

ŚWIADOMOŚĆ ZAGROŻEŃ CYWILIZACYJNYCH

- **BEZPIECZEŃSTWO**
- **SAMOKONTROLA**
- **OSTROŻNOŚĆ**

Czy jesteśmy przygotowani do dalszych zmian ?

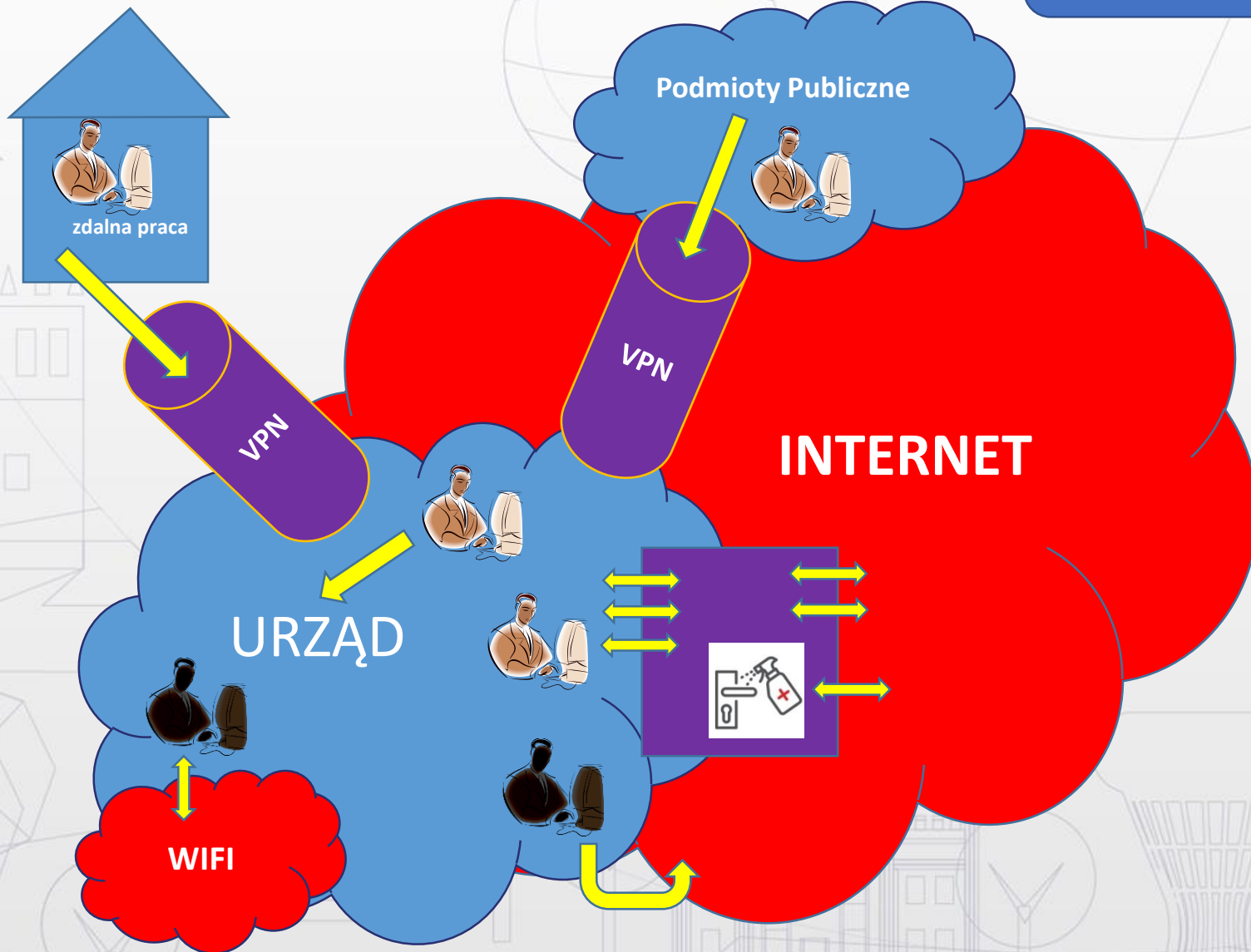
CUW – rozwiązanie hybrydowe, przepis na Smart Samorząd”

START

- **Infrastruktura**
- Zasoby ludzkie – specjaliści
- **Organizacja bezpieczeństwa**
- Budowanie kompetencji urzędników
- **Wdrożenie nowoczesnych rozwiązań systemowych**
- Zarządzanie, utrzymanie i rozwój systemów
- HelpDesk, szkolenia
- Propagowanie modelowych rozwiązań

META

BEZPIECZEŃSTWO – działania CUW



Świadomość

Odpowiedzialność

Ostrożność

Kopie danych

Wsparcie

Kontrola i audyty

Ransomware

ransom „okup” software „oprogramowanie”
szyfrowanie danych celem uzyskania okupu

Ooops, your files have been encrypted!



