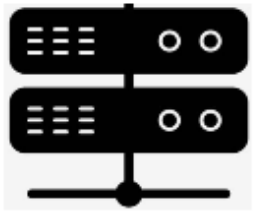
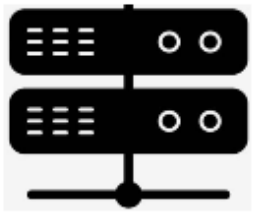
Kilka wiadomości na temat usługi poczty internetowej
i
dobrych praktyk dotyczących ochrony danych osobowych na komputerach osobistych

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl





Zilustrowana droga wiadomości email wysłanej przez Studenta/Wykładowcę

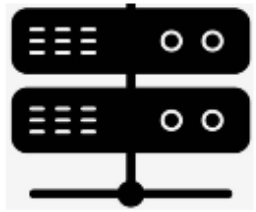
Dziekanat

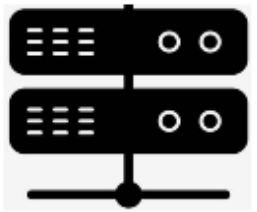
Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl

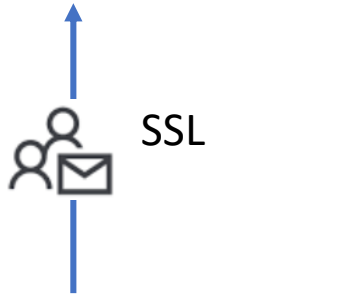




Wiadomość zostaje wysłana z komputera studenta

Na serwer na swojego dostawcy usługi poczty internetowej

1. Od strony technicznej – wszystko jest w porządku (szyfrowanie SSL)
2. Od strony prawnej – wszystko jest w porządku (student wyraził zgodę na przetwarzanie swoich danych osobowych w momencie zakładania darmowego konta)



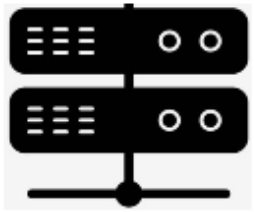
Dziekanat

Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl



Wiadomość zostaje dostarczona na serwer dostawcy usługi poczty. Zostaje odłożona razem z innymi wiadomościami które są przechowywane na serwerze dostawcy usługi poczty Internetowej przed dalszą wysyłką.

1.Od strony technicznej – wszystko jest w porządku (do serwera maja dostęp odpowiedni pracownicy dostawcy usług pocztowych. Administratorzy, osoby odpowiedzialne za backup danych)

2. Od strony prawnej – wszystko powinno być w porządku (student powinien wyrazić zgodę na przetwarzanie swoich danych osobowych w momencie zakładania darmowego konta pocztowego i wiedzieć kto ma do nich dostęp)

Dziekanat Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl

Wymiana Wiadomości pomiędzy serwerami pocztowymi.

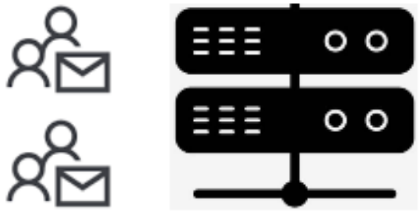
1.Na tym etapie brak jest szyfrowania wiadomości. Zostały przeprowadzone badania z których wynika iż 80% serwerów pocztowych na świecie nie szyfruje wiadomości wymienianych pomiędzy sobą. W tym momencie może dojść do: przechwycenia wiadomości, zmiany treści wiadomości, zainfekowania Wiadomości wirusem. Firma Microsoft próbowała zmienić obowiązujący protokół przesyłania wiadomości droga elektroniczną niestety próba ta była nieudana.

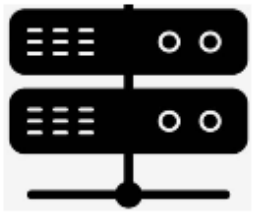
Dziekanat Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl





Wiadomość zostaje dostarczona na serwer UJD.

1.Od strony technicznej – wszystko jest w porządku (do serwera maja dostęp odpowiedni pracownicy techniczni UJD. Administratorzy, osoby odpowiedzialne za backup danych)

2. Od strony prawnej – wszystko jest w porządku (przetwarzamy adres mailowy studenta na podstawie przepisu prawa – rozporządzenie Ministra Nauki i Szkolnictwa Wyższego w sprawie studiów

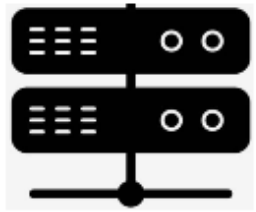
Dziekanat

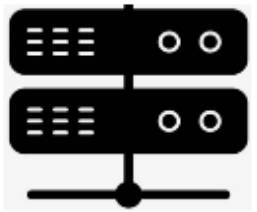
Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl





