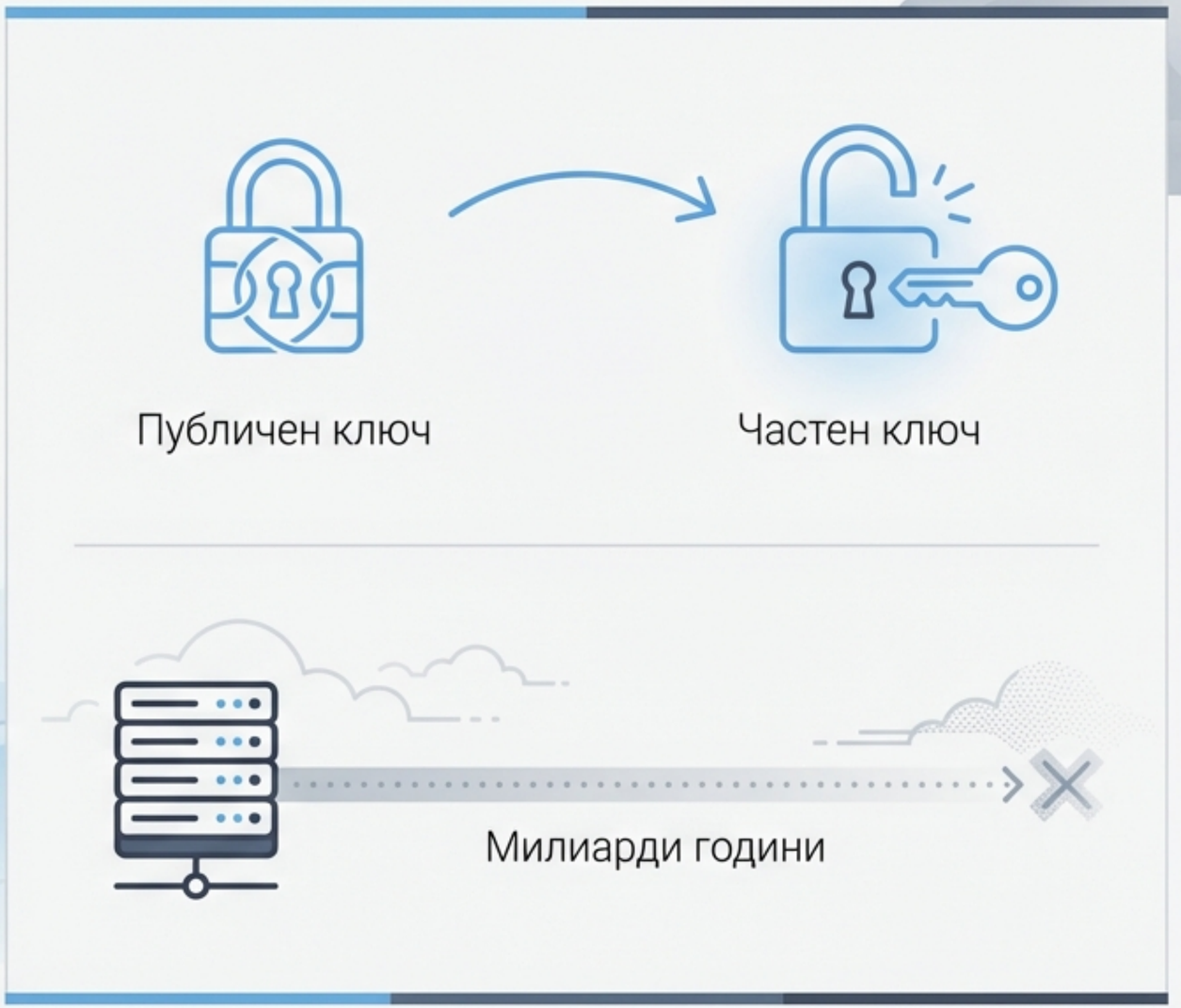
Неизбежната буря: Неизбежната буря: Навигация в квантовата заплаха за киберсигурността

Стратегическо ръководство за подготовка за пост-квантовата ера

NotebookLM

Основата на дигиталното доверие днес

Сигурността на днешния интернет се основава на асиметрична криптография (RSA, ECC, Diffie-Hellman). Тези алгоритми разчитат на математически проблеми, които са умишлено трудни за решаване от класическите компютри – като факторизиране на много големи числа. За един класически компютър решаването им би отнело милиарди години.



