Porady

E-mail: standardowy czy szyfrowany?

Paweł Wałuszko 27.01.2020

Podczas jednego z webinarów o tematyce ataków socjotechnicznych prowadzonych przez CyberForces i Xopero, kilku uczestników zapytało mnie, jak korzystać z szyfrowanego maila na co dzień oraz jaka jest różnica pomiędzy emailem zwykłym a szyfrowanym. Ponieważ wątek ten jest bardzo obszerny, postanowiłem napisać dla Was dłuższy materiał na ten temat.

Problematyczny standardowy e-mail

Mimo ogromnego sukcesu poczty elektronicznej warto zwrócić uwagę też na jej słabe strony. Można stwierdzić, że sposób, w jaki funkcjonuje dziś e-mail, nie uległ wielkim zmianom od lat 90. XX wieku. Z niewielkimi aktualizacjami, używamy protokołów opracowanych kilkadziesiąt lat temu.

Problematyka „zwykłego" e-maila niekoniecznie dotyczy wykorzystywania archaicznych protokołów lub ich założeń, ale bardziej faktu, że wówczas przyjęty standard funkcjonowania poczty internetowej nie przewidywał domyślnego szyfrowania korespondencji.

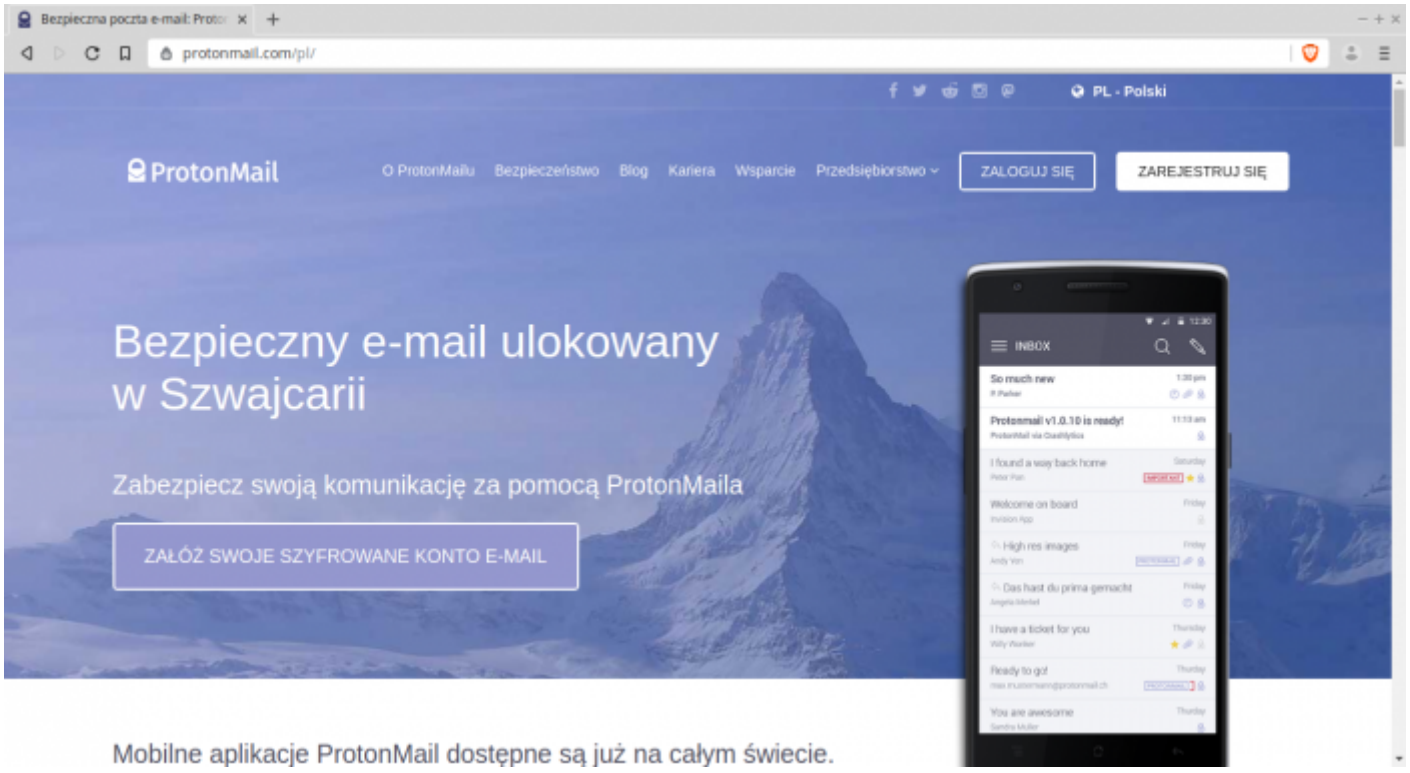
Podczas gdy wysyłanie i odbieranie wiadomości odbywa się poprzez protokoły takie jak SMTP, IMAP lub POP3, które z zasady są wspierane szyfrowaniem podczas przesyłania danych (np. TLS lub STARTTLS), samo przechowywanie danych odbywa się bez jakiegokolwiek zabezpieczenia przed odczytaniem przez nieproszonych gości. Stąd z punktu widzenia administratora lub usługodawcy, czytanie zawartości czyjejś skrzynki jest tak łatwe do wykonania, jak otwarcie pliku na komputerze.

