JOURNAL
COMPUTER SCIENCES INSTITUTE

JCSI 36 (2025) 312–319
Received: 16 April 2025
Accepted: 12 May 2025

Analysis of ergonomics and security of email software

Analiza ergonomii i bezpieczeństwa programów pocztowych

Marceli Szarapajew*, Tomasz Szymczyk

Department of Computer Science, Lublin University of Technology, Nadbystrzycka 36B, 20-618 Lublin, Poland

Abstract
Within the scope of the article, two studies were carried out on the most frequently used email programs. In the first study, parameters were measured regarding the speed and ergonomics of these programs, and the intuitiveness of their interfaces was compared. In the second study, the performance of email security mechanisms, the possibility to change their settings, and the security vulnerabilities detected in these programs in the past were verified. The results of the study clearly indicate the weaknesses of the security mechanisms studied, and also allowed to verify which email programs are the easiest and most intuitive to use.

Keywords: email; internet; ergonomics; cyber security

Streszczenie
W ramach artykułu przeprowadzono dwa badania dotyczące najczęściej używanych programów pocztowych. W pierwszym z nich wykonano pomiary parametrów dotyczących szybkości i ergonomii używania tych programów, a także porównana została intuicyjność ich interfejsów. W drugim badaniu zweryfikowane zostało działanie mechanizmów obrony przed zagrożeniami związanymi z wiadomościami e-mail, możliwości zmiany ich ustawień, a także przeanalizowane zostały luki bezpieczeństwa wykryte w tych programach w przeszłości. Wyniki badań jednoznacznie wskazują na słabości w działaniu badanych mechanizmów bezpieczeństwa, a także pozwoliły na zweryfikowanie, jakie programy pocztowe są najłatwiejsze i najbardziej intuicyjne w użytkowaniu.

Słowa kluczowe: poczta elektroniczna; internet; ergonomia; cyberbezpieczeństwo

*Corresponding author
Email address: **marceli.szarapajew@pollub.edu.pl** (M. Szarapajew)

1. Wstęp

Poczta elektroniczna (e-mail) jest jedną z najważniejszych form komunikacji w internecie. Jest to rozwinięcie tradycyjnej poczty, działające w sieci lokalnej lub globalnej [1]. Wiadomości e-mail, początkowo w postaci czystego tekstu, dzisiaj często są zaawansowane strukturalnie i graficznie, mogą też zawierać załączniki. Każdego dnia wysyła się ponad 361 bilionów wiadomości e-mail, i prognozuje się wzrost tej liczby z roku na rok [2]. Pod wpływem rozwoju poczty elektronicznej powstały różne programy obsługujące skrzynki pocztowe wielu dostawców. Obecnie odchodzi się od tradycyjnych programów na rzecz aplikacji webowych, używanych z poziomu przeglądarki internetowej.

Przy tworzeniu programów pocztowych istotne są dwie kluczowe kwestie. Pierwszą z nich jest ergonomia interfejsu. W czasach, kiedy wiele spraw można załatwić przez internet ważne jest, aby program pocztowy był dostosowany do potrzeb wszystkich użytkowników, niezależnie od ich wiedzy o komputerach, a także miał intuicyjny interfejs, który nie przytłacza użytkownika mnogością elementów i kolorów. Druga kwestia dotyczy zabezpieczeń przed różnymi zagrożeniami cyberbezpieczeństwa. Poczta elektroniczna jest coraz częściej wykorzystywana do zasypywania użytkowników spamem [3], wykradania ich haseł i poufnych danych, a nawet do przejmowania kontroli nad ich kontami i urządzeniami [4]. Ważne jest nie tylko zapobieganie otrzymywaniu niebezpiecznych wiadomości e-mail, ale także uświadamianie użytkownika o zagrożeniach i możliwości ich unikania.

W ramach tego artykułu przebadano popularne programy pocztowe pod kątem ergonomii interfejsu oraz dostępności funkcjonalności związanych z obsługą poczty elektronicznej, oraz zweryfikowano działanie zawartych w nich mechanizmów zabezpieczających przed popularnymi zagrożeniami bezpieczeństwa, takimi jak phishing, spoofing i malware [3].

2. Cel, zakres badań i hipotezy badawcze

Artykuł ma na celu porównanie popularnych programów do obsługi poczty elektronicznej w celu sprawdzenia dostępności ich interfejsów i mechanizmów obrony przed zagrożeniami. W badaniach uczestniczyła grupa badawcza, składająca się głównie ze studentów Politechniki Lubelskiej. Po przeprowadzeniu badań dogłębnie przeanalizowano i opisano ich wyniki, a na ich podstawie wyciągnięto odpowiednie wnioski.
W artykule zdefiniowano następujące hipotezy badawcze:

H1. Istnieje prawdopodobieństwo, że nie wszystkie programy do obsługi poczty elektronicznej dostępne na rynku są jednakowo ergonomiczne dla każdego użytkownika,
H2. Nie wszystkie programy do obsługi poczty elektronicznej dostępne na rynku są jednakowo bezpieczne i chronią użytkownika przed zagrożeniami bezpieczeństwa w ten sam sposób.

3. Przegląd literatury

W celu zapoznania się z zagadnieniami omawianymi w artykule przeprowadzono analizę dotychczasowych prac naukowych dotyczących poczty elektronicznej. Pierwsze z nich – ergonomia w programach pocztowych – nie pojawia się zbyt często w artykułach z ostatnich lat. Artykuł [5] opisuje badanie dotyczące umiejętności studentów w użytkowaniu podstawowego oprogramowania, w tym również pocztowego. U znacznej części grupy badawczej wykryto trudności z dodaniem załącznika do wiadomości e-mail, a u niektórych uczestników także z wysłaniem jakiejkolwiek wiadomości. Artykuł [6] skupia się na badaniu użyteczności programów pocztowych przez osoby niewidome. Wyniki pokazały, że najmniej problemów sprawia czytanie, wysyłanie i przeszukiwanie e-maili, zaś problematyczne były m.in. organizacja wiadomości i kontaktów oraz używanie kalendarza. Wskazuje się przy tym na problemy z nawigacją w interfejsach, a także na słabą wydajność aplikacji webowych w porównaniu do desktopowych. Oba artykuły mają ponad dziesięć lat, i nie uwzględniają zmian, jakie zaszły w programach pocztowych od tamtego okresu.

