходит с хранящимся в архиве материалом? Как долго предполагается хранить видеоматериалы, и кто будет иметь доступ к записям
- Проверена ли физическая безопасность инсталляции? Кабели и сетевое оборудование необходимо тщательно защитить.
- Предусмотрена ли процедура проверки безопасности системы через определенные промежутки времени? Удостоверьтесь в том, что предусмотренные вами процессы действуют и система работает исправно.
- Актуальны ли меры информационной безопасности в текущий момент?

В ЗАПИСНУЮ КНИЖКУ ПРОЕКТИРОВЩИКА

1. Обеспечь физическую защиту доступа к оборудованию инфраструктуры
2. Установи простой и понятный интерфейс взаимодействия системы с оператором
3. Используй защищенное VPN соединение со всеми распределенными элементами системы
4. Используй физическое или логическое разделение (VLAN) сети для систем безопасности и общей сетью
5. Принцип «белого списка» для всех элементов вашей системы
6. Актуализируй firmware/software