Bezpieczeństwo transakcji w gospodarce cyfrowej

dr Zbigniew Jakubowski

Zbigniew.Jakubowski@Compendium.pl

1

2

AGENDA

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." ...

Edward Snowden

4

Agenda

- Wprowadzenie
- Ochrona informacji podstawą działania firmy i bezpieczeństwa transakcji
- Aktualna sytuacja na rynku bezpieczeństwa
  - Cyberprzestępczość dobrze zorganizowana
  - Pandemia czyli wszystko na szybko, byle działało…
- Techniczne aspekty ochrony transakcji biznesowych
- Socjotechnika jako najskuteczniejsza metoda zdobywania danych i środków
- Odpowiedzialność kierownictwa za budowanie świadomości bezpieczeństwa
- Podsumowanie

5

5

WPROWADZENIE

6

6

Wprowadzenie

- Do końca lat 90 ubiegłego stulecia kodyfikacja norm bezpieczeństwa nie miała wspólnego mianownika – biznes nie może żyć bez norm
- Pierwszym ważnym dokumentem było pojawienie się RFC 2196
- Norma jednak ograniczała się głównie do operacji ochrony sieciowych i IT
- Przełomem była norma BS-7799 wydana przez BSI (ang. British Standard Institute) gdzie, po raz pierwszy zdefiniowano ochronę informacji jako cel nadrzędny, a nie tylko systemów sieciowych czy IT
- Musimy zrozumieć, że podstawą transakcji w cyberprzestrzeni jest bezpieczna wymiana informacji – dotyczy to wszystkich praktycznie usług, z których nagminnie korzystamy od telefonów GSM, poprzez zakupy przez Internet do kart płatniczych

7

7

AKTUALNA SYTUACJA NA RYNKU BEZPIECZEŃSTWA

8

Aktualna sytuacja na rynku bezpieczeństwa

- Decydującym zagrożeniem jest cyberprzestępczość – stare śpiewki typu script-kiddie, czy niezadowoleni pracownicy to tylko mały procent zagrożenia
- Kwota okupów ransomware znacznie wzrosła – ostatnie raporty to 7-9 BC czyli około 0.5 mln PLN
- Analiza kodu najnowszego "ransomware" i portfeli BC wskazuje na Iran, co może oznaczać, że agendy rządowe są zaangażowane w proces tworzenia kodu
- Polska jest w czołówce krajów najgorzej chroniących swoje dane i usługi. Przodujemy - Polska, Bułgaria, Meksyk, Indonezja oraz na Ukraina to czołówka rankingu. *Źródło: onet.pl.*
- Powody – znajdźmy sami we własnych decyzjach kadrowych i sprzętowych…

9

OCHRONA INFORMACJI PODSTAWĄ DZIAŁANIA FIRMY I BEZPIECZEŃSTWA TRANSAKCJI

10

Cechy informacji przydatnej w biznesie

- *Poufność* - oznacza, że informacja może być poprawnie odczytana jedynie przez upoważnione osoby (lub programy).
- *Autentyczność* - oznacza, że informacja może (mogła) być wygenerowana jedynie przez upoważnione osoby w sposób dający się później poprawnie odczytać.
- Dodatkowym mechanizmem pozwalającym chronić nasze dane jest *integralność* oznaczająca że informacja nie uległa zmianie w czasie przekazu. Jednak nie gwarantuje nam ona autentyczności jej nadawcy.
- *Niepodważalność* dokonanych zmian lub transakcji.

 11

11

Ochrona informacji podstawą działania biznesu

- Podstawą współczesnych transakcji jest wymiana informacji
- Cyfrowe waluty takie jak BitCoin opierają się o istnienie rozproszonej "księgi głównej", w której rejestrowane są transakcje – nie ma fizycznie czegoś takiego jak wypłata fizyczna w BitCoin
- Ochrona informacji jest więc podstawą bezpieczeństwa w cyberprzestrzeni
- Dotyczy to nie tylko wprost informacji o transakcjach biznesowych, ale również informacji, których znaczenia nie doceniamy
- Składanie informacji ze strzępków nie jest niczym nowym i w wywiadzie wojskowym USA ma nawet swoją nazwę – EEFI (ang. Essential Elements of Friendly Information)
- Prywatność i anonimowość w Internecie to nie jest bułka z masłem…