Wiadomość zostaje dostarczona do adresata
na komputer pracownika UJD

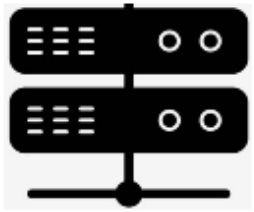
1. Od strony technicznej – wszystko jest w porządku (szyfrowanie SSL)
Komputer pracownika jest chroniony aktualnym programem antywirusowym
2. Od strony prawnej – wszystko jest w porządku (przetwarzamy adres mailowy studenta na podstawie przepisu prawa – rozporządzenie Ministra Nauki i Szkolnictwa Wyższego w sprawie studiów)

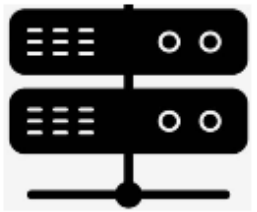
Dziekanat Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl





Jak zostało zilustrowane nie powinno się posługiwać usługą
Poczty Internetowej hostowaną na serwerach oferujących zarówno darmowe
jak i płatne konta pocztowe. Do każdego maila wysłanego przez serwer z
darmowym i płatnym kontem właściciel takiego hostingu ma dostęp i może odczytać zawarte tam dane.
Na kolejnych slajdach zostanie uwidoczniony jeszcze większy problem a mianowicie
odpowiedź pracownika UJD na takiego maila.

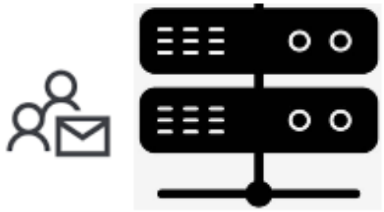
Dziekanat

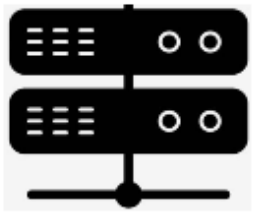
Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl





Odpowiedź Wykładowcy na maila od studenta

SSL

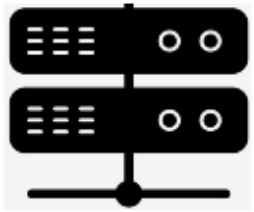
1. Technicznie ok– pracownik ma aktualny system operacyjny i aktualny program antywirusowy. Połączenie jest szyfrowane.
2. Prawnie ok - przetwarzamy adres mailowy studenta na podstawie przepisu prawa – rozporządzenie Ministra Nauki i Szkolnictwa Wyższego w sprawie studiów. Serwer pocztowy jest własnością Administratora Danych Osobowych

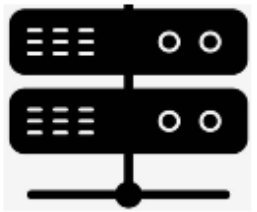
Dziekanat Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl

Serwer poczty
dowolnego dostawcy
Usług pocztowych np.
@gmail.com; @onet.pl; @wp.pl





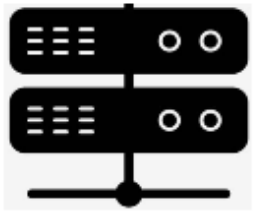
Wymiana Wiadomości pomiędzy serwerami pocztowymi

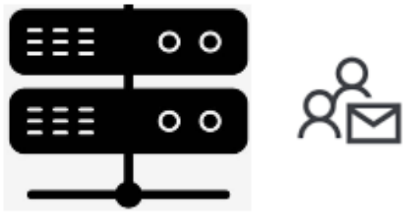
1. Technicznie jest PROBLEM– jak już zostało wspomniane na tym etapie brak jest szyfrowania. Treść wiadomości może zostać przechwycona i odczytana przez osoby nieuprawnione. Treść może również zostać zmieniona.
2. Prawnie jest PROBLEM – Uczelnia nie ma i nigdy nie będzie miała podpisanych odpowiednich umów powierzenia danych osobowych z wszystkimi możliwymi dostawcami usługi poczty internetowej.

Dziekanat Wykładowca

Student
/
Wykładowca prywatna poczta

Serwer Poczty @ujd.edu.pl





Jak widzimy nie ma sensu śledzenie dalszej drogi takiej wiadomości ponieważ w poprzednim etapie zostały złamane przepisy RODO dotyczące przetwarzania danych osobowych. Aby umożliwić prawidłowy i zgodny z prawem kontakt pracownika UJD ze studentem zostaną zaprezentowane narzędzia które to umożliwią.