NotebookLM

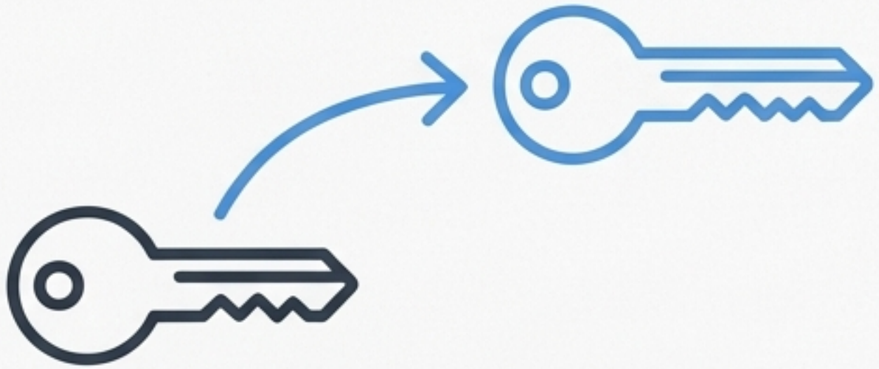
Квантовите изчисления пренаписват правилата на математиката

Публично-ключова криптография



- Алгоритъмът на Шор (Shor's Algorithm) може да факторизира големи числа експоненциално по-бързо.
- Това директно компрометира RSA и ECC, правейки ги остарели, след като се появи криптографски релевантен квантов компютър (CRQC).

Симетрична криптография



- Алгоритъмът на Гроувър (Grover's Algorithm) ускорява търсенето тип "груба сила", намалявайки ефективната сигурност (напр. AES-256 става еквивалентен на AES-128).
- Защитата може да бъде възстановена чрез удвояване на дължината на ключовете.

"Quantum computing threatens cybersecurity not because it hacks differently—but because it rewrites the mathematics that modern encryption depends on." - *Palo Alto Networks*

NotebookLM

Обратното броене се ускорява драстично

~~2052~~ → 2034

Прогнозата на Metaculus за деня, в който квантов компютър ще разбие RSA криптиране.



"Уверено прогнозирам Q-ден между 2028 и 2033 г." – Nic Carter, криптоанализатор.



Виталик Бутерин (съосновател на Ethereum) предупреждава, че криптографията с елиптични криви може да бъде изложена на риск по-рано, отколкото индустрията е предполагала.

Данни от Metaculus, цитирани в "BeInCrypto"

NotebookLM

Тихата жътва: Заплахата е активна днес

HNDL (Harvest Now, Decrypt Later) е киберзаплаха, при която **криптирани данни** се събират и съхраняват днес, за да бъдат декриптирани **в бъдеще, когато квантовите компютри** станат достатъчно мощни.

HNDL Процес: От Събиране до Дешифриране



Стъпка 1: Събиране (Collect)

Противниците пасивно прихващат и архивират криптиран трафик. Тази фаза е почти невъзможна за откриване.

Стъпка 2: Съхранение (Store)

Данните се съхраняват на евтини носители в очакване на изчислителен пробив.

Стъпка 3: Декриптиране (Decrypt)

Когато CRQC стане достъпен, съхранените данни се декриптират ретроактивно.

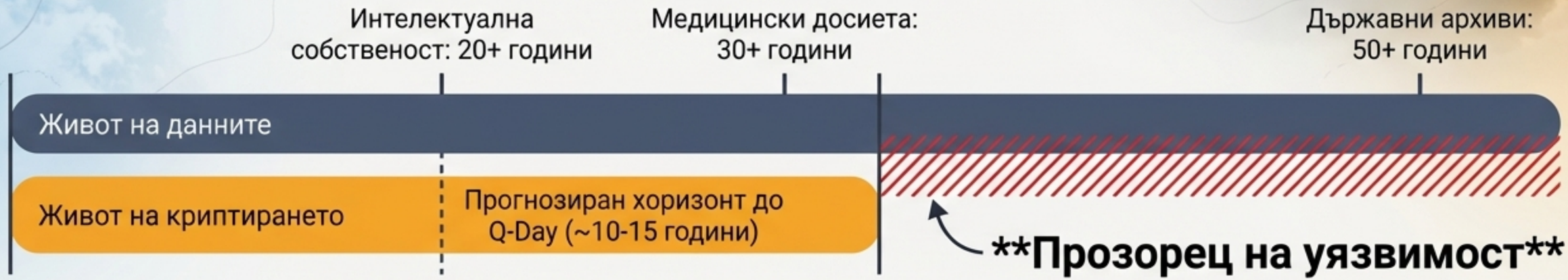
"Този модел на заплаха е една от основните причини, поради които преходът към пост-квантова криптография е спешен." - NIST, Transition to Post-Quantum Cryptography Standards