Zdecydowanie więcej jest prac dotyczących bezpieczeństwa poczty elektronicznej. Znaczna część z nich skupia się na wykrywaniu wiadomości zawierających różne rodzaje ataków. Artykuł [1] przedstawia mechanizm filtrowania niechcianych wiadomości napisany w Pythonie z użyciem algorytmów maszyny wektorów nośnych (SVM) i naiwnego Bayesa z różnymi rodzajami funkcji jądra i wyboru zmiennych (feature selection). Wśród badanych algorytmów najwyższą skutecznością wykazały się SVM z linearnym jądrem oraz TF-IDF. Podobną tematykę podejmuje artykuł [7], który opisuje badanie różnych rodzajów algorytmów klasyfikacji i ich skuteczności w wykrywaniu wiadomości zawierających różne rodzaje ataków. W badaniach najbardziej skuteczny okazał się algorytm Naive Bayes w połączeniu z TF-IDF. W artykule [8] zaproponowano program pocztowy wykrywający i klasyfikujący wiadomości e-mail zawierające ataki typu spoofing na bazie programu zaprojektowanego w artykule [9] z użyciem protokołu SSL. Program wykazał się wysoką skutecznością w zwalczaniu niebezpiecznych wiadomości e-mail i powiadamianiu o nich, a elastyczność jego kodu pozwala na przekształcenie go we wtyczkę do istniejących już webowych programów.

Istotną część artykułów stanowiły analizy treści różnych niebezpiecznych wiadomości e-mail. W ramach artykułu [10] przeprowadzono przegląd takich wiadomości oraz różnych rodzajów ataków w nich zawartych, a także sposobów bronienia się przed nimi i dostępnych narzędzi do analizy kryminalistycznej. Zdaniem autorów każde z badanych narzędzi sprawdza się w innych scenariuszach, i najlepiej, gdy są one używane razem. Artykuł [11] stanowi dogłębną analizę wiadomości e-mail zawierających ataki typu phishing. Przeanalizowane zostały konta nadawców, dane zawarte w wiadomościach oraz ich treść, po czym sklasyfikowano je na podstawie znalezionych w nich celów.

W artykule [12] opisano zaś przeprowadzoną wśród studentów z Arabii Saudyjskiej ankietę badającą świadomość o bezpieczeństwie oprogramowania, w tym pocztowego, a także poziom wiedzy o cyberbezpieczeństwie i jego skutkach. Przeprowadzona ankieta pozytywnie wpłynęła na świadomość o kwestiach związanych z bezpieczeństwem oprogramowania wśród studentów – świadomość o bezpieczeństwie programów pocztowych zwiększyła się nawet o 31%. Stwierdzono, że świadomość może być zwiększona jeszcze bardziej poprzez uwzględnienie innych zagadnień w kolejnych badaniach.

Przeprowadzona analiza literatury wykazała, że niewiele jest badań dotyczących ergonomii programów pocztowych, w szczególności w ostatnich latach. Badań dotyczących bezpieczeństwa jest więcej, jednak rzadko kiedy skupiają się one na programach pocztowych, a bardziej na samych wiadomościach e-mail. Stąd też istnieje potrzeba przeprowadzenia nowych badań skupiających się na programach, uwzględniając zmiany, jakie zaszły w nich w ostatnich latach oraz większą liczbę problemów dotyczących cyberbezpieczeństwa.

4. Materiał i metody

4.1. Badane programy i stanowisko badawcze

W ramach badań przebadanych zostanie dziesięć popularnych programów pocztowych, wybranych na podstawie ich popularności w Polsce, rodzaju (desktopowe i webowe) oraz systemów operacyjnych, na jakie są one dostępne:

1. Gmail,
2. Apple Mail,
3. Outlook,
4. Poczta Onet,
5. Poczta WP,
6. Poczta Interia,
7. Proton Mail,
8. Mozilla Thunderbird,
9. eM Client,
10. Evolution.

Badanie zostało przeprowadzone na stanowisku badawczym, którego główny element sprzętowy to laptop Lenovo Legion 5 15ACH6H [13]. Zainstalowano na nim dwie maszyny wirtualne – pierwsza z systemem operacyjnym Windows 10, druga z systemem Linux Mint – na jakich będą uruchamiane poszczególne programy pocztowe. Ponadto na obu maszynach został zainstalowany program do pomiarów myszki i klawiatury Mousotron [14].

4.2. Grupy badawcze

W pierwszej części badania wzięła udział grupa badawcza składająca się z osiemnastu osób – studentów informatyki, oraz innych osób, które mają codzienną styczność z programami pocztowymi. W tej grupie testowano oprogramowanie dla systemów Windows 10 i Linux Mint. W drugiej grupie badawczej, liczącej 20 studentów przetestowano oprogramowanie Apple Mail dla systemu macOS Sequoia. Ze stanowiskiem badawczym w pierwszej grupie łączono się zdalnie za pomocą programu

RustDesk. Przebieg przeprowadzania pomiarów regularnie nadzorowano w celu uniknięcia ewentualnych błędów. Z uwagi na brak kompatybilności programu Mousotron z systemem macOS [14] do pomiarów myszki został wykorzystany płatny program o podobnej funkcjonalności o nazwie Mouse Metrics [15].