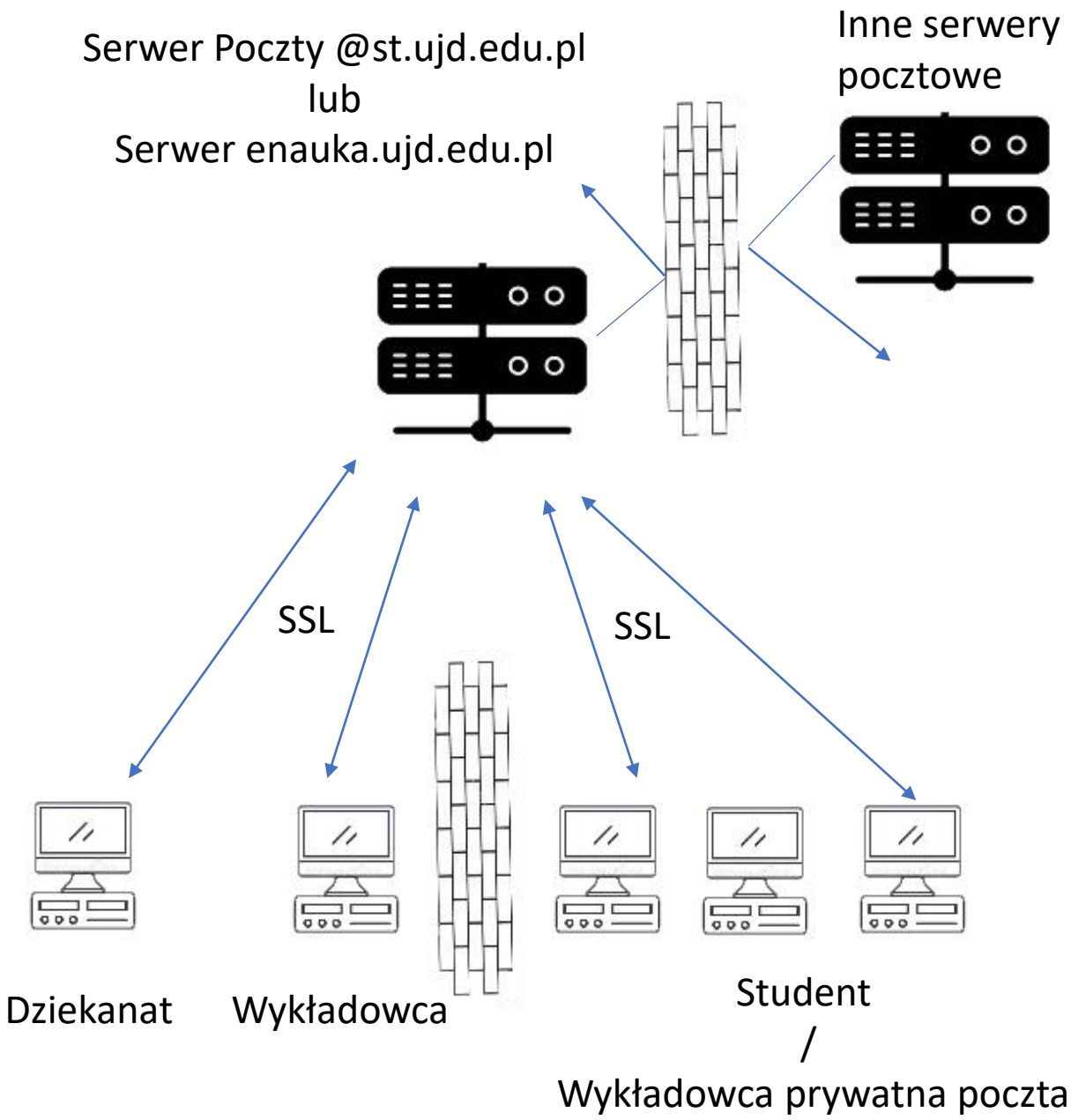
Dziekanat

Wykładowca

Student
/
Wykładowca prywatna poczta

Pierwsza opcją jest korzystanie z narzędzi dostarczonych przez ADO. W przypadku naszej Uczelni jest to:
1.Platforma Enauka za pomocą której mają Państwo możliwość prowadzenia procesu dydaktycznego. Mają tam konta wszyscy studenci i wykładowcy.
2.Serwer pocztowy który nie akceptuje maili z innych serwerów pocztowych jak również nie można z niego wysłać wiadomości na żaden inny serwer pocztowy. Konta na tym serwerze mają wszyscy studenci i wszyscy wykładowcy.
Dodatkowo zalecamy aby dostęp do kont na tym serwerze był prowadzony z poziomu przeglądarki internetowej.

