Dokumentacja projektowa

2022/2023

Zarządzanie systemami informatycznymi

Zagrożenia oraz metody ochrony danych w systemach informatycznych

Kierunek: Informatyka

Członkowie zespołu:
Zofia Sitek
Emilia Pawela
Wojtek Olech

Gliwice, 2022/2023

Spis treści

1 Wprowadzenie

1.1 Role w projekcie

W niniejszym projekcie Zofia zajęła się wyszukaniem oraz przedstawieniem zagrożeń systemów informatycznych, sposobów wyłudzeń danych. Emilia opracowała temat z zakresu ochrony systemów informatyczny, ochrony danych osoby prywatnej oraz firmy. Wojtek pochylił się nad tematem szyfrowania danych oraz ich rodzaju. Również zajął się montażem filmu dotyczącego wyłudzania danych. Dokumentacja została stworzona wspólnie.

1.2 Cel projektu

Przybliżenie tematu zagrożeń oraz metod ochrony danych w systemach informatycznych. Przedstawienie przykładowych zagrożeń na które może natknąć się potencjalny użytkownik w Internecie. Ukazanie popularnych sposobów wyłudzeń danych. Prezentacja sposobów obrony przed potencjalnymi wyłudzeniami oraz przedstawienie jak można chronić swoje dane, oraz urządzenia które je magazynują. Zapoznanie z sposobami ochrony danych przez firmy. Również przybliżenie tematu szyfrowań danych, oraz przedstawienie przykładowych szyfrowań.

2 Założenia projektowe

2.1 Założenia techniczne i nietechniczne

- Metody ochrony danych dla osób prywatnych
- Metdoy ochrony danych dla przedsiębiorstw
- Autoryzacja, uwierzytelnienie, identyfikacja

2.2 Stos technologiczny w ochornie danych

- Nośniki danych (np. dyski SSD, serwery NAS)
- Uwierzytelnienie dwuskładnikowe (np. telefon, laptop, pendive)
- Szyforwanie dysku (np. BitLocker, VeraCrypt)

3 Realizacja projektu

3.1 ZOSIA

3.2 Identyfikacja, uwierzytelenie, autoryzacja

- Identyfikacja to wskazanie tożsamości danej osoby.
- Uwierzytelnianie to weryfikacja tożsamości przypisywanej danej osobie w procesie identyfikacji, na przykład poprzez system loginu i hasła, odcisk palca czy biometrię behawioralną.
- Autoryzacja to z kolei zagwarantowanie użytkownikowi, programowi lub procesowi odpowiednich uprawnień do korzystania z danych zasobów, jeśli uwierzytelnienie przeszło pomyślnie.

Uwierzytelnianie wieloskładnikowe, nazywane też MFA, to mechanizm, który pozwala użytkownikowi zwiększyć bezpieczeństwo procesu logowania, w którym do weryfikacji użytkownika stosuje się więcej niż jeden składnik uwierzytelniania, a w cyfrowym świecie najczęściej dotyczy połączenia systemu loginów i haseł z tokenami SMS czy z biometrią behawioralną. Oprócz kodów, można korzystać także z fizycznych kluczy bezpieczeństwa, które podłącza się do portu USB.

Obecnie w większości popularnych serwisów można włączyć dwuetapową weryfikację, np.: Google, Gmail, Allegro, Facebook, Twitter, LinkedIn, WhatsApp, Dropbox.

Podsumowując autoryzacja jest więc finalnym celem procesu identyfikacji, a uwierzytelnianie ma za zadanie zweryfikować, jakie uprawnienia powinien uzyskać dany użytkownik.

3.3 Kopia zapasowa

Robienie kopi zapasowej jest bardzo ważne, ponieważ przy uszkodzeniu nośnika, na którym są dane są zapisane, można je odtworzyć i nie tracić uzyskanych postępów. Przykładowe nośniki, na których można robić kopie zapasową to:

- pendrive
- dysk SSD, HDD
- serwer NAS – kilka dysków które tworzą serwer

Ważne, aby nośniki które mają mieć kopie zapasową nie były cały czas podpięte do właściwego urządzenia, ponieważ również mogą ulec awarii. Najlepiej, aby kopia znajdowała się w innej lokalizacji, aby uniknąć uszkodzenia np. Podczas pożaru, zalaniu pomieszczenia.