4.3. Badanie intuicyjności i ergonomii programów pocztowych

Pierwsze badanie polegało na sprawdzeniu intuicyjności i dostępności interfejsów najpopularniejszych programów pocztowych. Uczestnicy mieli za zadanie wykonanie podstawowych czynności związanych z pocztą elektroniczną, a także zmierzenie w tym czasie następujących parametrów:

- czas wykonania danej czynności (w sekundach, z dokładnością 0,1 s), mierzony za pomocą stopera,
- długość ruchu kursora myszki w trakcie wykonywania czynności (w milimetrach), mierzona za pomocą programu Mousotron,
- liczba kliknięć przycisków myszki potrzebna do wykonania czynności, mierzona za pomocą programu Mousotron.

Sformułowano sześć scenariuszy badawczych do wykonania w każdym z badanych programów. Dotyczyły one podstawowych funkcjonalności programów pocztowych. Do czynności tych należą:

1. Utworzenie i wysłanie nowej wiadomości e-mail.
2. Wysłanie odpowiedzi na wcześniej utworzoną wiadomość i dołączenie do niej załącznika.
3. Utworzenie i wysłanie nowej wiadomości e-mail z wieloma adresatami.
4. Usunięcie wiadomości i opróżnienie kosza.
5. Wyszukanie wiadomości z danym słowem w jej treści i przejście do niej z poziomu wyszukiwarki.
6. Dodanie nowego adresata do kontaktów.

Liczba kliknięć oraz długość ruchu myszki były mierzone w trakcie wykonywania czynności przez program Mousotron [14], zaś czas był mierzony za pomocą stopera wbudowanego w aplikację zegara dla smartfonów OnePlus [16]. Każdy wykonany pomiar czasu uproszczono przy spisywaniu do liczby sekund z dokładnością 0,1 s. W celu skrócenia czasu wykonywania badania, czasy pisania wiadomości ze scenariuszy 1-3 zmierzono przed rozpoczęciem jego wykonywania, a następnie doliczono do łącznego czasu wykonania każdego scenariusza. Po pomyślnym wykonaniu scenariusza pomiary w programie Mousotron były wyzerowywane.

Po ukończeniu badania obliczono średnie i mediany zmierzonych parametrów dla poszczególnych scenariuszy, oddzielnie dla każdego badanego programu, a następnie z pomocą tych obliczeń została obliczona średnia i mediana dla poszczególnych scenariuszy dla wszystkich programów. Średnia dla pojedynczego programu została obliczona z następującego wzoru (1):

$$\overline{x_a} = \frac{x_1 + x_2 + x_3 + \cdots + x_n}{n} \tag{1}$$

gdzie n to liczba osób uczestniczących w badaniu, x_n to wartość konkretnego przeprowadzonego pomiaru, a a to numer scenariusza, dla którego obliczana jest średnia.

Średnią dla wszystkich programów obliczono z użyciem tego samego wzoru, gdzie w tym przypadku n to liczba obliczonych średnich dla pojedynczych programów, zaś x_n to wartość danej średniej. Mediana dla pojedynczego programu została ustalona poprzez zestawienie ze sobą wartości zmierzonych dla danego scenariusza przez poszczególnych uczestników od najmniejszej do największej, wybranie dwóch wartości znajdujących się pośrodku (jako że liczba uczestników badania jest parzysta) oraz obliczenie ich średniej arytmetycznej. Proces ten można opisać wzorem (2):

$$M = \frac{x_{n/2} + x_{n/2+1}}{2} \tag{2}$$

gdzie n to liczba osób uczestniczących w badaniu, a $x_{n/2}$ i $x_{n/2+1}$ to dwie wyznaczone wartości środkowe [17]. Analogicznie, jednak z pomocą wcześniej obliczonych median została obliczona mediana łączna dla wszystkich programów.

Wyniki badań, przedstawione na wykresach znajdują się w rozdziale 5.

4.4. Badanie intuicyjności i ergonomii programów pocztowych – metoda KLM

Do wykonania obliczeń związanych z tym badaniem została użyta również metoda Keystroke-Level Model (KLM), pozwalająca na obliczenie czasu wymaganego do wykonania danej czynności na sprzęcie komputerowym. Autorzy tej metody zakładają sześć różnych czynności, które składają się na wykonanie danej operacji na komputerze:

- K – naciśnięcie klawisza lub przycisku na klawiaturze – średni czas: od 0,08 s do 1,20 s, zazwyczaj 0,28 s,
- P – nakierowanie kursora na dany cel za pomocą myszki – średni czas: 1,10 s,
- H – skierowanie dłoni na klawiaturę lub inne urządzenie – średni czas: 0,40 s,
- D – manualne rysowanie n prostych linii o łącznej długości m cm – średni czas: $0{,}9n+0{,}16m$ s,
- M – przygotowanie mentalne na wykonanie danej akcji – średni czas: 1,35 s,
- R(t) (albo W(t)) – czas reakcji systemu o długości t sekund [18].

Ponadto kilka lat później zdefiniowano jeszcze B, czyli naciśnięcie danego przycisku myszki o średnim czasie 0,1 s [19].

Czas wykonania czynności oblicza się poprzez wykonanie danej akcji w programie, spisanie poszczególnych czynności wykonanych przed i w trakcie jej wykonywania oraz dodanie ich średnich czasów zdefiniowanych przez autorów metody do siebie. W trakcie badania zostały zmierzone czasy wykonania każdego scenariusza dla każdego badanego programu. Po zmierzeniu wszystkich czasów w analogiczny sposób, jak w głównym

badaniu obliczono średnie (z użyciem wzoru (1)) i mediany dla każdego scenariusza dla wszystkich programów. Metoda ta nie uwzględnia czynników takich, jak czytelność interfejsu, błędy użytkownika czy obecność alternatywnych ścieżek [20], dlatego też użyto jej tylko w celu porównania jej wyników z wynikami głównego badania.