W oby dwóch przypadkach zarówno od strony prawnej jak i technicznej Nie będzie żadnych problemów.



Jeżeli nadal chcą Państwo używać usług poczty internetowej w tradycyjny sposób (możliwość prowadzenia korespondencji z każdym serwerem pocztowym na świecie) to :

1) Jeżeli używają Państwo jakiegokolwiek klienta pocztowego np. MS Outlook, Mozilla Thunderbird lub innych to pliki magazynujące maile w tych klientach powinny się znaleźć w zaszyfrowanej przestrzeni dyskowej Państwa komputerów. Świetnie do tego celu może posłużyć darmowy program VeraCrypt. Instrukcja jak stworzyć zaszyfrowany kontener dostępna jest pod adresem http://www.info.ujd.edu.pl/media/domeny/54/static/pub/druki/dii/veracrypt_samouczek_dla_poczatkujacych.pdf

Plusem tej metody jest to że nawet jeśli Państwa komputer zostanie zgubiony to dane osobowe zawarte w korespondencji mailowej będą bezpieczne.

Minusem tego rozwiązania jest to iż zawsze przed pierwszym uruchomieniem klienta pocztowego trzeba będzie podłączyć zabezpieczony kontener aby program mógł odbierać i wysyłać wiadomości w przeciwnym wypadku będzie zgłaszał błędy lub nie będzie działać.

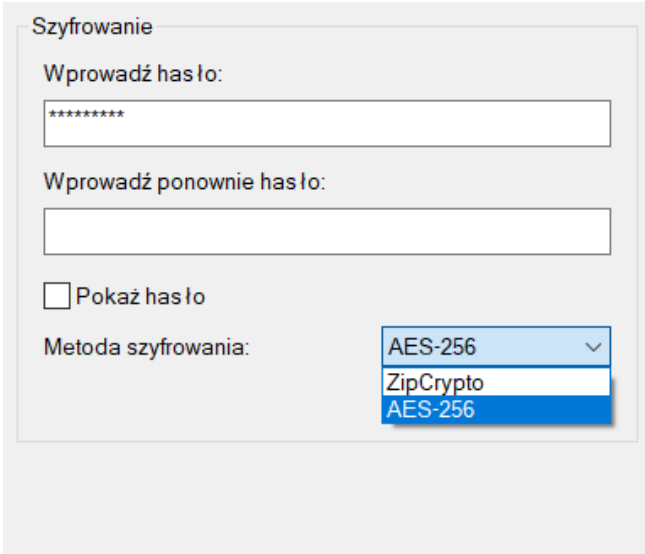
2) Jeżeli logują się Państwo do swoich kont pocztowych przez strony internetowe to tylko zapisywane dokumenty zawierające dane osobowe powinny być przechowywane w tak przygotowanej i zaszyfrowanej przestrzeni.

Wszystkie dokumenty zawierające dane osobowe na Państwa komputerach powinny być przechowywane na zaszyfrowanej części partycji – do tego celu można użyć wspomnianego tu programu VeraCrypt.

Kontakt przez oprogramowanie takie jak ZOOM, Skype czy usługi powiązane z MSOffice 365 wymaga najpierw uzyskania zgody studenta na tą formę kontaktu i poinformowanie go iż jego dane osobowe jak i przebieg całej rozmowy są nagrywane i mogą być przechowywane na serwerach znajdujących się fizycznie poza obszarem Unii Europejskiej.

Wzór zgody jest załącznikiem do zarządzenia Rektora nr R.021.1.41.2020 z dnia 11 maja 2020.

