Czytaj lub słuchaj artykuł online

Zeskanuj kod QR, aby otworzyć artykuł na XO.PL

Źródło artykułu:

https://xo.pl/it-na-wesolo-data-encryption

DANE I ICH OCHRONA

Szyfrowanie danych, czyli sejf z instrukcją obsługi na drzwiach

Centralny Magazyn Dokumentów imienia Pana Kierownika ma nowe serwery, **RAID**, **backupy**, plan odzyskiwania i wyjątkowo odporną psychicznie księgową. Po pożarze, skasowanym dokumencie i przygodzie z zamrażarką kierownik postanawia ostatecznie zapewnić firmie bezpieczeństwo. Kupuje wielki sejf, trzy kłódki i ogłasza: „OD DZISIAJ SZYFRUJEMY WSZYSTKO!". Jest tylko jeden drobny problem. Po godzinie nawet on nie potrafi już niczego otworzyć. Witamy w świecie szyfrowania danych — czyli jak chronić informacje przed niepowołanymi osobami, nie zamykając ich jednocześnie przed samym sobą.

Rozdział pierwszy: sejf z instrukcją obsługi na drzwiach

— PANIE FRANKU! ZŁODZIEJE NIE DOSTANĄ NASZYCH DANYCH!
— To świetnie, panie kierowniku. Co pan zrobił?
— ZAMKNĄŁEM DYSK W SEJFIE!
— A klucz do sejfu?
— WISZĄCY NA DRZWIACH. ŻEBY NIKT NIE ZGUBIŁ!
— ...
— CO PAN TAK PATRZY?!
— Sejf ma chronić przed kimś, kto nie powinien go otworzyć.
— NO PRZECIEŻ JEST ZAMKNIĘTY!
— A instrukcja otwarcia wisi na zewnątrz.
— TO PROSZĘ ZASZYFROWAĆ INSTRUKCJĘ!

🤣🤣🤣

Szyfrowanie zamienia czytelną informację w postać, której nie powinno dać się zrozumieć bez odpowiedniego klucza. Tę nieczytelną postać nazywamy **szyfrogramem**. Proces odwrotny to **odszyfrowywanie**.

Szyfrowanie ma przede wszystkim chronić **poufność** danych. Może sprawić, że skradziony dysk będzie dla złodzieja zbiorem niezrozumiałych informacji, ale nie zatrzyma automatycznie usunięcia plików ani nie zastąpi **backupu**. Sama kłódka nie ugasi pożaru magazynu.

Rozdział drugi: szyfrowanie, kodowanie i hash — trzy różne rzeczy

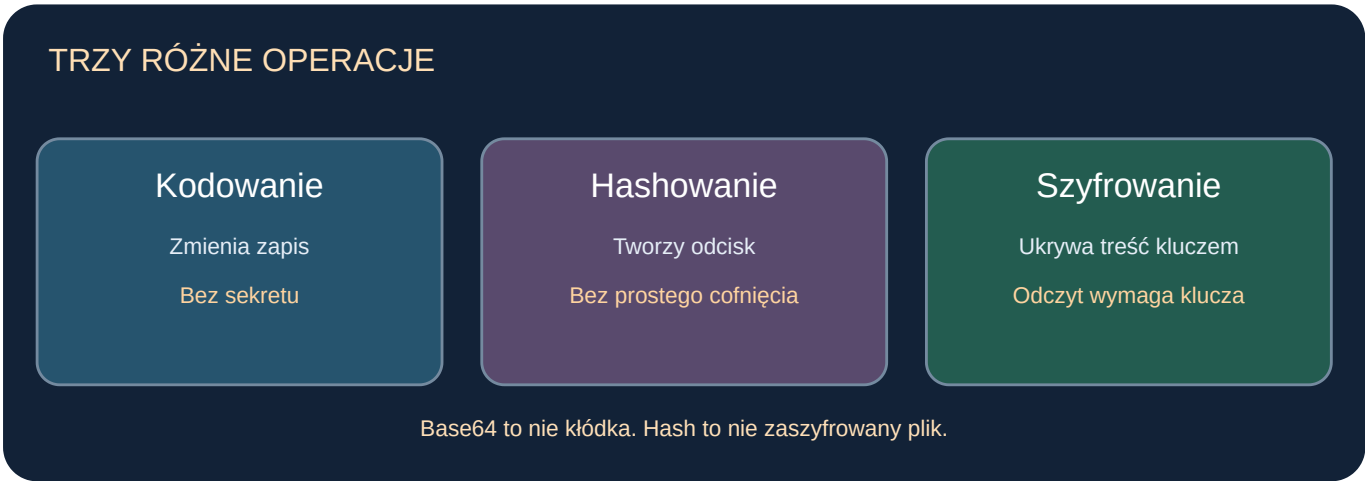
Na biurko Franka wpada kartka.

