Управление на външни запаметяващи устройства

Видове, рискове и защита на данните

Георги Емилов Исаев | НФСГ София | Икономическа информатика | 2025/2026

Цел и задачи на изследването

Основна цел

Анализ на уязвимостите в управлението на външни запаметяващи устройства и разработка на модел за комплексна защита на данните.

Четири ключови задачи

- Класификация на устройства и интерфейси
- Оценка на рисковете по NIST SP 800-30
- Изследване на методи за защита
- Практическа реализация в Active Directory

⚠ 37% от атаките срещу индустриални системи се извършват чрез USB устройства според ENISA (2023)

Видове устройства и интерфейси

Съвременните външни запаметяващи устройства предлагат значително разнообразие в скорост, капацитет и предназначение.

Тип устройство	Макс. скорост	Цена/GB	Основна ниша/употреба
USB Flash	до 400 MB/s	0,05-0,15 €	Ежедневен обмен
Външен SSD	до 2 000 MB/s	0,07-0,12 €	Висока скорост
Външен HDD	до 160 MB/s	0,02-0,04 €	Масово архивиране

100×

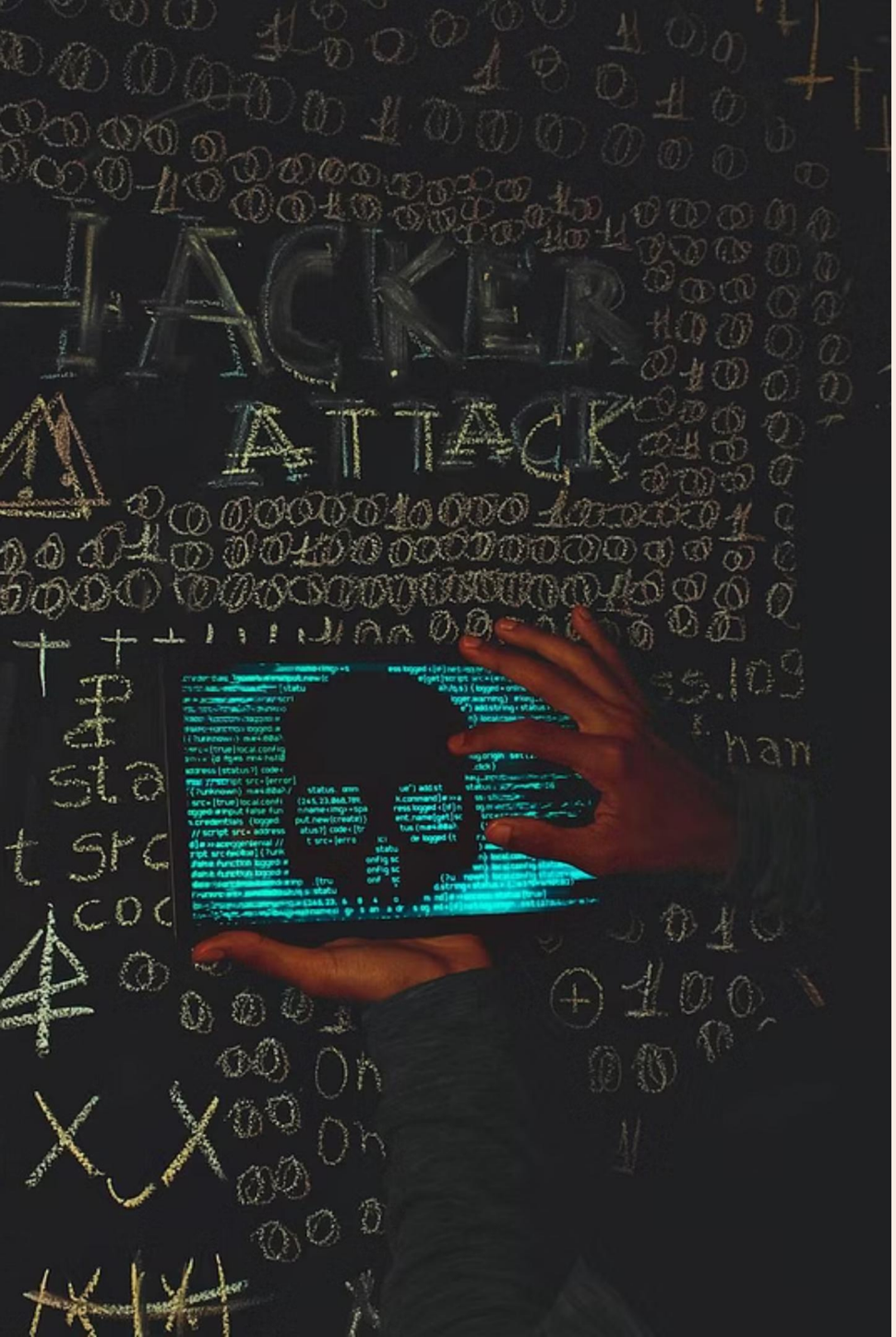
Разлика в скоростта

USB 2.0 (60 MB/s) срещу NVMe Gen 4 (7 000 MB/s)

10×

Разлика в цената

От USB flash до външен HDD по отношение на цена/GB



Рискове за киберсигурността

Оценка на уязвимостите по методологията NIST SP 800-30 и ISO 27005.