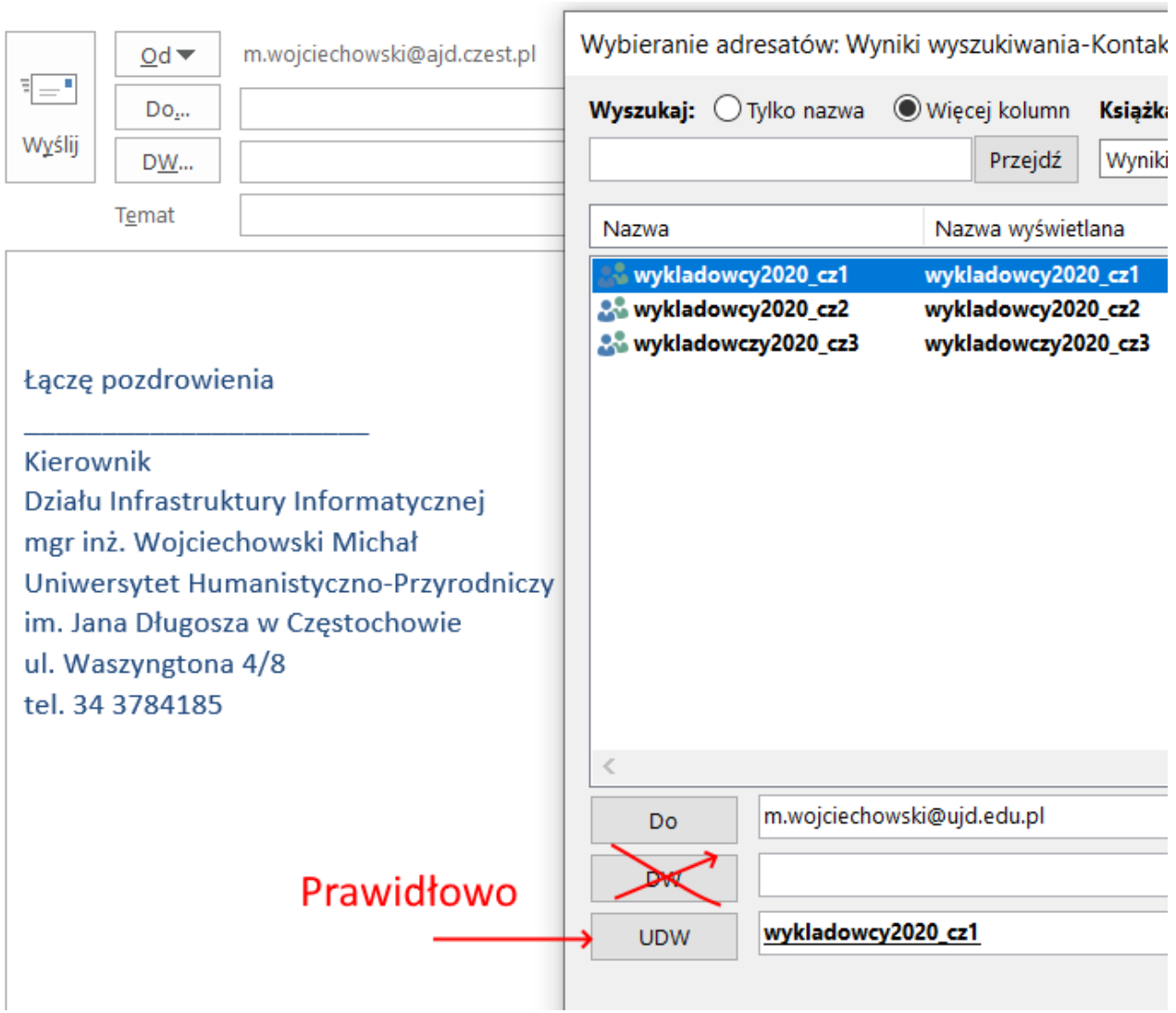
Aby zabezpieczyć korespondencję mailową ze studentem prowadzoną poprzez tradycyjną usługę poczty internetowej powinni Państwo wszelkie dane osobowe przesyłać w zaszyfrowanej części maila. Można to osiągnąć poprzez dodawanie zaszyfrowanych załączników a w treści takich wiadomości przesłać tylko informacje ogólnodostępne.
Można do tego wykorzystać darmowy program 7zip. Ważne jest aby przy kompresowaniu/pakowaniu plików z danymi osobowymi przy pomocy tego programu wybrać odpowiednie opcje szyfrowania.
Należy wprowadzić mocne hasło o długości min 10 znaków z czego powinna się tam znaleźć co najmniej jedna duża litera, jedna cyfra i jeden znak specjalny (.,! itp).
Dodatkowo należy zmienić domyślny sposób szyfrowania na AES-256 ponieważ jest on praktycznie niemożliwy do złamania w przeciwieństwie do domyślnego sposobu szyfrowania występującego w tym programie.