— PANIE FRANKU! ZASZYFROWAŁEM POUFNY DOKUMENT!
— Czym?
— BASE64!
— To kodowanie, nie szyfrowanie.
— ALE PRZECIEŻ LITERY WYGLĄDAJĄ JAK BEŁKOT!
— Każdy może je odkodować. Nie potrzeba żadnego sekretu.
— TO MOŻE HASH?!
— Hash służy do innych zastosowań. Nie jest sposobem przechowania dokumentu, który chcemy potem odszyfrować.
— CZYLI NIE KAŻDE NIEZROZUMIAŁE LITERY TO SZYFR?!
— Dokładnie.
— PANOWIE, INFORMATYKA ZNOWU UDOWADNIA, ŻE WYGLĄD BYWA MYLĄCY!

🤣🤣

Kodowanie, np. Base64, zmienia sposób zapisu danych, aby łatwiej je przesłać lub przechować w określonym formacie. Nie zapewnia tajności. **Hashowanie** oblicza zwykle krótki odcisk danych, wykorzystywany m.in. do sprawdzania integralności; z prawidłowej funkcji skrótu nie da się po prostu odwrócić operacji i odzyskać oryginalnego dokumentu. Hasła powinno się przechowywać przy użyciu specjalizowanych, wolnych funkcji haszujących z solą, takich jak Argon2id, a nie zwykłego szybkiego SHA-256.

Szyfrowanie natomiast ma umożliwiać odczyt osobie posiadającej właściwy klucz. Nie wszystko, co wygląda jak losowy ciąg znaków, jest bezpiecznie zaszyfrowane.



Rozdział trzeci: jeden klucz otwiera i zamyka

— PANIE FRANKU, PROSZĘ MI TO WYJAŚNIĆ PROSTO!
— Wyobraźmy sobie sejf, do którego używamy tego samego tajnego klucza, by zamknąć i otworzyć zawartość.
— TAKI ZWYKŁY SEJF?!
— Podobna idea. To szyfrowanie symetryczne.
— A CZY JEST SZYBKIE?!
— Bardzo. Dlatego doskonale nadaje się do dużych ilości danych.

— TO ZASZYFRUJMY CAŁY MAGAZYN!
— Możemy zaszyfrować jego dyski. Murów raczej nie trzeba.
— PROSZĘ NIE OGRANICZAĆ MOJEJ WIZJI!

🤣🤣

Szyfrowanie symetryczne wykorzystuje ten sam tajny klucz do szyfrowania i odszyfrowania albo klucze bezpośrednio od niego wywiedzione. Popularnym, sprawdzonym algorytmem jest **AES**, występujący między innymi w wersjach z kluczami 128-, 192- i 256-bitowymi. AES-256 nie oznacza, że hasło użytkownika musi mieć 256 znaków; klucz szyfrujący i hasło, z którego można go bezpiecznie wyprowadzić, to różne rzeczy.

Istotny jest także **tryb działania** i poprawna implementacja. Dla plików i wiadomości często stosuje się szyfrowanie uwierzytelnione, np. AES-GCM, które potrafi również wykryć nieuprawnioną zmianę szyfrogramu. Samo hasło „AES” na pudełku programu nie jest jeszcze gwarancją bezpieczeństwa.