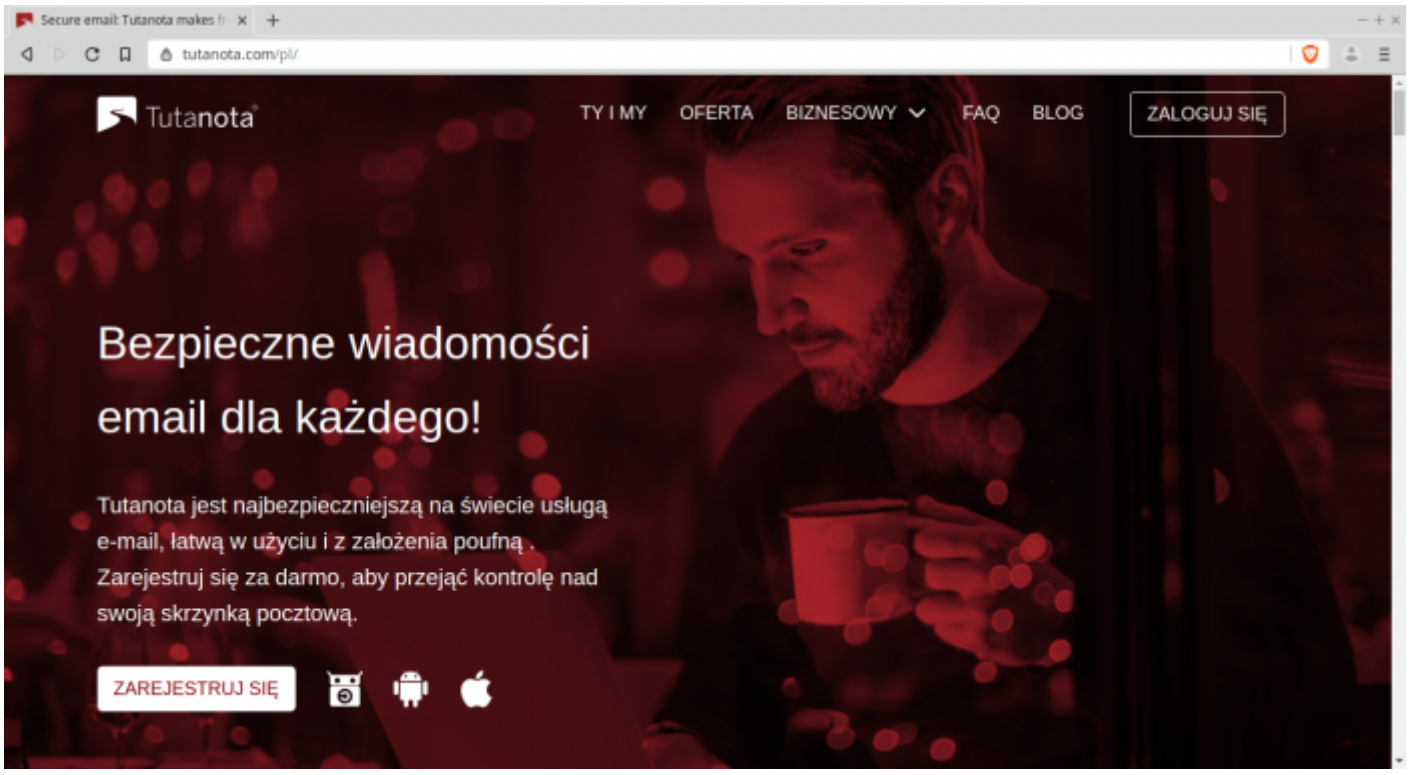
Dla użytkownika końcowego konsekwencje tego stanu rzeczy mogą być dość nieprzyjemne. Nawet jeżeli wzorowo zadbamy o zabezpieczenie konta i urządzeń, na których odbieramy pocztę, jeśli ktoś zhakuje naszego usługodawcę, treść prywatnych wiadomości stanie się dla niego dostępna. Dla wielu użytkowników taki wyciek jest równoznaczny nie tylko z utratą prywatności, ale także z rozpowszechnieniem danych, które mogą zostać wykorzystane do kradzieży tożsamości.