TIME LEFT 00:00:00

JAK USTRZEC SIĘ PRZED RANSOMWARE ?

- **Stać edukacja** użytkowników. Nawet najlepsze techniczne zabezpieczenia nie pomogą, jeśli użytkownicy nie będą przestrzegać podstawowych zasad bezpieczeństwa.
- Wykonuj regularnie **kopię zapasową** istotnych danych. Zadbaj o to, by co najmniej jedna kopia zapasowa była przechowywana na odizolowanym systemie, niedostępnym z maszyn, których kopie przechowuje. **Dane z dysku lokalnego nie są kopiowane przez IT.**
- Zadbaj o odpowiednią architekturę sieci. Wyodrębnij odpowiednie segmenty, zwróć szczególną uwagę na to, jakie usługi dostępne są pomiędzy poszczególnymi maszynami oraz z internetu.
 - Na bieżąco **aktualizuj system operacyjny** oraz oprogramowanie.
 - **Używaj aktualnego oprogramowania antywirusowego** na serwerze poczty oraz stacjach roboczych.

W PRZYPADKU ATAKU RANSOMWARE

- **Jak najszybciej odizoluj zarażone maszyny od reszty sieci** – odłącz je od wszelkich połączeń sieciowych (przewodowych i bezprzewodowych) oraz urządzeń do przechowywania plików (dyski przenośne i podobne).
- **Zrób zdjęcie ekranu z wyświetlanym komunikatem** przez ransomware. Upewnij się, że wszystkie informacje są na zdjęciu czytelne. Przegraj plik z notatką okupu (ransom note) i przykładowe zaszyfrowane pliki na czysty przenośny nośnik danych (np. pendrive) – będą jeszcze potrzebne.
- W celu zminimalizowania strat (zaszyfrowania wszystkich plików) **wyłącz komputer.**
- **IT rozważy zgłoszenie incydentu do CERT Polska** – najlepiej zaraz po wykryciu zdarzenia. W tym celu skorzysta z <https://incydent.cert.pl> oraz podejmie działania zabezpieczające i ewentualna próbę odszyfrowania danych.
- **Jeśli dysponujesz kopią zapasową, przygotuj nowy komputer, sformatuj dysk, zainstaluj system od nowa i przywróć dane z backupu.**
- Po usunięciu skutków ataku **ustal, w jaki sposób do niego doszło** oraz podejmij działania zapobiegawcze, by uniemożliwić powtórzenie się sytuacji (edukacja użytkowników, zabezpieczenia fizyczne, aktualizacja oprogramowania).

W PRZYPADKU ATAKU RANSOMWARE



Ooops, your files have been encrypted!

Polish

Co się zdarzyło z moim komputerem?

Twoje ważne pliki są szyfrowane. Wiele dokumentów, zdjęć, filmów, baz danych i innych plików nie jest już dostępnych, ponieważ zostały zaszyfrowane. Być może szukasz sposobu na odzyskanie plików, ale nie marnuj czasu. Nikt nie może odzyskać plików bez naszej usługi odszyfrowywania.

Czy mogę odzyskać moje pliki?

Pewnie. Gwarantujemy, że można odzyskać wszystkie pliki bezpiecznie i łatwo. Ale nie masz tyle czasu.

Możesz odszyfrować niektóre z plików za darmo. Spróbuj teraz klikając <Decrypt>.

Ale jeśli chcesz odszyfrować wszystkie pliki, musisz zapłacić.

Masz tylko 3 dni na przesłanie płatności. Następnie cena zostanie podwojona.

Ponadto, jeśli nie zapłacisz za 7 dni, nie będziesz w stanie odzyskać plików na zawsze.

Będziemy mieli wolne wydarzenia dla użytkowników, którzy są tak biedni, że nie mogli zapłacić za 6 miesięcy.

Jak mam zapłacić?

Płatność jest akceptowana tylko w programie Bitcoin. Aby uzyskać więcej informacji, kliknij przycisk <About bitcoin>.

Sprawdź bieżącą cenę Bitcoin i kup trochę bitcoinów. Aby uzyskać więcej informacji, kliknij opcję <How to buy bitcoins>.

Wyślij odpowiednią kwotę na adres podany w tym oknie.