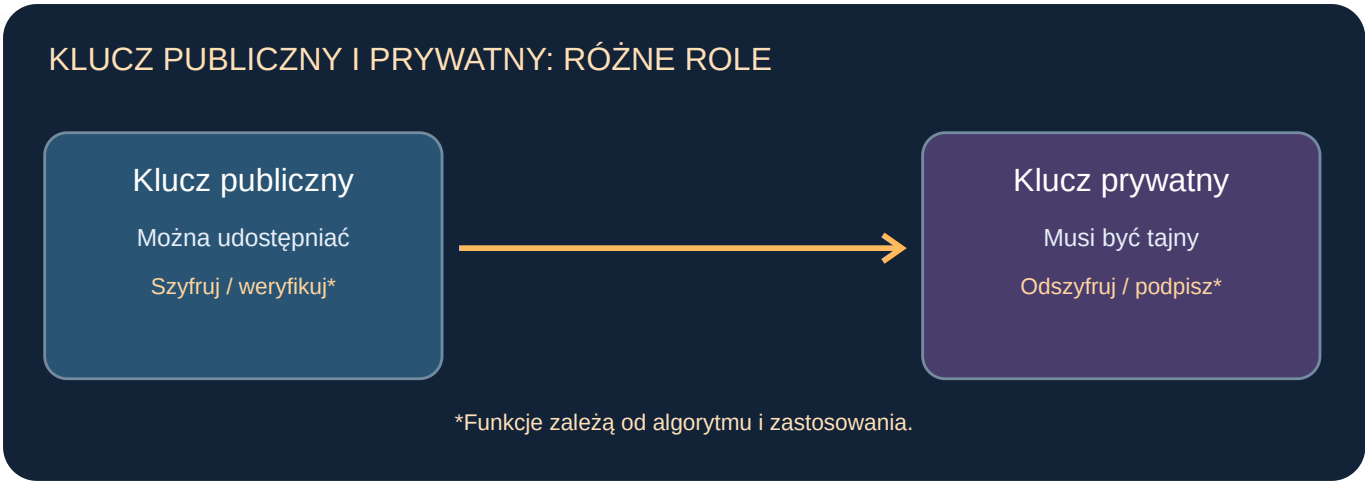
Rozdział czwarty: klucz publiczny, klucz prywatny i bardzo towarzyski kierownik

— PANIE FRANKU! MÓWI PAN, ŻE KLUCZ MA BYĆ TAJNY, A TERAZ JAKIŚ „PUBLICZNY”?!
— Istnieje też kryptografia asymetryczna. Ma parę powiązanych kluczy: publiczny i prywatny.
— CZYLI JEDEN ROZDAJĘ WSZYSTKIM?!
— Publiczny można udostępniać.
— A PRYWATNY?!
— Chronimy.
— TO MOŻE PRYWATNY WYŚLĘ PRACOWNIKOM Z NAPISEM „TAJNE”?!
— Nie, bo przestanie być tajny.
— ALE NAPIS BĘDZIE WIELKIMI LITERAMI!

🤣🤣

W wielu systemach **klucz publiczny** może służyć do zaszyfrowania sekretu dla właściciela odpowiadającego mu **klucza prywatnego**. W innych zastosowaniach, np. podpisach cyfrowych, role są inne: kluczem prywatnym podpisuje się dane, a publicznym weryfikuje podpis. Nie każdy algorytm asymetryczny służy do wszystkiego.

Na przykład **RSA** może być używany w określonych schematach szyfrowania i podpisów, **ECDSA** służy do podpisów, a **ECDH** do uzgadniania wspólnego sekretu. Nazwy bywają podobne, zadania różne.



Rozdział piąty: dlaczego szyfrowanie łączy oba światy?

— PANIE FRANKU, TO KTÓRE SZYFROWANIE JEST LEPSZE?!
— Zależy do czego. Symetryczne jest wydajne przy dużych plikach. Asymetryczne pomaga bezpiecznie uzgodnić lub przekazać klucze i uwierzytelnić strony, zależnie od protokołu.
— TO PROSZĘ ZROBIĆ Z OBU JEDEN!
— W praktyce często właśnie tak działają nowoczesne systemy.
— WIDZI PAN?! ZNOWU MIAŁEM RACJĘ!
— Pan kierownik właśnie odkrył szyfrowanie hybrydowe.
— PROSZĘ WPISAĆ DO PROTOKOŁU: „WYNALAZŁEM INTERNET”!