NotebookLM

Когато давността на данните надхвърля давността на криптирането

Компрометиране настъпва, ако Ld > На

Ld = изискван живот на тайната на данните
На = хоризонт за декриптиране на противника



Сектори с най-висока експозиция

- Финансови институции
- Правителствени агенции
- Отбранителна индустрия
- Здравеопазване
- Облачни доставчици

NotebookLM

Ефектът на доминото: Един пробив застрашава цялата национална инфраструктура

Енергийната мрежа е в основата на почти всички други критични сектори. Нейният срив би предизвикал верижни откази.



Здравеопазване
Отказ на животоподдържащи системи.

Транспорт
Отказ на системи за контрол на трафика.

Комуникации
Срив на телекомуникационни мрежи.

Водоснабдяване
Спиране на пречиствателни станции.

Финанси
Спиране на банкови операции и трансакции.

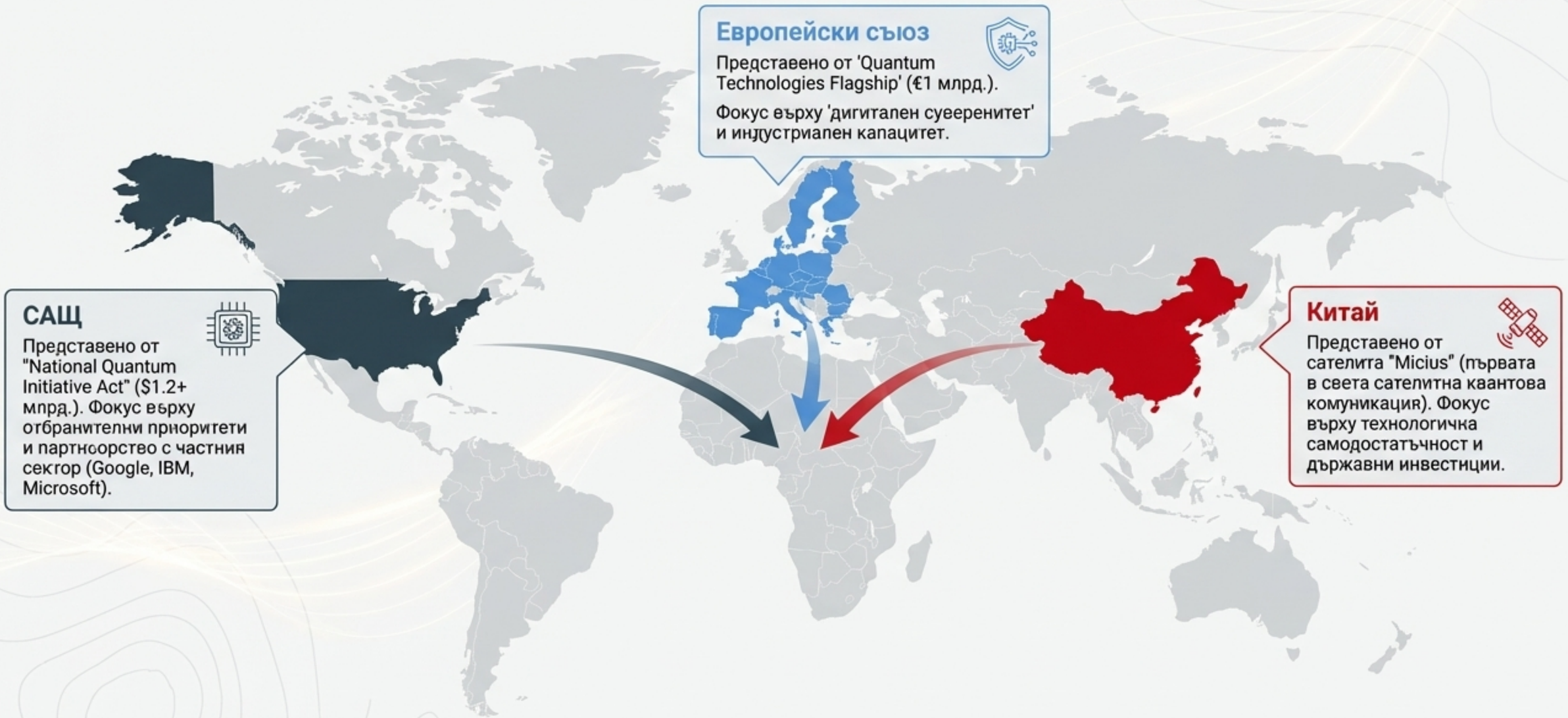
Спешни служби
Затруднена координация и реакция.