4.5. Badanie bezpieczeństwa programów pocztowych

Drugie badanie polegało na zweryfikowaniu zabezpieczeń przed niebezpiecznymi treściami w wiadomościach e-mail, w szczególności pod kątem linków i załączników, jakie są zawarte w badanych programach, a także mechanizmów powiadamiania o nich użytkownika.

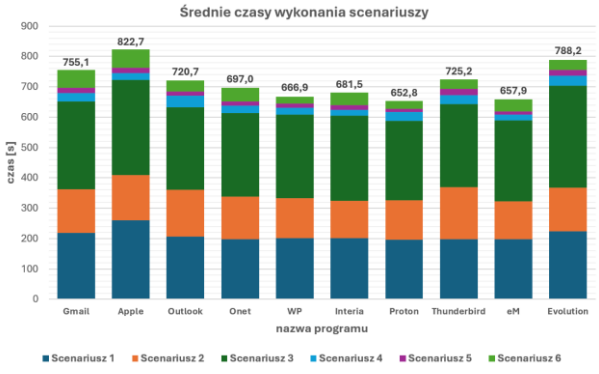
Na potrzeby badania wykorzystano kilka skrzynek pocztowych podzielonych na dwie grupy. Pierwsza grupa to konta użyte w pierwszym badaniu. Druga grupa to nowo założone skrzynki w usłudze Proton Mail, z których na wcześniejsze skrzynki wysyłano wiadomości z różnymi rodzajami zagrożeń cyberbezpieczeństwa.

W badanych programach pocztowych przeanalizowano zachowanie podczas: odbierania i odczytywania danej wiadomości, klikania w zawarty w niej link, próby pobrania załączonego pliku, a także przekazywania wiadomości innemu odbiorcy. Ponadto zostały sprawdzone ich ustawienia, w szczególności te dotyczące bezpieczeństwa użytkownika, ale także ustawienia prywatności, w tym te dotyczące wysyłania statystyk użytkowania czy przetwarzania danych osobowych. Na ocenę programu wpłynęła również analiza luk bezpieczeństwa, która została przeprowadzona po skończeniu właściwego badania.

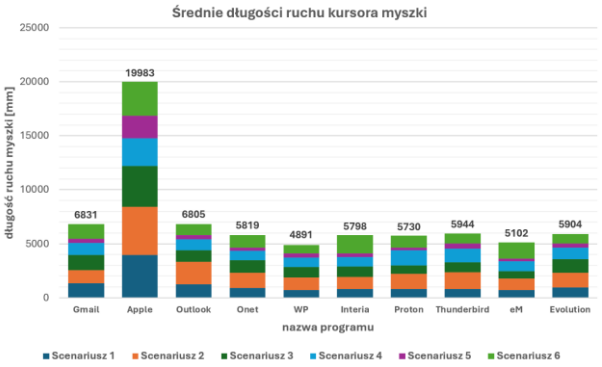
5. Wyniki badań

5.1. Wyniki badania ergonomii

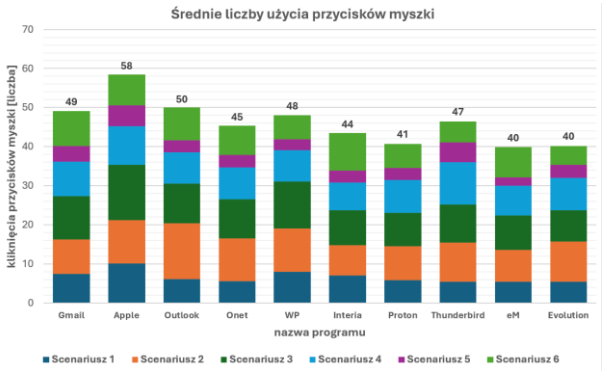
Na rysunkach 1-3 zostały przedstawione średnie czasy, długości ruchu kursora i liczby kliknięć myszki dla każdego scenariusza w poszczególnych programach, obliczone z pomiarów wykonanych przez użytkowników.



Rysunek 1: Średnie czasy wykonania scenariuszy dla poszczególnych programów.

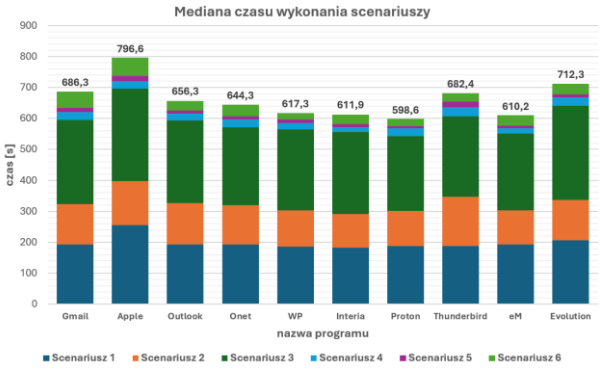


Rysunek 2: Średnie długości ruchu kursora myszki przebyte podczas wykonania scenariuszy dla poszczególnych programów.

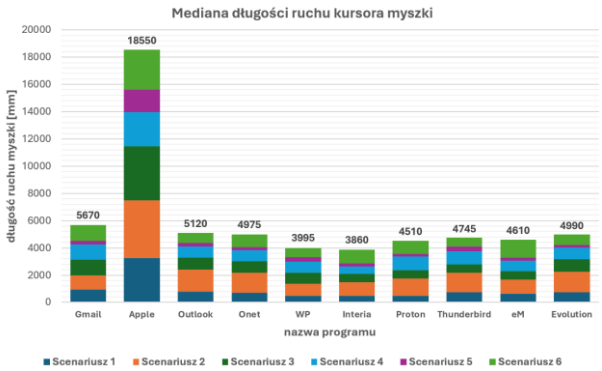


Rysunek 3: Średnie liczby użycia przycisków myszki wykonanych podczas wykonania scenariuszy dla poszczególnych programów.