🤣🤣

W praktyce wiele narzędzi łączy obie rodziny kryptografii. Dane szyfruje się wydajnym algorytmem symetrycznym, a kryptografia asymetryczna pomaga uzgodnić lub zabezpieczyć klucze oraz potwierdzić tożsamość. Przykładem takiego połączenia są współczesne połączenia **TLS**, używane przez **HTTPS**.

Ważny szczegół: **HTTPS nie oznacza, że cały serwer jest zaszyfrowany**. Chroni transmisję między właściwie uwierzytelnionymi punktami połączenia. Treść może być jawna po odszyfrowaniu na serwerze lub urządzeniu użytkownika. Szczegóły **certyfikatów** i uwierzytelniania opisujemy osobno w **artykule o certyfikatach**, a samo **HTTP** i **HTTPS** w **osobnym rozdziale**.

Rozdział szósty: szyfrowanie dysku to nie to samo co szyfrowanie pliku

— PANIE FRANKU! ZASZYFROWAŁEM DYSK I TERAZ NIKT NIE ZOBACZY MOICH DOKUMENTÓW!
— Jeśli dysk zostanie skradziony w stanie wyłączonym i jest prawidłowo zabezpieczony, to duża zaleta.
— A KIEDY KOMPUTER PRACUJE?!
— Po odblokowaniu uprawnione programy i użytkownicy widzą dane. Złośliwe oprogramowanie działające z odpowiednimi uprawnieniami może też mieć do nich dostęp.
— TO JA GO NIE BĘDĘ WŁĄCZAŁ!
— Wtedy rzeczywiście nikt nie popracuje.
— BEZPIECZEŃSTWO PRZEDE WSZYSTKIM!

🤣🤣

Szyfrowanie całego dysku, np. BitLocker, **FileVault** czy LUKS/dm-crypt, chroni dane spoczywające na nośniku, zwłaszcza po utracie wyłączonego urządzenia. Po odblokowaniu system korzysta z plików normalnie — dlatego nie jest to ochrona przed wszystkimi zagrożeniami podczas pracy.

Szyfrowanie pojedynczego pliku lub archiwum pozwala chronić konkretny zestaw danych, np. kopię wysyłaną do chmury. **Szyfrowanie transmisji** zabezpiecza informacje w drodze przez sieć. W każdym przypadku trzeba wiedzieć, *co* jest chronione, *kiedy* oraz przed *kim*. Żaden z tych mechanizmów sam nie zapewnia pełnego bezpieczeństwa danych.

Rozdział siódmy: hasło przyklejone do dysku

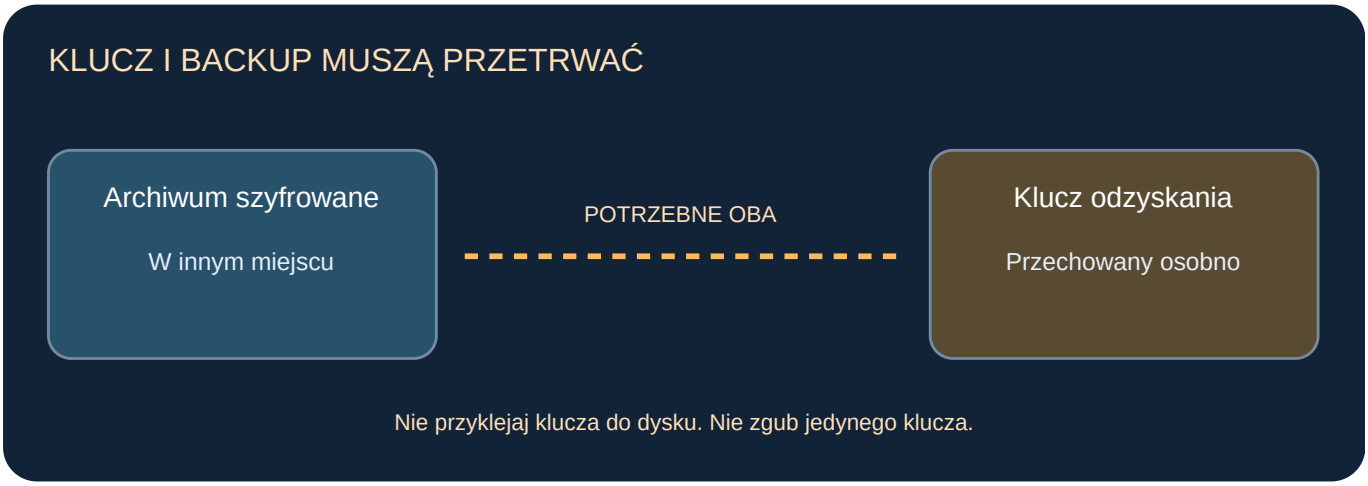
Księgowa wchodzi z dyskiem spod skarpetek.