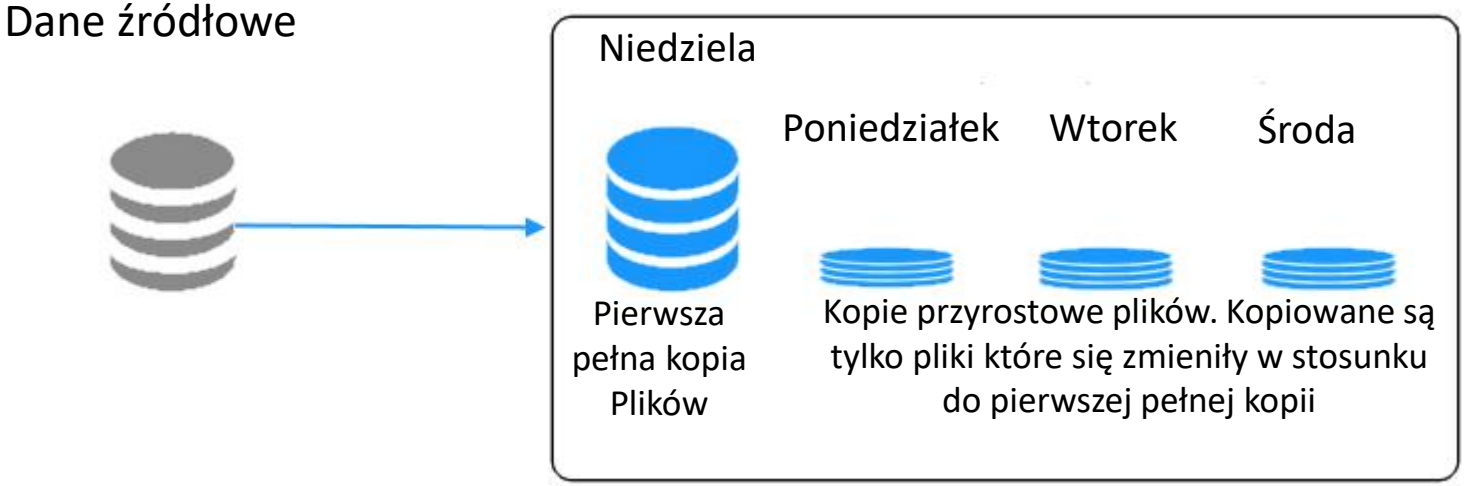
Plusem jest to że wysyłane dane osobowe tradycyjną pocztą internetową zabezpieczycie Państwo przed dostępem osób niepowołanych.

Minusem jest to że nie można używać cały czas jednego hasła i dodatkowo trzeba to hasło przekazać studentowi inną drogą niż samą wiadomość. Można do tego celu wysłać wiadomość z hasłem na inne konto mailowe studenta lub przesłać ją mu sms-em jeśli posiadają Państwo nr telefonu studenta. Dodatkowym problemem może okazać się sama ilość haseł jaką Państwo wygenerują i ich przechowywanie. Z pomocą może przyjść darmowy program KeePass. Instrukcja instalacji obsługi znajduje się pod tym adresem
http://www.info.ujd.edu.pl/media/domeny/54/static/pub/druki/dii/KeePass_instrukcja.pdf

Kolejnym problemem w wysyłaniu wiadomości mailowych jest wysyłanie maili do wielu osób jednocześnie. W tym celu powinno się używać zawsze pola UDW- ukryte do wiadomości. Dobrą praktyką jest wysłanie maila do samych siebie. W pole DO wpisujemy swój adres a w pole UDW wpisujemy adresatów wiadomości. Obojętnie czy mają Państwo stworzoną grupę adresów mailowych czy dodają Państwo te adresy po kolei nigdy nie powinno się ich wstawiać w pola Do ani DW – do wiadomości. Jeśli tak Państwo postępujecie to udostępniacie daną osobowa jaką jest adres email osobom nieupoważnionym do ich przetwarzania.



Pomimo tego iż będą Państwo przechowywać pliki z danymi osobowymi na zaszyfrowanej części partycji to niestety ten kontener chroni tylko przed nieupoważnionym dostępem do jego zawartości czyli plików z danymi osobowymi. Nie ochroni Państwa od utraty takiego pliku w kontenerze lub co gorsza w wyniku błędu dysku od dostępu do całej zawartości takiego kontenera dlatego warto wyrobić w sobie systematyczność w robieniu kopii zapasowej ważnych plików. Z pomocą może tu przyjść darmowy program EaseUS Todo Backup Free do którego podstawową instrukcję można znaleźć pod tym adresem http://www.info.ujd.edu.pl/media/domeny/54/static/pub/druki/dii/EaseUS_instrukcja.pdf . Warto też przyjrzeć się darmowemu programowi Personal Backup.
Pierwszy można ściągnąć klikając w ten link: https://pl.easeus.com/backup-software/todo-backup-free.html
Drugi klikając w ten link: https://personal-backup.rathlev-home.de/download/pb-setup-6.1.0400.exe



Pomimo iż Państwa komputer jest chroniony przed złośliwym oprogramowaniem (ang. malware – zbitka słów malicious „złowrogi, złośliwy” i software „oprogramowanie”) przez program antywirusowy który zawsze musi być aktualny nie jest w stanie w niektórych systuacjach ochronić użytkownika przed jego łatwowiernością. Coraz częściej zdążają się maile które same w sobie nie zawierają złośliwego oprogramowania ale poprzez użycie metod socjotechniki prowadzą użytkownika do tego aby sam zezwolił na instalacje jakiegoś oprogramowania lub samowolnie wykonał polecenia których normalnie by nie wykonał a w wyniku których może np. stracić pieniądze.
Na kolejnych slajdach znajdą Państwo klika wskazówek jak się bronić przed atakami przeprowadzanymi poprzez usługę poczty internetowej ale nie tylko.

