NIS2: КРАТЪК НАРЪЧНИК ЗА БИЗНЕС ЛИДЕРИ

5 КРИТИЧНИ НЕЩА, КОИТО ТРЯБВА ДА ЗНАЕТЕ

CYBER ONE

ЗА КАКВО Е ТОЗИ НАРЪЧНИК?

NIS² Е ФАКТ

СРОКЪТ ТЕЧЕ. ПОСЛЕДСТВИЯТА СА СЕРИОЗНИ.

ТОЗИ КРАТЪК НАРЪЧНИК ВИ ОБЯСНЯВА – КАКВО Е NIS², ЗАСЯГА ЛИ ВИ И КАКВО ТРЯБВА ДА НАПРАВИТЕ

НЕКА ЗАПОЧВАМЕ

MYTHS

"НИЕ НЕ СМЕ КРИТИЧНА ИНФРАСТРУКТУРА. NIS2 НЕ Е ЗА НАС."

FACTS

NIS2 ЗАСЯГА **18 СЕКТОРА** И КОМПАНИИ СЪС 50+ СЛУЖИТЕЛИ ИЛИ €10M+ ОБОРОТ.

ПОПАДАТЕ ЛИ ПОД NIS²? ПРОВЕРЕТЕ:

ОСНОВНИ СЕКТОРИ (ВИСОКО КРИТИЧНИ)

ЕНЕРГЕТИКА

ТРАНСПОРТ

БАНКИ И ФИНАНСИ

ЗДРАВЕ ОПАЗВАНЕ

ПИТЕЙНА ВОДА

ДИГИТАЛНИ ИНФРАКСТРУКТУРИ
(ОБЛАЧНИ УСЛУГИ, ДАТА ЦЕНТРОВЕ, DNS)

ИКТ УПРАВЛЕНИЕ (MSP, MSSP)

ПУБЛИЧНА АДМИНИСТРАЦИЯ

ВАЖНИ СЕКТОРИ

ПОЩИ И КУРИЕРИ

УПРАВЛЕНИЕ НА ОТПАДЪЦИ

ХИМИЧЕСКА ПРОМИШЛЕНОСТ

ХРАНИТЕЛНА ИНДУСТРИЯ

ПРОИЗВОДСТВО
(МЕДИЦИНСКИ УСТРОЙСТВА, ЕЛЕКТРОНИКА, МАШИНИ)

ЦИФРОВИ УСЛУГИ
(ОНЛАЙН ПЛАТФОРМИ, СОЦИАЛНИ МРЕЖИ)

РАЗМЕР НА КОМПАНИЯТА

СРЕДНИ ПРЕДПРИЯТИЯ
50+ СЛУЖИТЕЛИ ИЛИ €10M+ ОБОРОТ

ГОЛЕМИ ПРЕДПРИЯТИЯ
250+ СЛУЖИТЕЛИ ИЛИ €50M+ ОБОРОТ

ВАЖНО ЗА ДОСТАВЧИЦИ

Ако доставяте услуги на компания под NIS2, това засяга и **ВАС.**

Вашите клиенти ще изискват доказателства за киберсигурност. Без съответствие = загубени договори.

NIS^2 въвежда лична отговорност на ръководството.

Вашите задължения като CEO/Борд:

- ✔ Одобрявате мерките за киберсигурност
- ✔ Наблюдавате прилагането им
- ✔ Провеждате редовни обучения (задължително!)
- ✔ Носите лична отговорност при нарушения

Санкции за ръководството

АКО ПОПАДАТЕ В:

ОСНОВНИ СЕКТОРИ

До €10 милиона глоба* или
2% от глобалния оборот

ВАЖНИ СЕКТОРИ

До €7 милиона глоба* или
1,4% от глобалния оборот

СЪЩО И

Временно отстраняване от длъжност

Забрана за заемане на управленски позиции

Публично оповестяване (репутационна катастрофа)

Вече НЕ можете да кажете:

"IT отделът се грижи за това."

Сега трябва да кажете:

“Киберсигурността е стратегически приоритет на борда."

***До 01.06.2026г. се налагат глоби и имуществени санкции в размер, намален с 50% от горепосочените условия**

10ТЕ ЗАДЪЛЖИТЕЛНИ МЕРКИ ПО NIS2

1. Управление на риска
- Редовна оценка на заплахи
- Документирани политики
- План за действие

2. Управление на инциденти
- Процедури за реагиране
- 24-часово докладване при атака
- Окончателен доклад до 1 месец

3. Бизнес непрекъснатост
- Планове за възстановяване
- Backup и тестове
- Crisis management

4. Сигурност на доставчиците
- Оценка на партньори
- Договорни клаузи
- Мониторинг на риска

5. Сигурност при разработка
- Security by design
- Управление на уязвимости
- Patch management