— Panie kierowniku, zaszyfrowałam archiwum.
— DOSKONALE! A HASŁO?!
— Jest zabezpieczone osobno.
— JAK TO OSOBNO?! JA SWOJE PRZYKLEIŁEM DO DYSKU!
— To może pomóc złodziejowi.
— TO JE ODKLEJĘ!
— I gdzie pan je przechowa?
— W GŁOWIE!
— A kopia awaryjna?
— PANOWIE, NIE KAŻCIE MI ROBIĆ **BACKUPU** MOJEJ GŁOWY!

🤣🤣🤣

Klucz szyfrujący, hasło i sposób odzyskania dostępu wymagają planu równie mocno jak sama kopia danych. Długie, unikalne hasła i bezpieczne mechanizmy wyprowadzania kluczy pomagają chronić pliki. Przy szczególnie ważnych danych konieczna jest również niezależna metoda odzyskania kluczy.

Hasło zapisane na papierze nie jest automatycznie złym rozwiązaniem. Odpowiednio zabezpieczona kartka przechowywana oddzielnie od nośnika może być sensowną kopią awaryjną. Przyklejenie hasła do tego samego zaszyfrowanego dysku to już inna historia. Równie ryzykowne jest posiadanie jednego klucza, którego nikt nie będzie potrafił odzyskać.



Rozdział ósmy: kierownik szyfruje hasło do hasła

— PANIE FRANKU! ZNALAZŁEM IDEALNY SYSTEM!
— Jaki?
— HASŁO DO **BACKUPU** PRZECHOWUJĘ W ZASZYFROWANYM PLIKU!
— Dobrze. A czym go odszyfrujemy?
— DRUGIM HASŁEM!
— Gdzie ono jest?
— W DRUGIM ZASZYFROWANYM PLIKU!
— A hasło do drugiego?
— W TRZECIM!
— A gdzie kończy się ten łańcuch?
— ...
— Panie kierowniku?
— PROSZĘ MI NIE PSUĆ NIESKOŃCZONOŚCI PYTANIAMI!

🤣🤣

Zabezpieczenia powinny mieć **realną procedurę awaryjnego odzyskania**. Menedżer haseł, awaryjne klucze, osobno przechowywane dane dostępowe, kontrola dostępu kilku upoważnionych osób czy zabezpieczona koperta mogą być elementami planu. Ważne, żeby w razie utraty telefonu, awarii menedżera lub niedostępności konkretnej osoby istniała niezależna droga dostępu.

Nie oznacza to, że każdy pracownik powinien znać klucz. Wprost przeciwnie: **dostęp otrzymują tylko osoby, które rzeczywiście go potrzebują**, a sytuacje awaryjne są przemyślane i przetestowane. Żaden system nie zyskuje na tym, że jest tak skomplikowany, iż nikt nie umie go obsłużyć.