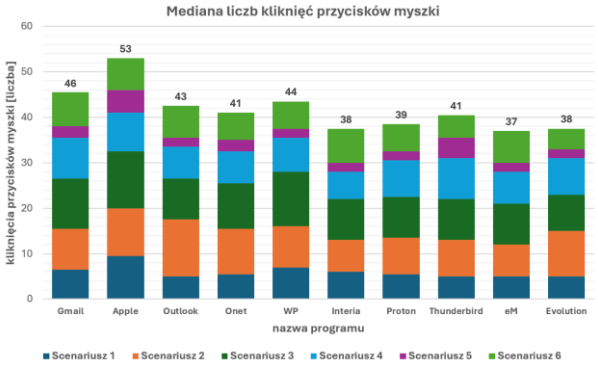
Rysunki 4-6 przedstawiają mediany poszczególnych pomiarów czasów dla badanych programów.



Rysunek 4: Mediana czasu wykonania scenariuszy dla poszczególnych programów.



Rysunek 5: Mediana długości ruchu kursora myszki przebytych podczas wykonania scenariuszy dla poszczególnych programów.



Rysunek 6: Mediana liczb użycia przycisków myszki wykonanych podczas wykonania scenariuszy dla poszczególnych programów.

Wśród badanych programów pocztowych wykonanie poszczególnych czynności zajęło łącznie najmniej czasu w programach Proton Mail (652,8 s) i eM Client (657,9 s). Do ich wykonania potrzebowano najmniejszej długości ruchów myszki w Poczcie WP (4891 mm) i w eM Client (5102 mm). W eM Client i w Evolution poszczególne czynności z kolei wymagały najmniejszej liczby kliknięć jej przycisków (po 40 kliknięć). W każdym z tych aspektów najbardziej wyraźnie przegrał program pocztowy od Apple'a (822,7 s, 19983 mm, 58 kliknięć), gorzej od większości programów wypadł również Gmail (755,1 mm, 6831 mm, 49 kliknięć).

5.2. Analiza wyników

5.2.1. Badanie ergonomii – obserwacje i uwagi

W trakcie badania ergonomii programów pocztowych nie stwierdzono większych problemów z wykonywaniem scenariuszy przez uczestników, zdarzały się jednak przypadki, kiedy przed wykonaniem kolejnego scenariusza pomiary nie zostały zresetowane, albo zapominano o napisaniu tytułu wiadomości czy umieszczeniu załącznika, i wtedy należało wykonać czynność od nowa. Ponadto u niektórych uczestników stwierdzono wyraźnie wyższy czas wykonywania części czynności, niż u pozostałych – w szczególności w scenariuszach 1-3, w których konieczne było przepisanie wiadomości z klawiatury.

W trakcie badania zauważono, że wraz z kolejnymi programami stopniowo poprawiało się obeznanie uczestników z poszczególnymi czynnościami, dzięki czemu wykonywano je sprawniej i szybciej. Najprawdopodobniej to właśnie miało negatywny wpływ na wyniki programów Gmail i Outlook. W przypadku programu Apple Mail tak słaby wynik wynika prawdopodobnie z faktu, że u większości badających go osób stwierdzono jedynie powierzchowną styczność z systemem macOS. U tych osób powszechne było mylenie przycisków na klawiaturze z uwagi na inną jej budowę.

W niektórych programach znalezienie elementów interfejsu odpowiadających za dodanie załącznika do wiadomości czy przejście do listy kontaktów pochłaniało więcej czasu, szczególnie tam, gdzie były one oznaczone jedynie małą ikoną. Te elementy powinny być bardziej wyszczególnione, aby dostęp do związanych z nimi funkcji był łatwiejszy. Powinno być również sprawdzane skalowanie ich interfejsów w różnych rozmiarach okna – w niektórych programach zmniejszenie jego rozmiaru powodowało, że część elementów interfejsu albo znikała, albo wyświetlała się w nieprawidłowy sposób.

Wyniki badania potwierdzają obserwację zawartą we wnioskach w artykule [5], gdzie zwrócono uwagę na brak umiejętności wykonywania podstawowych czynności w oprogramowaniu mimo w miarę dobrego obeznania z nim. Zgodne z prawdą jest również stwierdzenie dotyczące potrzeby pomocy przy wykonywaniu scenariuszy częściej, niż jest to widoczne. W artykule [6] pada z kolei stwierdzenie, że u użytkowników webowych programów częsty jest problem ze skupieniem się na konkretnej części interfejsu na rzecz interfejsu przeglądarki internetowej – w przeprowadzonym tutaj badaniu nie zostało to zauważone, a nawet jeśli takie momenty następowały, to nie miały one wyraźnego wpływu na wyniki.

Czasy obliczone metodą KLM w przeciwieństwie do czasów zmierzonych w trakcie głównego badania są bardzo zbliżone dla każdego programu – wynika to z tego, że metoda ta zakłada, że istnieje tylko jedna możliwa ścieżka, za pomocą której można wykonać daną czynność, i że czas potrzebny np. na zlokalizowanie danego przycisku czy wpisanie znaku na klawiaturze zawsze jest taki sam. Różnice w czasach wynikają z różnic w ścieżkach wykonania czynności między programami. Brakuje również możliwości zweryfikowania stopnia obeznania z interfejsami poszczególnych programów przez użytkowników

5.2.2. Analiza zabezpieczeń przed zagrożeniami

Badanie bezpieczeństwa rozpoczęto od analizy zabezpieczeń poszczególnych programów przed różnorakimi zagrożeniami. W każdym z tych programów odebrano sześć wiadomości, które zawierały poniższe rodzaje zagrożeń bezpieczeństwa:

1. Spam,
2. Spam z wieloma adresatami jednocześnie,
3. Niebezpieczny załącznik,
4. Niebezpieczny link,
5. Niebezpieczny link i załącznik jednocześnie,
6. Phishing.