Szyfrowany e-mail

Naturalną odpowiedzią na wyżej wymienione problemy jest zabezpieczenie standardowego e-maila poprzez dodanie funkcji szyfrowania treści wiadomości. Niestety, szyfrowany e-mail nie jest jeszcze standardem i może przysporzyć wiele niedogodności, szczególnie jeżeli wysyłamy za jego pomocą wiadomości do użytkowników, którzy nie posiadają szyfrowanego konta poczty elektronicznej.

Najłatwiejszym sposobem na szyfrowanie wiadomości jest skorzystanie z usług, które automatycznie zadbają o szyfrowanie i odszyfrowywanie zawartości maili. Obecnie najbardziej popularnymi z nich są Protonmail (Szwajcaria) oraz Tutanota (Niemcy):





Jak można zauważyć, po stronach usługodawców założenie szyfrowanej skrzynki e-mail jest tak proste, jak standardowej. Wiadomości wysłane pomiędzy dwoma usługodawcami są automatycznie szyfrowane i odszyfrowywane na urządzeniach użytkowników. *De facto* nawet usługodawcy nie są w stanie odszyfrować wiadomości, dając nam gwarancję prywatności i bezpieczeństwa korespondencji.

Natomiast szyfrowane wiadomości wysłane do użytkowników posiadających standardowe konta e-mail (np. Gmail) działają troszeczkę inaczej. Gdy użytkownik e-maila szyfrowanego wysyła wiadomość do użytkownika ze zwykłym kontem e-mail, odbiorca nie otrzymuje wiadomości od razu, lecz jest proszony o kliknięcie linku, który otworzy docelową wiadomość w oknie przeglądarki internetowej. Po kliknięciu, odbiorca musi podać hasło, które wcześniej otrzymał od nadawcy (najlepiej poprzez inną usługę, np. telefonicznie).

Po wpisaniu odpowiedniego hasła wiadomość zostaje odszyfrowana i istnieje możliwość odpowiedzi w tym samym oknie przeglądarki. Przy kliknięciu „wyślij” nowa wiadomość jest automatycznie szyfrowana i wysyłana do odbiorcy.

	E-mail standardowy	E-mail szyfrowany
Szyfrowanie podczas autoryzacji	✔	✔
Szyfrowanie podczas transmisji	✔	✔
Szyfrowanie treści (przechowywanie)	**x**	✔

Korzystanie z szyfrowanego maila na istniejącej skrzynce e-mail

Szyfrowane konto e-mail w dużej mierze rozwiązuje problem zabezpieczania korespondencji przed odczytaniem przez osoby postronne. Aczkolwiek, nie każdy jest gotowy, aby zmienić swojego dostawcę e-mail, a tym samym adres poczty. Dość często do jednego adresu e-mail podpiętych jest już tysiące usług, stąd migracja na inny może być bardzo czasochłonna lub wręcz niemożliwa.

Warto wiedzieć więc, że istnieje też możliwość wysyłania szyfrowanych wiadomości przy użyciu standardowych kont e-mail, choć wiąże się to z dość dużym utrudnieniem. Po pierwsze, musimy wybrać oprogramowanie, które będzie odpowiedzialne za stworzenie klucza prywatnego i publicznego oraz za szyfrowanie i odszyfrowywanie wiadomości e-mail. Takim oprogramowaniem jest np. Gpg4win lub Kleopatra.

Przy uruchomieniu oprogramowania będziemy musieli wygenerować dwa wirtualne klucze: prywatny i publiczny. Klucz prywatny to wirtualny klucz w postaci pliku, za pomocą którego możemy odszyfrować otrzymane wiadomości. Klucz powinien być szczególnie chroniony, gdyż posiadanie go pozwoli komukolwiek na odszyfrowanie naszych wiadomości. Inaczej mówiąc — powinien być traktowany tak, jak hasło.