Базирано на анализа от 'QUANTUM COMPUTING THREATS TO ENERGY GI

NotebookLM

Глобалната надпревара: Нациите се мобилизират за квантовото бъдеще

Квантовите технологии се разглеждат като стратегически актив и лост за власт, което води до интензивна конкуренция между големите сили.



NotebookLM

Създаване на нов стандарт за сигурност: Отговорът на NIST

National Institute of Standards and Technology

Пост-квантовата криптография (PQC) се състои от алгоритми, които работят на *класически компютри*, но са проектирани да бъдат устойчиви както на класически, така и на квантови атаки.

PQC не изисква квантов хардуер за имплементация.

FIPS 203: ML-KEM (CRYSTALS-Kyber)



Предназначение: Установяване на ключове (Key Encapsulation). Замества RSA и ECC Diffie-Hellman.

Характеристики: Компактни ключове, висока производителност.

FIPS 204: ML-DSA (CRYSTALS-Dilithium)



Предназначение: Цифрови подписи (Digital Signatures).

Характеристики: Опростеност и устойчивост на атаки тип "side-channel".

FIPS 205: SLH-DSA (SPHINCS+)



Предназначение: Цифрови подписи.

Характеристики: По-консервативен, базиран на хеш-функции, осигуряващ дългосрочна сигурност.

NotebookLM

От препоръки към мандати: Правителствата налагат преход

Водещи световни агенции по сигурността вече са определили **конкретни срокове** и изисквания за миграция към PQC.

NSA: Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)

Изисква от правителствените и отбранителните системи да мигрират към PQC алгоритми. Краен срок за пълен преход: **2035 г.**

Белият дом: National Security Memorandum-10 (NSM-10)

Нарежда на всички федерални агенции на САЩ да направят инвентаризация на съществуващата криптография и да започнат планиране на прехода

CISA / NSA / NIST: Quantum Readiness Roadmap

Разширява насоките към критичната инфраструктура и частния сектор, като набляга на криптографската инвентаризация и координацията с доставчиците.

Готовността вече не е по избор, а е в ход.

NotebookLM

Strategic Editorial

Предизвикателството на миграцията: Процес, изискващ години, а не месеци

Миграцията към PQC е многогодишна програма. Повечето мащабни ИТ миграции (напр. към облачни услуги) отнемат **повече от 5 години** и изискват огромна координация.

- **Наследствени системи**: Криптографията е дълбоко вградена в хардуер, фърмуер и стари приложения, които трудно се обновяват.
- **Верига на доставки**: Дори ако една организация обнови своите системи, нейните партньори и доставчици може да изостават, създавайки слаби звена.
- **Неравномерна спешност**: Много организации признават риска, но чакат пътните карти на своите доставчици, преди да действат, което създава забавяния.
- **Скрити зависимости**: Криптографията често се крие в компилиран код, SDK на трети страни и API-та, които стандартните скенери пропускат.



NotebookLM

Вашата пътна карта за квантова готовност: Пет ключови стъпки



Инвентаризация

Открийте и каталогизирайте цялата криптография във вашата среда.

Приоритизация

Оценете риска въз основа на давността и стойността на данните.

Планиране

Разработете многогодишна пътна карта за миграция, включително хибридни подходи.