Przeanalizowane zostało zachowanie tych programów przy wykonywaniu różnych interakcji z otrzymanymi wiadomościami, w tym dotyczących klikania na zawarte w nich linki i załączniki.

Badania wykazały, ze najlepiej działającym z testowanych mechanizmów był filtr antyspamowy. Aż 8 z 10 programów oznaczyło poprawnie przynajmniej jedną z otrzymanych wiadomości jako spam. Najczęściej jako spam oznaczane były wiadomości 1 i 2, jednak programy pocztowe Onetu i Interii oznaczyły w ten sposób również wiadomość 6, testującą mechanizmy antyphishingowe. Większość badanych programów (oprócz Thunderbirda i Evolution) ponadto posiada możliwość dodania własnych reguł pozwalających na rozszerzenie zakresu działania filtru antyspamowego.

Nieco inaczej sytuacja wygląda w przypadku potencjalnie niebezpiecznych linków i załączników. Mimo, że

wiele badanych programów teoretycznie posiada mechanizmy skanujące wiadomości w poszukiwaniu takowych, to jedynie Gmail wykrył niebezpieczny załącznik w jednej z nich (wiadomość 5) i zablokował jej odbiór. Co więcej, wiadomość 3, w której również został zawarty niebezpieczny załącznik nie tylko nie została zablokowana, ale jednocześnie załącznik został oznaczony jako bezpieczny. Pozostałe programy nawet nie próbowały ostrzec użytkownika przed zagrożeniem przed pobraniem załączników. Żaden z programów nie oznaczył również zawartych linków jako niebezpieczne, jednak Poczta WP i Proton Mail przy klikaniu w każdy link proszą użytkownika o potwierdzenie przejścia do danej strony – Poczta WP jednocześnie ostrzega użytkownika o możliwych zagrożeniach, jakie z tym się wiążą.

Zawiodły również mechanizmy antyphishingowe – wiadomość 6 nie została oznaczona przez żaden program w trakcie testów jako próba wyłudzenia danych. Niewykluczone jest, że wszystkie te mechanizmy byłyby bardziej skuteczne w pojedynku z autentycznymi, niebezpiecznymi wiadomościami, jednak zweryfikowanie tego w praktyce byłoby jednocześnie czasochłonne (w szczególności, gdy należy sprawdzić wszystkie badane mechanizmy) i ryzykowne.

5.2.3. Analiza ustawień bezpieczeństwa i prywatności

Elementem badania bezpieczeństwa programów pocztowych było również sprawdzenie ustawień tych programów pod kątem możliwości dostosowania mechanizmów bezpieczeństwa oraz opcji prywatności. W większości badanych programów dostępne dla użytkownika ustawienia są podstawowe – żaden z nich nie oferuje np. możliwości wyłączenia czy skorygowania ustawień skanowania linków i załączników w wiadomościach e-mail, a w niektórych z nich zabrakło nawet czarnej listy nadawców. Najczęściej badane programy pozwalają na dostosowanie działania filtra antyspamowego, głównie poprzez możliwość definiowania własnych reguł antyspamowych, a także m.in. poprzez umożliwienie usuwania niechcianych wiadomości zamiast przenoszenia ich do odpowiedniego folderu. Najbardziej rozbudowane reguły antyspamowe można utworzyć w programach Apple Mail, Gmail i w Poczcie WP, w Poczcie Interii możliwe jest tylko dodawanie do filtra poszczególnych adresów nadawców, zaś Outlook umożliwia jedynie zwiększenie skuteczności filtra poprzez ustawienie jego trybu na ścisły.

Proton Mail oferuje szereg dodatkowych opcji, takich jak automatyczne anulowanie subskrypcji newsletterów, blokowanie śledzenia czy zaawansowana ochrona konta przed włamaniem. Pokaźną liczbę takich ustawień posiadają również Thunderbird i Outlook. W programach obsługujących skrzynki wielu dostawców zestaw ustawień bezpieczeństwa wygląda trochę inaczej – nie ma w nich np. rozbudowanych ustawień filtra antyspamowego czy weryfikacji dwuetapowej, dlatego też przy korzystaniu z nich ważne jest również przejrzenie i modyfikacja ustawień z poziomu przeglądarki. Powszechne jest za to blokowanie zdalnych mediów w treściach wiadomości, a także szyfrowanie e-maili. Apple Mail jako jedyny posiada ochronę aktywności poprzez ukrywanie adresu IP. Gmail oraz poczta WP, Onetu i Interii posiadają zdecydowanie najmniej ustawień bezpieczeństwa.

Część badanych programów ma również możliwość wyłączenia części mechanizmów wpływających negatywnie na prywatność użytkownika, takich jak wysyłanie statystyk jego użytkowania czy personalizacja reklam. Należący do Google'a Gmail pozwala jedynie na wyłączenie personalizacji reklam wyświetlanych w programie – jest to szczególnie istotne ze względu na fakt, że Google jest znany ze zbierania dużej liczby danych o użytkownikach [21]. Outlook należący do Microsoftu oferuje dla odmiany dużo bardziej rozbudowane opcje – niestety nie jest możliwe wyłączenie zbierania podstawowych danych o użytkowniku, ale można wyłączyć np. zewnętrzne pliki cookie, możliwość dostępu do danych na urządzeniu, geolokalizację i więcej. Na wyłączenie zbierania danych o użytkownikach pozwalają w pełni Proton Mail i Thunderbird.