Popularne schematy ataków fałszywymi mailami

Przestępcy wykorzystujący emaile do swoich ataków często korzystają z wcześniej opracowanych wzorów. Najpopularniejsze scenariusze ataku używane ostatnio w Polsce to:

-**faktura od kontrahenta**

Wiadomość od nieznanego nadawcy zawiera najczęściej załącznik ze słowem „faktura” w nazwie oraz informację o konieczności pilnego opłacenia zaległości.

-**windykacja**

Wiadomość podszywająca się pod jedną z dużych firm windykacyjnych sugerująca, że odbiorca posiada zaległości płatnicze.

-**wezwanie na rozprawę lub pozew**

Wiadomość podszywająca się pod sąd lub kancelarię prawną, wskazująca numer sprawy i termin oraz miejsce kolejnej rozprawy.

-**paczka do odebrania**

Nadawca podszywa się pod operatora pocztowego lub firmę kurierską i informuje o braku możliwości dostarczenia przesyłki ze względu np. na nieobecność odbiorcy.

-**faktura od operatora telekomunikacyjnego**

Nadawca podszywa się jedną z dużych firm telekomunikacyjnych lub np. dostawcę mediów i informuje o wystawieniu kolejnej faktury.

-**wiadomość od banku**

Nadawca podszywa się pod jeden z banków i informuje np. o podejrzanej aktywności na koncie wymagającej pilnej weryfikacji.

-**wiadomość z serwisu aukcyjnego**

Nadawca podszywa się pod serwis aukcyjny lub sprzedawcę i informuje o problemach z kontem lub zakupem.

-**wygrana na loterii**

Informacja o rzekomej dużej wygranej.

Niespodziewane wiadomości mailowe

Uniwersalna zasada mówi, że jeżeli nie znasz nadawcy i nie spodziewasz się wiadomości, to lepiej jej nie otwierać. Przestępcy najczęściej podszywają się pod znane firmy lub wysyłają swoje wiadomości z kont zwykłych użytkowników. Jeśli nie kojarzysz adresu nadawcy lub otrzymujesz fakturę od firmy, w której zakupów nie pamiętasz, lepiej taką wiadomość zignorować.

Za podejrzane warto także uznać wszystkie wiadomości zawierające błędy językowe lub ortograficzne oraz wiadomości adresowane w sposób ogólny (np. „Szanowny Kliencie”), nie zawierające Twoich danych.

Czasem zdarza się także, że przestępcy włamują się na skrzynkę kogoś z Twoich znajomych i wysyłają wiadomość do wszystkich jego kontaktów. Warto zatem pamiętać, że podejrzane wiadomości od znanych Ci osób warto sprawdzić i zadzwonić do nadawcy.

Wiadomości zawierające fałszywe linki

Czasem złośliwe e-maile nie zawierają załączników lecz zawierają linki wyglądające na prawdziwe, prowadzące na przykład do strony logowania banku. Przestępcy potrafią tak skonstruować swoją wiadomość, że patrząc na jej treść widzisz prawidłowy link (np. www.bank.pl/logowanie), jednak kiedy klikniesz, przeniesiesz się do fałszywej strony pod innym adresem. Aby sprawdzić dokąd prowadzi link wystarczy najechać na niego kursorem myszki – wtedy na dole okna przeglądarki lub programu pocztowego pojawi się treść adresu, do którego naprawdę prowadzi. Warto ją zweryfikować przed kliknięciem.

Uwaga na niebezpieczne załączniki

Każdą wiadomość z załącznikiem lub zawierającą link do pobrania pliku trzeba traktować jako podejrzaną. Przestępcy często wysyłają pliki spakowane w formie archiwum ZIP lub RAR. Samo otwarcie archiwum nie jest groźne – niebezpieczeństwo może czaić się w środku. Jeśli archiwum jest zabezpieczone hasłem podanym w treści wiadomości to najczęściej zawiera niebezpieczne oprogramowanie.