Изграждане

Проектирайте системи за криптографска гъвкавост (Crypto-Agility).

Координация

Работете с доставчици, партньори и регулатори.

NotebookLM

Strategic Editorial

Стъпки 1-3: Разберете, оценете и планирайте



1

Инвентаризация

Цел: Пълна видимост. Не можете да защитите това, което не виждате.

- Използвайте автоматизирани инструменти за сканиране, за да откриете всички криптографски активи: TLS, VPNs, PKI, фърмуер, API-та.
- Документирайте алгоритми, дължини на ключове, сертификати и техните собственици.



2

Приоритизация

Цел: Фокусирайте усилията там, където рискът е най-голям.

- Идентифицирайте данни с дълъг живот на тайната: интелектуална собственост, държавни архиви, биометрични данни, здравни досиета.
- Тези системи трябва да мигрират първи, за да се намали прозорецът на HNDL уязвимост.



3

Планиране

Цел: Създайте реалистична стратегия за преход.

- Разработете поетапен план за внедряване.
- Планирайте **хибридна криптография**: комбиниране на класически и PQC алгоритми, за да се осигури обратна съвместимост по време на прехода.
- Тествайте в пилотни среди.

NotebookLM

Стъпки 4-5: Изградете гъвкавост и координирайте екосистемата

4 Раздел 4: Изграждане на криптографска гъвкавост (Crypto-Agility)

> "Способността бързо да се изключи използването на слаби криптографски алгоритми, когато бъде открита уязвимост, и да се приемат нови, без значителни промени в инфраструктурата." - NIST

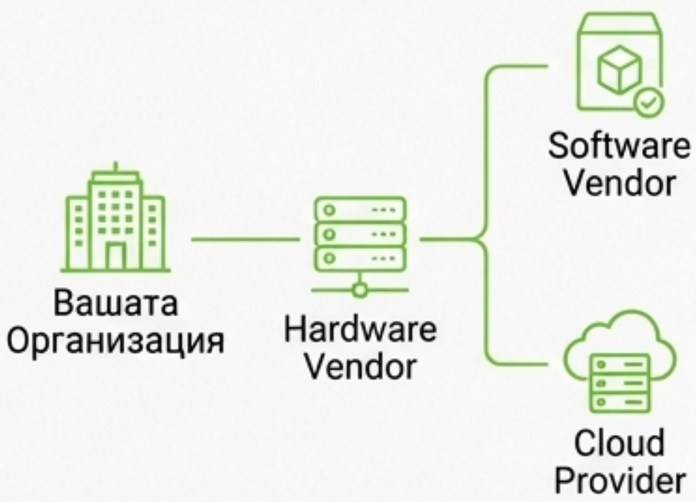
Как се постига:

- Избягвайте "hardcoded" криптографски имплементации.
- Използвайте конфигурационни файлове и API-та, които реферират към идентификатори на алгоритми.
- Проектирайте архитектури, които позволяват лесна смяна на криптографски библиотеки.

5 Раздел 5: Координация с екосистемата

Основна идея: Квантовата готовност не е проект на една организация.

- Изисквайте пътни карти за PQC от вашите доставчици на софтуер, хардуер и облачни услуги.
- Синхронизирайте плановете си за миграция с партньорите си.
- Следете регулаторните изисквания и стандарти във вашия сектор.



NotebookLM



Подготовката за бурята не е избор, а необходимост

1



Заплахата е настояще, не бъдеще: "Тихата жътва" (HNDL) се случва сега, докато данните все още са защитени с класическа криптография.

2



Хоризонтът е по-близо от очакваното: Прогнозите за Q-Day се изместват към края на това десетилетие, оставяйки **ограничен прозорец** за действие.

3



Решението е стандартизирано и достъпно: Пост-квантовата криптография (PQC) е готова за внедряване и има ясна подкрепа от глобални органи като **NIST**.

4



Пътят напред е ясен: Петстепенната пътна карта (Инвентаризация, Приоритизация, Планиране, Изграждане, Координация) осигурява структуриран подход за всяка организация.

Всяка криптирана информация, която защитим днес с PQC, е актив, който няма да се превърне в утрешен пробив. Проактивната миграция е единственият начин да се гарантира дългосрочната конфиденциалност в пост-квантовата ера.

NotebookLM