Klucz publiczny to z kolei klucz, który może być podany do publicznej informacji (warto pamiętać, że aby wysłać wiadomość, nadawca musi znać klucz publiczny odbiorcy). Po wygenerowaniu klucza publicznego przez oprogramowanie powinniśmy przekazać go osobom, z którymi chcemy się porozumiewać szyfrowanym mailem. Klucz publiczny może być wysłany do odbiorcy jakimkolwiek sposobem: e-mailem, wiadomością tekstową lub poprzez dowolny komunikator. Gdy osoba pisząca do nas szyfrowanego maila posiada nasz klucz publiczny, może przystąpić do tworzenia i nadania wiadomości.

Tekst zaszyfrowany kluczem odbiorcy wysyłany jest jako normalny tekst standardowym kontem e-mail. Odbiorca zaszyfrowanej wiadomości otrzyma tekst, który będzie możliwy do odczytania tylko i wyłącznie przy użyciu prywatnego klucza, po skopiowaniu treści wiadomości i wklejeniu zawartości do oprogramowania szyfrującego. Dla wszystkich innych osób, które mogłyby ten tekst przeczytać po drodze, zawartość wiadomości będzie zupełnie nieczytelna. W tym momencie warto zaznaczyć, że technologia kluczy prywatnych i publicznych opracowana jest w taki sposób, aby uczynić niemożliwym odszyfrowanie wiadomości przy użyciu klucza publicznego.

Kleopatra

Wtyczki

Jak można zauważyć, używanie nieszyfrowanej skrzynki do wysyłania szyfrowanych wiadomości jest dość skomplikowane, dlatego istnieje wiele usług, które automatyzują i upraszczają ten proces. Wtyczki takie jak Mailvelope oraz FlowCrypt ułatwiają zarządzanie kluczami, szyfrowanie i odszyfrowywanie treści wiadomości w popularnych usługach, takich jak Gmail. Ponadto istnieje wiele wtyczek do klientów poczty elektronicznej, takich jak Microsoft Outlook czy Mozilla Thunderbird, które w bardzo podobny sposób ułatwiają korzystanie z szyfrowania wiadomości. Przykładem takiej wtyczki do Microsoft Outlook jest GpgOL. Natomiast dla klientów biznesowych szyfrowany e-mail może być standardem przy odpowiedniej konfiguracji serwera poczty, choć pełna implementacja jest zadaniem dla administratorów sieci firmowej.

Podsumowując

W dobie powszechnego śledzenia użytkowników oraz lukratywnego biznesu handlowania danymi ze zhackowanych kont, korzystanie z szyfrowanego maila jest bardzo sensownym pomysłem. Osobiście dla osób prywatnych polecam stopniową migrację z usług nieszyfrowanych na usługi szyfrowane. Każdy z nas może zacząć od założenia szyfrowanej skrzynki i stopniowo przenosić komunikację i subskrypcje na nowe konto. Ponadto, funkcje takie jak przekazywanie wiadomości ze starej skrzynki, mogą pomóc w zachowaniu wiadomości, których nie zaktualizowaliśmy o nowe dane mailowe. Z biegiem czasu, skrzynka szyfrowana stanie się naszą domyślną.

Jeśli chodzi o przedsiębiorstwa już teraz polecam zastanowić się nad infrastrukturą i polityką komunikacji wewnętrznej. Korzystanie z szyfrowanego maila nie jest o wiele trudniejsze dla użytkowników końcowych, zwłaszcza jeżeli całe przedsiębiorstwo korzysta z tej technologii. Szyfrowanie i odszyfrowywanie wiadomości jest zautomatyzowane, a user experience – niemal identyczny. Ponadto pamiętajmy, że jako biznes mamy wiele do stracenia i wyciek danych nie będzie tylko problemem działów IT, ale wpłynie negatywnie na całą firmę.

27.01.2020

[Paweł Wałuszko]

Business Development Manager i Ekspert ds. Bezpieczeństwa. Doświadczony menedżer w branży IT, który swoje doświadczenie zdobywał m.in. w Dolinie Krzemowej; entuzjasta oprogramowania open - source.

VPN do użytku prywatnego – czy warto?

OPSEC, czyli sztuka ochrony danych według armii USA