5.2.4. Analiza incydentów bezpieczeństwa

W celu przeprowadzenia analizy incydentów bezpieczeństwa związanych z badanymi programami zostały przeszukane rekordy znajdujące się w bazie rekordów CVE [22], opisujących znane luki i incydenty bezpieczeństwa w popularnym oprogramowaniu, wraz z informacjami dotyczącymi ich usunięcia. Najwięcej, bo 1525 luk w bazie posiada program Thunderbird, gdzie dotyczą one np. problemów z przechowywaniem danych w pamięci, błędów z kodzie, a także możliwości wykonania dowolnego, również złośliwego kodu [23]. Na drugim miejscu jest Outlook z 271 rekordami w bazie – luki znalezione w tym programie wiązały się zazwyczaj z wymuszeniem podwyższenia przywilejów, wyciekami danych czy możliwością zdalnego wykonania dowolnego złośliwego kodu z jego poziomu [24]. Trzecim najczęściej występującym programem w bazie jest Apple Mail – tam luki dotyczyły m.in. przejęcia przez hakera kontroli nad skrzynką pocztową. Warto dodać, że wszystkie z nich zostały wykryte w 2018 roku lub wcześniej [25].

W przypadku Gmaila baza CVE zwraca siedemnaście rekordów, i wszystkie z nich nie dotyczą bezpośrednio jego, a aplikacji wykorzystujących jego skrzynkę pocztową [26]. Znany jest jeden incydent dotyczący programu eM Client, dotyczący możliwości wykonania ataku man-in-the-middle poprzez wysłanie jednej wiadomości e-mail [27]. Baza uwzględnia również ok. dwadzieścia luk wykrytych w programie Evolution [28]. Poza bazą CVE znany jest również jeden incydent bezpieczeństwa wykryty w Poczcie Onet [29]. W bazie jak na razie nie znajduje się żaden rekord dotyczący programu Proton Mail.

W tabeli 1. zawarto liczbę rekordów CVE znalezionych dla poszczególnych programów.

Tabela 1: Liczba luk bezpieczeństwa wykrytych w poszczególnych programach pocztowych [22]

Program	Liczba luk
Gmail	17
Apple Mail	86
Outlook	271
Onet	0 (1 spoza bazy)
WP	0
Interia	0
Proton	0
Thunderbird	1525
eM Client	1
Evolution	20

6. Wnioski

Przeprowadzone badania pozwoliły na sprawdzenie, jakie preferencje dotyczące ergonomii w popularnych programach do obsługi poczty elektronicznej występują u użytkowników o różnym stopniu obeznania ze sprzętem komputerowym. Udało się wyszczególnić elementy, z którymi mieli oni największe problemy, a także słabości interfejsów poszczególnych programów. Możliwe stało się również zweryfikowanie działania poszczególnych wbudowanych w te programy mechanizmów zabezpieczających użytkownika przed zagrożeniami, a także wskazanie, które z nich należy rozbudować czy też poprawić. Obie postawione hipotezy badawcze zostały potwierdzone.

Na podstawie wyników pierwszego badania można stwierdzić, że najbardziej ergonomicznymi z badanych programów pocztowych są Proton Mail, poczta WP i eM Client. Najłatwiejszymi czynnościami dla uczestników były tworzenie i wysyłanie nowej wiadomości e-mail, zaś najwięcej problemów przysporzyło opróżnianie kosza z usuniętymi wiadomościami oraz dodanie nowego kontaktu. Często kłopotliwe dla uczestników było odnalezienie przycisku potrzebnego do wykonania czynności, gdy nie był wyróżniony spośród innych przycisków w jego sąsiedztwie – w szczególności dotyczyło to dodawania nowego załącznika oraz przejścia do listy kontaktów. Zauważono, że z każdą kolejną próbą poszczególne scenariusze były wykonywane przez uczestników coraz dokładniej i coraz szybciej. Czas wykonywania scenariuszy dotyczących wysyłania wiadomości e-mail zależał w największym stopniu od szybkości pisania na klawiaturze. Dowiedziono także, że metoda KLM nie jest zbyt miarodajną metodą w badaniu ergonomii programów pocztowych.

W badaniu bezpieczeństwa można wyróżnić dwa zwycięskie programy – Proton Mail i Outlook. Najsłabiej w kontekście działania mechanizmów i liczby ustawień bezpieczeństwa wypadają Poczta Onet, Poczta Interia i Evolution. Najlepiej działający i najbardziej rozbudowany (pod względem możliwości dodania własnych reguł) filtr antyspamowy posiadają Apple Mail, Gmail i Poczta WP. W większości programów zawiodły jednak mechanizmy zabezpieczające przed niebezpiecznymi linkami i załącznikami – tylko Gmail zablokował jedną taką wiadomość.

W celu zwiększenia bezpieczeństwa programów pocztowych powinno się pozwolić użytkownikowi na skanowanie nie tylko linków i załączników w wiadomościach od nieznanych nadawców, ale również u wszystkich pozostałych. Skanowanie powinno być też bardziej agresywne. Możliwe powinno być również dodawanie poszczególnych domen zawartych w linkach do czarnej i białej listy. Jeśli chodzi o konkretne programy – Gmail powinien umożliwić użytkownikowi wyłączenie mechanizmów takich, jak zbieranie danych diagnostycznych. W Outlooku i w innych badanych desktopowych programach brakuje możliwości definiowania własnych reguł antyspamowych. Z kolei w poczcie Onetu, WP i Interii mechanizmy bezpieczeństwa powinny zostać znacząco rozbudowane i przeprojektowane. Te programy posiadają również najwięcej reklam wśród badanych programów.

O ile działanie mechanizmów bezpieczeństwa w programach pocztowych jest często zależne od ich twórców, to jest możliwe samodzielne zabezpieczenie się przed związanymi z nimi zagrożeniami. Można to zrobić na następujące sposoby:

- używanie zaufanego, bezpiecznego klienta poczty elektronicznej,
- zainstalowanie rozszerzenia do przeglądarki internetowej blokującego reklamy i skrypty śledzące użytkownika,
- modyfikacja ustawień programu pocztowego i konta do własnych potrzeb,
- dokładne sprawdzanie treści dołączonych do wiadomości linków (w tym domen) przed ich kliknięciem,
- sprawdzanie załączników dołączonych do wiadomości przed ich otwarciem na komputerze,
- użycie sieci VPN do ukrycia swojego adresu IP oraz tożsamości.