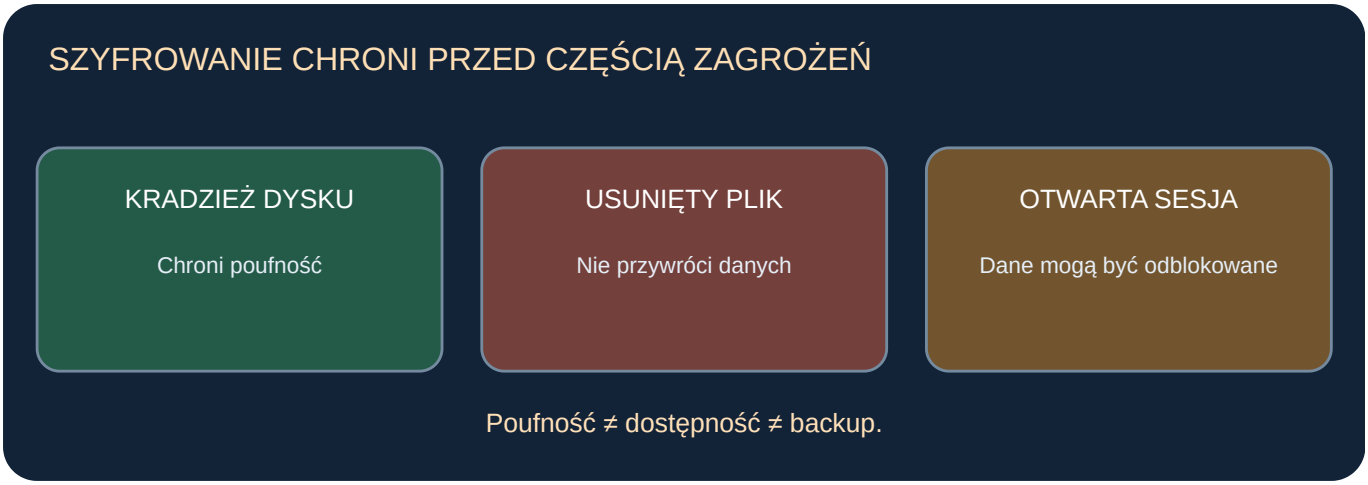
Rozdział dziewiąty: kłódka nie obroni przed młotkiem

— PANIE FRANKU! NASZ DYSK JEST ZASZYFROWANY! JEST NIEZNISZCZALNY!
— Nie, panie kierowniku.
— JAK TO NIE?!
— Szyfrowanie nie naprawia sprzętu, nie powstrzymuje pożaru i nie przywraca usuniętych plików.
— A RANSOMWARE?!
— Może zaszyfrować lub usunąć dane, do których system ma dostęp, nawet jeżeli sam dysk jest już szyfrowany.
— CZYLI MOGĘ MIEĆ ZASZYFROWANY ZASZYFROWANY DYSK?!
— Tak. I nadal nie mieć dokumentów.
— TO JEST JAKIŚ SEJF W SEJFIE, KTÓREGO NIE MA!

🤣🤣

Poufność mówi, kto może przeczytać dane. **Integralność** — czy dane nie zostały nieuprawnienie zmienione. **Dostępność** — czy można z nich skorzystać wtedy, gdy są potrzebne. To różne cele. Szyfrowanie pomaga przede wszystkim w poufności, a odpowiednie mechanizmy uwierzytelnienia danych mogą także wykrywać manipulacje. Nie zapewnia samoistnie dostępności ani odzyskiwania po awarii.

Właśnie dlatego **backup** nadal jest konieczny, a **odzyskiwanie danych** pozostaje osobnym zagadnieniem. Szyfrowanie i **backup** nie rywalizują ze sobą — rozwiązują różne problemy.



Rozdział dziesiąty: napastnik nie musi łamać AES

— PANIE FRANKU! UŻYWAMY AES-256! NIKT NAM NIC NIE ZROBI!
— A administrator ma hasło „123456”?
— ...
— A komputer pozostaje zalogowany i odblokowany?
— ...
— A ktoś podsunął pracownikowi fałszywy ekran logowania?
— ...
— Panie kierowniku?
— PROSZĘ NATYCHMIAST ZMIENIĆ WSZYSTKIM HASŁO NA „AES256”!

🤣🤣

W prawdziwym świecie przestępca często nie próbuje matematycznie złamać silnego algorytmu. Prościej ukraść hasło, przejąć konto, wykorzystać błąd programu, podmienić instalator, wykorzystać zbyt szerokie uprawnienia albo odczytać pliki, gdy komputer jest już odblokowany.