6. Тестване на защитите
- Penetration testing
- Одити
- Оценка на ефективност

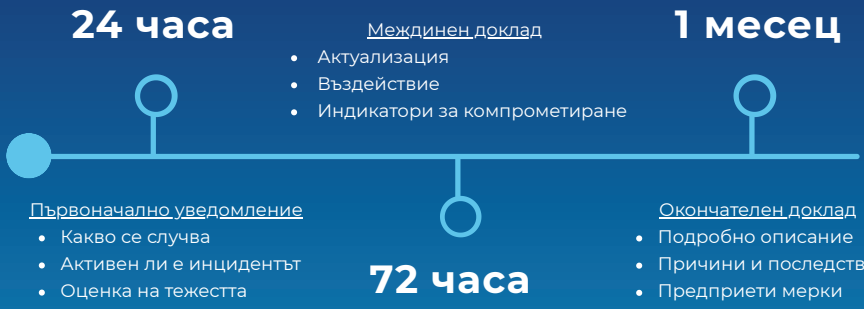
7. Обучение на персонала
- Редовни тренинги
- Симулирани фишинг атаки
- Политики за киберхигиена

8. Криптография
- Шифроване на данни
- Сигурни комуникации

9. Контрол на достъпа
- Принцип на минимални привилегии
- Проверки при наемане
- Инвентаризация на активи

10. Многофакторна автентикация
- Задължителна MFA за критични системи
- Защитени комуникации

Докладването е БЪРЗО и **задължително**



Срокове при значителен инцидент ⓘ

Към кого трябва да се докладва?

Всяка една организация, която попада под директивата трябва да се свърже в указаното време на **Министерство на електронното управление (МЕУ)**.

⚠ Неспазване = Отделна санкция
Забавено докладване носи допълнителни глоби.

Подгответе се СЕГА

- ☐ План за реагиране при инциденти
- ☐ Определени отговорни лица
- ☐ Процедури за комуникация
- ☐ Връзка с Държавна агенция „Електронно управление"

ⓘ Значителен инцидент е когато има: Сериозно оперативно прекъсване, Финансови загуби, Засяга клиенти и/или партньори, Обществен интерес

Това е непрекъснат процес (не еднократен проект)

"Ще имплементираме NIS^2 и ще приключим."

"Ще изградим система за непрекъснато управление на киберриска."

Защо не можете да "приключите" NIS2

Заплахите се променят

Нови уязвимости всеки ден
Нови тактики на хакери
Променяща се инфраструктура

Регулаторът следи

Инспекции без предизвестие
Искане на документация
Одити за ваша сметка

Бизнесът еволюира

Нови системи
Нови служители
Нови партньори

Променете мисленето

Старо мислене	Ново мислене NIS2
киберсигурност = ИТ проблем	Киберсигурност = бизнес риск
Инвестиция при нужда	Непрекъсната инвестиция
Реактивен подход	Проактивен подход
Техническа отговорност	Отговорност на ръководството

Какво да направите (в 7 стъпки)

Стъпка 1: Определете статуса (1 седмица)

- [ ] Попадате ли под NIS2?
- [ ] Основен или важен субект?
- [ ] Консултирайте се с експерти

Стъпка 2: Оценете състоянието (2-4 седмици)

- [ ] Gap analysis - къде сте сега?
- [ ] Какви са пропуските?
- [ ] Приоритизирайте рисковете

Стъпка 3: Създайте план (1 месец)

- [ ] Технически мерки
- [ ] Организационни промени
- [ ] Бюджет и ресурси
- [ ] Времева рамка

Стъпка 4: Ангажирайте ръководството

- [ ] Презентация пред борда
- [ ] Одобрение на инвестиции
- [ ] Назначаване на отговорници

Стъпка 5: Стартирайте обучения (непрекъснато)

- [ ] Обучение на ръководство
- [ ] Обучение на персонал
- [ ] Симулации на инциденти

Какво да направите (в 7 стъпки)

Стъпка 6: Изградете процедури (2-3 месец)

- [ ] Политики и процедури
- [ ] План за инциденти
- [ ] Докладване и комуникация

Стъпка 7: Партнирайте си с експерти (препоръчително)

- [ ] Консултанти за NIS2
- [ ] Доставчици на киберсигурност
- [ ] Одитори

Финалният въпрос

НЕ питайте:

"Колко струва да спазваме NIS2?"

ПИТАЙТЕ

"Колко ще ни струва да **НЕ** спазваме NIS2?"

Цената на неспазване

- Глоби: до **€10M**
- Репутационна щета: **безценна**
- Загубени договори: **неизчислими**
- Киберинцидент: **€4.45M** средно в Европа
- Ваше отстраняване: **безценно**

Цената на съответствие

- Инвестиция в устойчивост
- Защита от киберзаплахи
- Конкурентно предимство
- Спокоен сън

Не чакайте санкция да ви накара да действате.

CyberOne ви помага с

- ✅ **Gap Analysis** - Безплатна първоначална оценка
- ✅ **Карта за съответствие** - Ясен план за действие
- ✅ **Имплементация** - Технически и организационни мерки
- ✅ **Обучения** - За ръководство и персонал
- ✅ **Постоянна подкрепа** - Непрекъснато управление на риска

Свържете се с нас
info@cyberone.bg +359 882 333 156

CYBER ONE

Този e-book е създаден от екипа на CyberOne - вашият партньор за киберсигурност и регулаторно съответствие в България.