Literatura

[1] Y. Fang, G. Mogos, Detecting attacks on e-mail, Indonesian Journal of Electrical Engineering and Computer Science 33(3) (2024) 1576–1588, https://doi.org/10.11591/ijeecs.v33.i3.pp1576-1588.

[2] How Many Emails Are Sent Per Day? (2023–2027), https://www.oberlo.com/statistics/how-many-emails-are-sent-per-day, [10.06.2024].

[3] A Comprehensive Guide to Email Threats and How to Protect Yourself, https://abusix.com/blog/a-comprehensive-guide-to-email-threats-and-how-to-protect-yourself, [26.03.2025].

[4] What Is Email Security? – Protect Against Email Threats, https://www.cisco.com/site/us/en/learn/topics/security/what-is-email-security.html, [26.03.2025].

[5] M. Eichelberger, I.B. Brubaker, "How do I send an Email?" : Technology Challenges for First-Year Students in the College Library, Library Hi Tech 33(3) (2015) 329–339, https://doi.org/10.1108/LHT-03-2015-0027.

[6] B. Wentz, J. Lazar, Usability Evaluation of Email Applications by Blind Users, Journal of Usability Studies 6(2) (2011) 75–89, https://doi.org/10.5555/2010380.2010384.

[7] L. Pullagura, D.M. Rao, N.V. Kumari, R. K. Lanke, S.K. Gowda Katta, R. Chiwariro, A Study of Suspicious E-Mail Detection Techniques, In 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (2024) 1120–1126, https://doi.org/10.1109/IDCIoT59759.2024.10467633.

[8] T.P. Fowdur, L. Veerasoo, An email application with active spoof monitoring and control, In 2016 International Conference on Computer Communication and Informatics (ICCCI) (2016) 1–6, https://doi.org/10.1109/ICCCI.2016.7480002.

[9] T.P. Fowdur, D. Mooloo, An SSL-Based Client-Oriented Anti-Spoofing Email Application, Proceedings of IEEE Africon (2013) 1–5, https://doi.org/10.1109/AFRCON.2013.6757757.

[10] E. Altulaihan, A. Alismail, M.M. Hafizur Rahman, A.A. Ibrahim, Email Security Issues, Tools, and Techniques Used in Investigation, Sustainability (Switzerland) 15(13) (2023) 10612, https://doi.org/10.3390/su151310612.

[11] L. Burita, P. Matoulek, K. Halouzka, P. Kozak, Analysis of phishing emails, AIMS Electronics and Electrical Engineering 5(1) (2021) 93–116, https://doi.org/10.3934/electreng.2021006.

[12] M.A. Alqahtani, Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis, Computational Intelligence and Neuroscience 2022 (2022) 1–12, https://doi.org/10.1155/2022/6775980.

[13] Specyfikacja laptopa Lenovo Legion 5 15ACH6H, https://psref.lenovo.com/syspool/Sys/PDF/Legion/Lenovo_Legion_5_15ACH6H/Lenovo_Legion_5_15ACH6H_Spec.pdf, [07.10.2024].

[14] Mousotron – strona główna programu, https://www.blacksunsoftware.com/mousotron.html, [10.10.2024].

[15] Aplikacja Mouse Metrics Distance & Click w Mac App Store, https://apps.apple.com/us/app/mouse-metrics-distance-click/id6737716371, [27.12.2024].

[16] Aplikacja OneplusClock w Google Play, https://play.google.com/store/apps/details?id=com.oneplus.deskclock&pli=1, [21.03.2025].

[17] Opis i wzór na medianę – Zintegrowana Platforma Edukacyjna, https://zpe.gov.pl/a/przeczytaj/D141WaQJ8, [15.04.2025].

[18] S.K. Card, T.P. Moran, A. Newell, The keystroke-level model for user performance time with interactive systems, Communications of the ACM 23(7) (1980) 396–410, https://doi.org/10.1145/358886.358895.

[19] D. Kieras, Using the Keystroke-Level Model to Estimate Execution Times, University of Michigan, Ann Arbor, 2001.

[20] A. Dampc, Keystroke level model, https://medium.com/archiwum-ux-watch/keystroke-level-model-5616238c9789, [12.06.2024].

[21] How Google Collects Data About You and the Internet, https://www.pingdom.com/blog/how-google-collects-data-about-you-and-the-internet/, [11.01.2025].

[22] Baza rekordów CVE – strona główna, https://cve.mitre.org/, [13.01.2025].

[23] Baza rekordów CVE – wyniki wyszukiwania dla hasła „thunderbird”, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=thunderbird, [13.01.2025].

[24] Baza rekordów CVE – wyniki wyszukiwania dla hasła „outlook”, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=outlook, [13.01.2025].

[25] Baza rekordów CVE – wyniki wyszukiwania dla hasła „apple mail”, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=apple+mail, [13.01.2025].

[26] Baza rekordów CVE – wyniki wyszukiwania dla hasła „gmail”, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=gmail, [13.01.2025].

[27] Baza rekordów CVE – opis rekordu CVE-2020-12618, https://www.cve.org/CVERecord?id=CVE-2020-12618, [13.01.2025].

[28] Baza rekordów CVE – wyniki wyszukiwania dla hasła „evolution”, https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=evolution, [13.01.2025].

[29] A. Haertle, Poważny błąd Onetu pozwalał pobrać pocztę i dane użytkowników, https://zaufanatrzeciastrona.pl/post/powazny-blad-onetu-udostepnial-poczte-i-dane-uzytkownikow/, [13.01.2025].