Dlatego szyfrowanie uzupełniamy m.in. aktualizacjami, silnym uwierzytelnianiem, rozsądnymi uprawnieniami, zabezpieczeniem urządzeń, ochroną kluczy i przemyślaną konfiguracją. **Bezpieczeństwo całego systemu nie jest równe nazwie algorytmu w ustawieniach.**

Rozdział jedenasty: czy da się obiecać szyfr na zawsze?

— PANOWIE! CHCĘ SZYFROWANIE ODPORNE NA WSZYSTKO PRZEZ NASTĘPNE STO LAT!
— Nie da się uczciwie zagwarantować absolutnego bezpieczeństwa na zawsze.
— NAWET JAK ZAPŁACĘ WIĘCEJ?!
— Nawet wtedy. Zmieniają się techniki ataku, oprogramowanie i możliwości obliczeniowe.
— A KOMPUTERY KWANTOWE?!
— Mogą w przyszłości poważnie zagrozić części dzisiejszych metod kryptografii klucza publicznego.
— CZYLI JUTRO ZŁAMIĄ NAM WSZYSTKIE DYSKI?!
— Nie. To nie działa w ten sposób.
— PANIE FRANKU, JA JUŻ NIE WIEM, CZY BAĆ SIĘ ZŁODZIEJA, CZY FIZYKA!

🤣🤣

Wystarczająco zaawansowany komputer kwantowy mógłby podważyć bezpieczeństwo szeroko używanych rozwiązań opartych na RSA i kryptografii krzywych eliptycznych. Dlatego rozwijane i wdrażane są **algorytmy postkwantowe** do odpowiednich zastosowań. Nie oznacza to, że obecne komputery kwantowe potrafią dziś rutynowo odszyfrowywać zabezpieczone dane firmowe.

AES-256 nie jest zagrożony w ten sam sposób co RSA czy ECC. Znane ataki kwantowe na symetryczne szyfrowanie mają inny charakter, a poprawnie użyty AES-256 pozostaje silnym wyborem. W praktyce trzeba patrzeć także na sposób wyprowadzenia klucza z hasła, błędy implementacji, przechowywanie sekretów i to, jak długo dane muszą pozostać poufne.

Rozdział dwunasty: backup zaszyfrowany tak skutecznie, że nikt go nie otworzy

— PANIE KIEROWNIKU! MAMY TRZY KOPIE ARCHIWUM!
— WSPANIALE!
— WSZYSTKIE ZASZYFROWANE!
— JESZCZE LEPIEJ!
— ALE NIKT NIE MA KLUCZA ODZYSKIWANIA!
— ...
— ...
— A CZY NIE MOŻNA ODZYSKAĆ KLUCZA Z **BACKUPU**?!
— **Backup** też jest nim zaszyfrowany.
— TO POPROSZĘ MNIE NIE INFORMOWAĆ O TAKICH SZCZEGÓŁACH!

🤣🤣🤣

Jeśli szyfrujemy **kopie zapasowe**, musimy zadbać o **przechowanie kluczy, ich niezależną kopię awaryjną oraz przetestowanie odszyfrowania**. Inaczej możemy mieć wiele identycznie nieczytelnych archiwów. Z drugiej strony nie zostawiamy kluczy obok dysku w miejscu dostępnym dla złodzieja.

Rozsądnym podejściem może być szyfrowanie archiwów **przed wysłaniem do chmury**, przy zachowaniu oddzielnych uprawnień i kopii odzyskiwania. Trzeba jednak pamiętać, że szyfrowanie nie chroni samoistnie przed usunięciem lub nadpisaniem archiwów: do tego potrzebne są retencja, niezależne dostępy i inne warstwy **backupu**.

Rozdział trzynasty: podpis cyfrowy i pieczątka kierownika

— PANIE FRANKU! PODPISAŁEM DOKUMENT CYFROWO!
— Doskonale.
— TO TERAZ NIKT GO NIE PRZECZYTA!
— Podpis cyfrowy nie służy do ukrywania treści.
— TO PO CO JEST?!
— Pomaga potwierdzić, kto podpisał dane i czy ich treść została zmieniona. Weryfikacja wymaga też zaufania do odpowiednich kluczy lub **certyfikatów**.
— CZYLI MOGĘ PODPISAĆ JAWNY DOKUMENT?!
— Oczywiście.
— TO PO CO MI PIECZĄTKA „ŚCIŚLE TAJNE”?!