Załącznik może być także przesyłany w formie niespakowanej. Powinno się dobrze przyjrzeć nazwie pliku. Najważniejsze są jej ostatnie znaki. Jeśli plik ma podwójne rozszerzenie (czyli końcówkę nazwy po kropce), np. PDF.EXE czy DOC.SCR to nie należy go otwierać.

Z reguły bezpieczne są pliki graficzne (JPG, GIF, PNG), filmy (AVI, MPG, MKV) czy muzyka (MP3). Niebezpieczne pliki to przede wszystkim pliki wykonywalne oraz skrypty. Niestety mogą mieć one wiele różnych rozszerzeń – najczęściej stosowane to EXE, PIF, VBS czy JS. Jeśli nie znasz danego rozszerzenia to bezpieczniej jest pliku nie otwierać. Nie należy się także sugerować ikonką pliku (miniaturką) –przestępcy mogą ją łatwo zmodyfikować.

Niebezpieczne makra

Pliki takie jak dokumenty Word (DOC, DOCX) czy Excel (XLS, XLSX) także są używane przez przestępców. Samo otwarcie pliku z reguły nie jest groźne, jednak mogą one zawierać tzw. makro, czyli dodatkowy program pobierający na komputer np. konia trojańskiego. Uruchamianie makr jest domyślnie wyłączone, jeśli zatem widzisz prośbę o jego włączenie, to najczęściej jest to próba ataku.

W miarę możliwości powinno się używać menedżera haseł i uwierzytelniania dwuskładnikowego

Użyj znanego menedżera haseł np. proponowanego KeePass-a, aby zmienić wszystkie swoje hasła online na silne, unikalne dla każdego logowania. Może to zająć trochę czasu, ale warto, aby uniknąć ryzyka. Podczas konfigurowania haseł dla kont skonfiguruj także uwierzytelnianie dwuskładnikowe (2FA) jako dodatkową warstwę zabezpieczeń dla kont, które ją oferują. Zrób to samo, gdy konfigurujesz urządzenia IoT w swoim domu (i szukaj urządzeń IoT z obsługą 2FA przy zakupie!).

Korzystaj z usługi VPN na komputerze i telefonie

Bądź anonimowy, używając VPN do szyfrowania połączenia z internetem. To doskonała metoda nie tylko na zagwarantowanie sobie prywatności w sieci, ale również na bezpieczeństwo przy korzystaniu z nowych sieci Wi-Fi. VPN dodatkowo sprawi, że przeglądanie stron internetowych będzie przyjemniejsze: mniej reklam, anonimowy adres IP, większa prywatność.

Nie korzystaj z komputerów publicznych ani sieci Wi-Fi

Kiedy podróżujesz lub nie jesteś w domu, spróbuj korzystać z Internetu tylko za pomocą własnego komputera lub urządzenia mobilnego (oczywiście z włączoną usługą VPN). Komputery publiczne (na przykład te w hotelach lub kawiarniach internetowych) są dostępne dla innych osób, które mogą umieszczać na nich keyloggery lub inne złośliwe programy, które nawiedzą Twoje konta online, przekazując dane oszustom internetowym. A już w żadnym przypadku nie loguj się w takich miejscach do swojej bankowości online lub nie dokonuj zakupów w sieci.

Zabezpiecz swój router i Wi-Fi

Nieautoryzowani użytkownicy mogą próbować włamać się do twojej sieci domowej lub sieci firmowej, do której podłączone są wszystkie istotne urządzenia: telefony, komputery, serwery. Dlatego niezwykle istotna jest ochrona . Upewnij się, że zmieniłeś hasło administratora routera i ustawiłeś hasło do sieci Wi-Fi na naprawdę silne, którego haker nie będzie w stanie złamać.

Dbaj o aktualizacje systemu operacyjnego komputera i smartfona

Ilekroć wydawane są aktualizacje oprogramowania, natychmiast je pobierz. Bardzo często zawierają bowiem aktualizacje w zakresie bezpieczeństwa.

Aktualizuj wszystkie aplikacje zainstalowane na Twoim smartfonie i komputerze

Podobnie jak w przypadku aktualizacji systemu operacyjnego, aktualizacje oprogramowania dostarczają również łatek bezpieczeństwa. Pobierz je natychmiast jak będą dostępne.

Nastaw limity na swoim koncie bankowym

Na co dzień nie potrzebujesz mieć nieograniczonych limitów na codzienne wydatki. A jeśli planujesz jakiś większy, to raczej nie jest to spontaniczna decyzja, ale przemyślany wydatek. W takiej sytuacji możesz zmienić limity i ponownie nastawić je po dokonaniu zakupu. Nawet jeśli dojdzie do utraty danych finansowych i wykorzystania ich przez oszustów, straty będą ograniczone.