3.4 Zabezpieczenie dostępu do danych

Napopularniejszym zabepieczeniem danych jest hasło. Ważne żeby było ono silne, aby uniknąć nie powołanego dostępu do danych. Silne hasło zawiera:

- Co najmniej 6 znaków (im więcej znaków, tym silniejsze hasło)
- Zawiera kombinację liter, cyfr i symboli.
- Cyfry od 0 do 9
- Symbole specjalne (np. @*)
- Litery (od A do Z)
- W większości haseł rozróżniane są wielkie i małe litery - tak więc kombinacja wielkich (od A do Z) małych liter (od a do z)

Unikaj:

- Wybierania hasła podobnego do wcześniejszego
- Haseł zawierających imiona i nazwiska, nazwy użytkowników, prawdziwe nazwiska, nazwy firm itp.
- Wyrazów zapisanych w odwrotnej kolejności
- Sekwencji (qwerty, abcdef, 12345 itd.)
- Udostępniania haseł
- Zapisywania swoich haseł i przechowywania ich w pobliżu komputera lub systemu logowania
- Używania słowa „hasło” lub podobnych (spróbuj unikać używania cyfr zamiast liter, np. „ha5l0”)

Spróbuj:

- Wybrać hasło, które zapamiętasz

- Regularnie zmieniać hasła
- Nie korzystać z tego samego hasła na wielu kontach i programach
- Wybrać hasło, które nauczysz się wpisywać szybko, bez spoglądania na klawiaturę
- Przekształcić łatwe do zapamiętania wyrażenie w akronim

Przykład: susanlovesbrad - Su5@nL0ve58r@d

Również można zabezpieczać dane biometrycznie. Coraz popularniejsze stają się czytniki linii papilarnych, rozpoznawanie twarzy.

3.5 Szyfrowanie nośników danych

Szyforwanie dysku jest ważne aby, nasze dane nie zostały wykradzione. Szyfrowanie dysku może działać na różne sposoby. Np. BitLocker wymaga podania ustalonego kodu PIN przed zalogowaniem się do komputera. VeraCrypt pozwala stworzyć wirtualny, zaszyfrowany dysk i w nim ukryć pliki. Partycję można otworzyć tylko i wyłącznie z poziomu programu, wpisując najpierw ustalone wcześniej hasło.

Smartfony można bardzo łatwo zaszyfrować – zarówno zawartość ich pamięci wewnętrznej, jak i zewnętrznych nośników. Systemy Android mają taką opcję dostępną z poziomu ustawień telefonu (Ustawienia – Zabezpieczenia – Szyfrowanie). W taki sam sposób można zabezpieczyć zarówno pamięć urządzenia, jak i kartę pamięci.

Można również magazynować dane w chmurze, które również oferują szyfrowane. Jest to także odpowiednik wcześniej wspomnianych kopi zapasowych. Polega na tym, że pliki i dokumenty są przechowywane na specjalnie dostosowanym serwerze zewnętrznym. Można mieć do nich dostęp po zalogowaniu się na swoje konto w aplikacji. Dzięki temu można je przeglądać w dowolnym miejscu, w którym jest połączenie z internetem. Pierwszym i podstawowym zabezpieczeniem jest tutaj właśnie login i hasło dostępu. W momencie wysyłania plików do chmury jest ryzyko, że ktoś niepowołany może się do nich dostać. Chroni przed tym szyfrowanie plików. Można wybrać zewnętrzną aplikację do zaszyfrowania danych przed wysłaniem lub zsynchronizowaną z chmurą. Kolejna możliwość to po prostu chmura z wbudowanym szyfrowaniem danych.

3.6 Zabezpieczenie danych w sieci

- Korzystanie z najnowszej wersji systemu operacyjnego.

- Zabezpieczenie komputera programem antywirusowym.
- Nie otwieranie podejrzanych wiadomości i linków.
- Pobieranie programów tylko z zaufanych źródeł.
- Dbanie o anonimowość w sieci.
- Korzystanie z silnych haseł o których była mowa wcześniej.