🤣🤣

Podpis cyfrowy nie jest tym samym co szyfrowanie. Umożliwia sprawdzenie autentyczności podpisu i integralności podpisanych danych w kontekście zaufania do klucza. **Hash** też może pomagać wykrywać zmiany, ale sam zwykły hash dołączony do pliku nie potwierdza, kto go stworzył — napastnik mógłby podmienić plik i obliczyć nowy skrót.

Możemy więc mieć dokument jawny i podpisany, dokument tajny i niepodpisany, albo dokument jednocześnie zaszyfrowany i podpisany. Inne zadanie, inne narzędzie.

Rozdział czternasty: instrukcja bezpieczeństwa dla zwykłego człowieka

Na tablicy w magazynie pojawiają się cztery pytania:

1. Co chronimy? Zdjęcia, dokumenty, dane osobowe, laptop, archiwum czy transmisję?

2. Przed kim i przed czym? Kradzieżą dysku, podejrzeniem danych w sieci, przypadkowym odczytem, przejęciem konta czy utratą nośnika?

3. Kto ma mieć dostęp? Właściciel, kilku administratorów, konkretni pracownicy, a może tylko upoważniony odbiorca pliku?

4. Jak odzyskamy dostęp? Co zrobimy po utracie hasła, telefonu lub klucza? Czy potrafimy przywrócić i odszyfrować **backup**?

— PANIE FRANKU! A NIE MA JEDNEGO PRZYCISKU „BEZPIECZNIE”?!
— Nie, ale można przygotować prostą procedurę dopasowaną do potrzeb.
— I NIE MUSIMY BUDOWAĆ FORT KNOX?!
— Nie. Trzeba zachować proporcje i zdrowy rozsądek.
— TO JEST PIERWSZA DOBRA WIADOMOŚĆ W TYM TYGODNIU!

🤣🤣

Dla domowego użytkownika dobrym początkiem bywa szyfrowanie laptopa, blokada ekranu, mocne hasła, aktualizacje i oddzielnie zabezpieczone kopie najważniejszych plików. Firma powinna dopasować rozwiązania do rodzaju danych, obowiązków prawnych i realnych zagrożeń. Zabezpieczenie tak skomplikowane, że nikt nie umie go obsłużyć ani odzyskać, nie jest dobrym zabezpieczeniem.

Finał: najbezpieczniejszy magazyn na świecie

W magazynie odbywa się uroczyste otwarcie nowego sejfu.

— PANOWIE! MAMY SZYFROWANE DYSKI!
— Tak.
— ZASZYFROWANE **BACKUPY** W INNYCH MIEJSCACH!
— Tak.
— OSOBNO ZABEZPIECZONE KLUCZE!
— Zgadza się.
— I SPRAWDZILIŚMY, CZY POTRAFIMY JE ODSZYFROWAĆ?!
— Wczoraj. Udało się.
— WSPANIALE! TO TERAZ OTWIERAMY SEJF!

Kierownik wyciąga klucz. Podchodzi do drzwi. Zatrzymuje się.

— PANIE FRANKU...
— Tak?
— KTOŚ ZASZYFROWAŁ MI ZAMEK?!
— Nie. Włożył pan klucz odwrotnie.
— ...
— ...
— PROSZĘ TEGO NIE WPISYWAĆ DO RAPORTU!

🤣🤣🤣🤣

Zapamiętaj: szyfrowanie pomaga chronić tajemnice, ale nie zatrzymuje wszystkich awarii i nie zastępuje **backupu**. Silny algorytm potrzebuje poprawnego wdrożenia, dobrze chronionych kluczy oraz możliwości ich odzyskania. **Najlepszy szyfr to taki, który powstrzymuje niepowołanych — nie właściciela danych.**

Dyrekcja Centralnego Magazynu Dokumentów informuje: sejf został otwarty bez udziału komputerów kwantowych. Księgowa odmówiła przechowywania klucza pod skarpetkami. Tym razem.