MALWARE

Автоматично разпространение на зловреден софтуер при свързване. Критичен риск за организационната сигурност.

THEFT

Несанкциониран достъп до конфиденциални данни. Критичен риск с тежки правни последствия.

RANSOMWARE

Шифроване на данни с изискване за откуп. Висок риск за бизнес критични системи.

BADUSBATTACK

Префалшифициране на USB контролера за маскиране като клавиатура. Среден риск с висока сложност.

Мерки за защита на данните

Технически мерки

01

Криптиране

BitLocker To Go (AD/GPO) · VeraCrypt (FOSS) · LUKS (Linux)

02

Антивирус

Автоматично сканиране при свързване на устройство

03

Backup

Стратегия 3-2-1: 3 копия, 2 носителя, 1 offsite

Контрол и политики

- **Device Whitelisting** – разрешаване само на одобрени устройства
- **Деактивиране на AutoRun** – предотвратяване на автоматично изпълнение
- **RBAC** – контрол на достъпа базиран на роли
- **Организационна рамка:** 10-точкова политика (ISO 27001 + NIST 800-53)
- **GDPR чл. 32/33** – правна уредба за защита на лични данни

Defense in Depth подход – многослойна защита за максимална сигурност

Практическа демонстрация

Имплементация в Active Directory среда

Среда: Windows Server 2019/2022 с Active Directory

OU (Organizational Unit) структура:

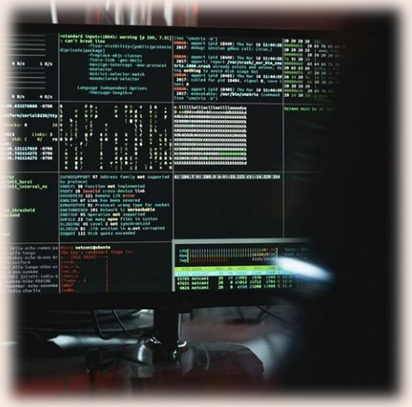
- USB-Blocked → забрана за запис
- USB-Allowed → запис само с BitLocker

Операция	USB-Allowed	USB-Blocked
Четене	✓ Разрешено	✓ Разрешено
Запис	✓ с BitLocker	✗ Забранено
Одит (Event 4663)	✓ Записва се	✓ Записва се

GPO политики осигуряват централизиран контрол и проследяване на всички USB операции

Реални казуси

Уроци от исторически инциденти в киберсигурността.



Stuxnet (2010)

Атака срещу иранска ядрена програма чрез USB.

Поука: Изолирана мрежа ≠ безопасна. Физически достъп до дори изолирани системи винаги е възможен.

Heathrow Airport (2017)

Загуба на USB с лични данни на 1 000+ пътници.

Поука: Криптирането е задължително. GDPR глоба £120K за несъответствие с регулациите.

IBM (2018)

Въвеждане на комплексна и много строга USB политика.

Поука: Цялостен подход → -50% инциденти. Инвестицията в сигурност се отплаща.

Приноси и заключение

Всички поставени цели са постигнати успешно.

Задача	Реализация	Резултат
1. Класификация	Раздел 2.1, Таблици 1-2	5 типа, 7 интерфейса
2. Рискове	Раздел 3.1, Таблица 3	8 риска по NIST
3. Защита	Раздел 3.2, Таблици 4, 6	3 решения, Defense in Depth
4. Практика	Раздел 3.6, Фиг. 1-8	GPO + BitLocker в AD

Систематизиран анализ

Класификация на 5 типа устройства и 7 интерфейса със съпоставка на характеристики

Матрица на риска

Оценка на 8 риска по NIST SP 800-30 с приоритизация по вероятност и въздействие

Модел Defense in Depth

Многослойна защита с криптиране, антивирус, контрол на достъп и одит

Чеклист NIST CSF 2.0

Практически чеклист за имплементация в организация по рамката NIST Cybersecurity Framework

Благодаря за вниманието!

Георги Емилов Исаев

НФСГ София | Икономическа информатика | 2025/2026

diploma.isaewwxx.dev

github.com/isaewwxx

georgi@capybarahost.eu

Готов съм за въпроси.