 12

12

TECHNICZNE ASPEKTY OCHRONY TRANSAKCJI BIZNESOWYCH

 13

13

Kryptografia – podstawowe narzędzie ochrony informacji

- Transakcje biznesowe dziś to tylko wymiana informacji – wymiana gotówki praktycznie nie istnieje
- Kryptografia odpowiednio zastosowana pozwala na zapewnie wszystkich cech dobrej informacji/transakcji dokonywanych przez biznes
- Kryptografia niestety wymaga dobrej implementacji ponieważ w przeciwnym razie daje nam tylko poczucie fałszywego bezpieczeństwa
- Dwa systemy kryptograficzne – szyfrowanie symetryczne i kryptografia klucza publicznego – szczegóły wychodzą znacznie poza ramy czasowe i programowe niniejszego wystąpienia
- Magiczne sformułowania RODO o doborze właściwej siły algorytmów kryptograficznych wiele tu nie pomagają…

14

Kryptografia – podstawowe narzędzie ochrony informacji

- Kryptografia ze względu na to, że mamy dużą różnicę w wydajności szyfrowania symetryczne i asymetrycznego, nawet 1:1000, jest wdrażana jako rozwiązanie hybrydowe
- Negocjacja kluczy szyfrowych odbywa się pod ochroną silnej kryptografii asymetrycznej a sama informacja jest szyfrowana szybkimi algorytmami symetrycznymi
- Protokoły wykorzystujące taki schemat to powszechnie znany IPSec czy SSL/TLS
- W kryptografii chroni nas nie tajność algorytmu, ale “workload” czyli nakład pracy konieczny do znalezienia klucza

15

Komponenty NSA Suite B

- Advanced Encryption Standard (AES) z kluczami 128 i 256 bits.
- AES w trybie Counter Mode (CTR) dla ruchu o niskiej przepustowości
- Tryb Galois/Counter Mode (GCM) dla zastosowań szerokopasmowych
- Elliptic Curve Digital Signature Algorithm (ECDSA) — podpis cyfrowy
- Elliptic Curve Diffie–Hellman (ECDH) — negocjacja kluczy DH v 2
- Secure Hash Algorithm 2 (SHA-256 and SHA-384) — funkcja skrótu kryptograficznego

16

Zalecane przez NIST długości kluczy

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

17

Porównanie kosztów Diffie-Hellman i krzywych eliptycznych

Security Level (bits)	Ratio of DH Cost : EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

RSA na sterydach…

18

SOCJOTECHNIKA JAKO NAJSKUTECZNIEJSZA METODA ZDOBYWANIA DANYCH I ŚRODKÓW

19

Atak socjotechniczny

- Atak socjotechniczny jest wymierzony w podstawowe relacje i zależności międzyludzkie.
- Jest to najbardziej niebezpieczna forma ataku na bezpieczeństwo, gdyż nie ma możliwości systemowego lub sprzętowego zabezpieczenia i uchronienia się od takiego działania.

20

Rzeczywistość

- Inwestujemy duże pieniądze w systemy zabezpieczeń i ich utrzymanie
- Pracownik jako istotny zasób Firmy
- Może nas pokonać pojedyncza osoba bez pojęcia o rzeczywistości – tak zaczyna się atak na Firmę
- Często padamy ofiarą "social engineering" – to ludzkie. Jeśli ktoś rozrzuci nowe klucze USB nie mamy problemu, a co jak klucz USB będzie miał przypięty pęk kluczy i nosił ślady zużycia???
- W polskich firmach budowanie świadomości pracowników jest zastąpione często batem lub pałką. Pytanie – czy chcemy tą rzeczywistość kontynuować?

21

Socjotechnika to nie tylko rozmowa…

- Phishing
- Spear Phishing
- Vishing
- Scam
- BEC – Business E-mail Compromise
- "Deep fake" – podrabianie głosu sztuczną inteligencją

22

ODPOWIEDZIALNOŚĆ KIEROWNICTWA ZA BUDOWANIE ŚWIADOMOŚCI BEZPIECZEŃSTWA

23

Odpowiedzialność kierownictwa za budowanie świadomości bezpieczeństwa

- Zarząd firmy ma podstawową rolę w budowaniu świadomości bezpieczeństwa pracowników firmy
- Świadomość pracowników to dodatkowy element bezpieczeństwa firmy i chyba jedyny, który skutecznie chroni przed socjotechniką
- Nie jest dopuszczalne wręczenie pracownikowi dokumentów bezpieczeństwa i żądanie podpisania deklaracji, że się z nimi zapoznał
- Zawsze niezależnie z której normy bezpieczeństwa korzystamy zasada jest prosta – najpierw szkolę, potem wymagam

24

PODSUMOWANIE

25

Podsumowanie

- Myśl co robisz
- Żadnych szybkich decyzji
- Nigdzie nie zostawiaj swoich danych jeśli nie musisz z powodów prawnych
- Stosuj dobrą kryptografię
- Pamiętaj o korelacji danych
- Chroń swoją prywatność fizycznie
- Pamiętaj o konsekwencjach swoich działań

26

Dziękuję za uwagę

Pytania?

Zbigniew.Jakubowski@Compendium.pl

27