3.7 Ochrona danych w przedsiębiorstwach

- Narzędzia CRM- które mogą przechowywać dane klientów w scentralizowanej lokalizacji. Platformy CRM mogą uwzględniać lokalizację danych i unikać przechowywania danych w wielu obszarach.
- Uwirzytelnanie wieloskładnikowe przez klientów oraz pracowników o którym mowa była wcześniej
- Szyforwanie - na poziomie plików, które może chronić przesyłane dane i utrudniać hakerom dostęp do oprogramowania lub zasobów w chmurze.
- Ochorna przed złośliwym oprogramowaniem – odpowiednie programy antywisusowe kóre działają jak zapory ogniowe i odpowiednio zabezpieczają urządzenia. Profesjonalne programy antywirusowe dają dużo większe możliwości niż zwykłe skanowanie dysku. Przykładowo – w wypadku kradzieży lub zgubienia laptopa firmowego, mają możliwość namierzenia go i zdalnego usunięcia wszystkich danych, analizują system i aplikacje pod kątem luk bezpieczeństwa wykorzystywanych przez hakerów czy sprawdzają bezpieczeństwo strony www jeszcze przed kliknięciem w link.
- Technologia BlockChain - w tłumaczeniu z angielskiego znaczy łańcuch bloków. Jest to metoda porządkowania i przechowywania danych w następujących po sobie blokach, które wspólnie tworzą jeden wirtualny łańcuch. Jest to zatem swoista baza danych, choć od typowej bazy różni się kilkoma cechami, które czynią z technologii blockchain niezwykle użyteczne i unikalne narzędzie. Przede wszystkim wszelkie zapisy wprowadzone do rejestru transakcji są całkowicie nieodwracalne, a zatem nie można ich usunąć ani zmodyfikować, dzięki czemu dane są chronione przed wszelkimi próbami oszustw. Ponadto zgromadzone dane nie są przechowywane na wybranym serwerze, lecz w całej sieci, na którą składa się tysiące komputerów. Takie rozproszenie ma podwójną

zaletę. Po pierwsze, zawsze można uzyskać dostęp do danych, a po drugie, nie grozi ich utrata choćby z powodu awarii sprzętu, cyberataków, klęsk żywiołowych czy innych nieprzewidzianych zdarzeń. Nie bez znaczenia jest też fakt, że technologia blockchain jest skonstruowana tak, aby z jednej strony zapewniać przejrzystość i transparentność zapisów, z drugiej zaś gwarantować anonimowość jej użytkownikom i poufność szczegółowych danych.

3.8 WOJTEK

4 Wnioski

- *Spostrzeżenia*
- Warto wiedzieć jak przedsiębiorstwa przechowują nasze dane, aby czuć się bezpiecznie.
- Posiadanie wiedzy na temat zabeczpieczania własnych danych jest ważne aby uniknąc nieprzyjemnych sytuacji w przyszłości z powodu braku rozwagi.
- *Osiągnięcia*
- to my jakieś mamy XD?
- *Potencjał rozwoju*
- brak ;/

5 Bibliografia

- https://klinikadanych.pl/artykuly/metody-zabezpieczania-przesylu-danych
- https://fingerprints.digital/identyfikacja-uwierzytelnianie-autoryzacja-czym-sie-roznia/
- https://www.ing.pl/wiem/bezpieczenstwo/jak-chronic-swoje-dane-osobowe
- https://fingerprints.digital/metody-uwierzytelniania-ktore-sa-bezpieczne/
- https://www.x-kom.pl/poradniki/5280-bezpieczenstwo-w-sieci-jak-zabezpieczyc-wazne-dane.html
- https://www.x-kom.pl/poradniki/5280-bezpieczenstwo-w-sieci-jak-zabezpieczyc-wazne-dane.html
- https://www.dell.com/support/kbdoc/pl-pl/000132376/tworzenie-silnego-has
- https://www.techtarget.com/searchcustomerexperience/answer/How-do-companies-protect-customer-data
- https://lepiej.tauron.pl/bezpieczenstwo-i-finanse/czym-jest-technologia-blockchain-i-jakie-daje-korzysci/

- ://www.omegasoft.pl/blog/jak-zabezpieczyc-i-chronic-dane-osobowe-w-firmie/
- https://www.endpointprotector.com/blog/5-ways-big-companies-protect-their-data/