Po dokonaniu płatności kliknij <Check Payment>. Najlepiej czas na sprawdzenie: 9:00 -

Payment will be raised on

5/15/2017 22:46:50

Time Left

02: 23: 59: 24

Your files will be lost on

5/19/2017 22:46:50

Time Left

06: 23: 59: 24

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

115p7UMMngo1pMvvpHijcRdfJNXj6LrLn

Copy

Check Payment

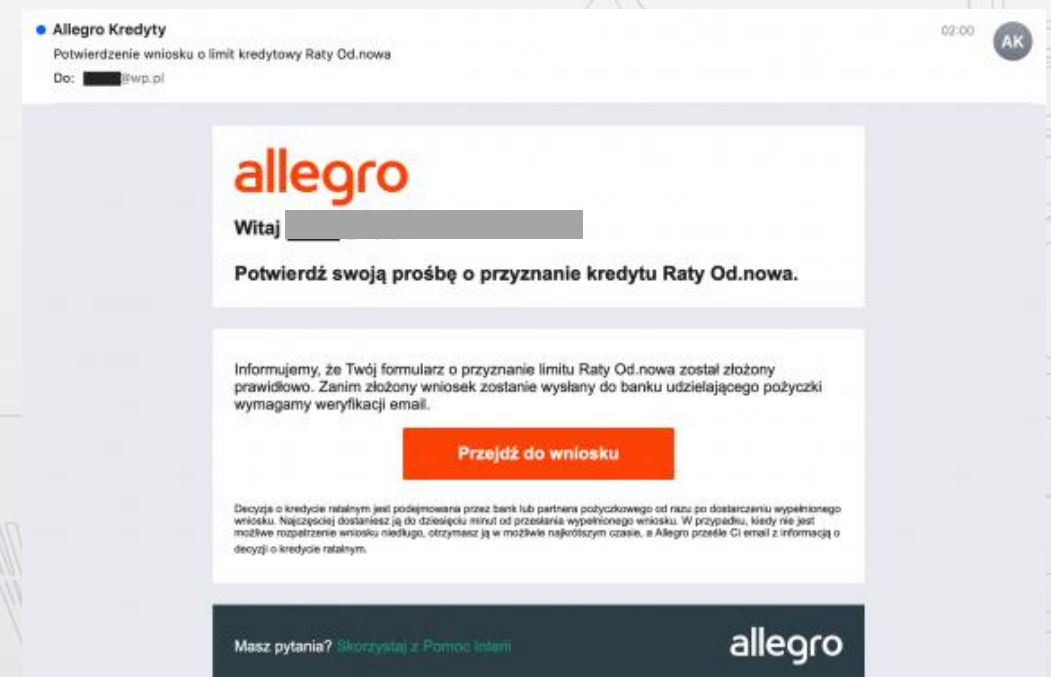
Decrypt

Źródło	Przyczyny			
	bezpośrednia	pośrednia		
poprzez e-maila	niskie zabezpieczenia na serwerze	brak oprogramowania antywirusowego na komputerze	jeszcze nie wykrywalny wirus	ignorowanie ostrzeżeń systemowych przez użytkownika
poprzez FTP	środowisko niezbyt bezpieczne			
poprzez pendrive	pendrive używany w kilku komputerach min. (w zawirusowanym)			
poprzez podłączenie do WIFI	sieć niezabezpieczona, łączona jest z siecią wewnętrzną urzędu			

Skutki		Jak przeciwdziałać ?					
zaszyfrowanie danych na komputerze	zaszyfrowanie danych na kilku komputerach (w przypadku udostępnianych folderów)	Aktualizować oprogramowanie serwera, analizować zagrożenia (logi), kupować wsparcie na urządzenia i systemy bezpieczeństwa.	PILNOWA: aby oprogramowanie Windows (System) i NOD 32 ESET były aktualne	nie otwierać e-maili nieoczekiwanych - ostrożność co do linków i poleceń	podnoszenie świadomości, ostrzeżenia IOD	wykonywanie kopii okresowo na taśmach	deponowanie dodatkowych kopii danych na izolowanych serwerach danych

UWAŻAJ NA PHISHING

Metoda oszustwa, w której **przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji** (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań.



Zagrożenia – fałszywy e-mail

https://pl-facebook.pl

Portal szkoleniowy CB... Podpisy można zbiera...

facebook

Adres e-mail lub numer telefonu: Hasło:

Zaloguj się

Nie pamiętasz nazwy konta?

Facebook pomaga kontaktować się z innymi osobami oraz udostępniać im różne informacje i materiały.



Rejestracja

To szybkie i proste.

Imię Nazwisko

Numer telefonu komórkowego lub e-mail

Nowe hasło

Data urodzenia

16 wrz 1994

Płeć

Kobieta Mężczyzna

Ustawienie niestandardowe

Klikając przycisk Rejestracja, akceptujesz nasz [Regulamin](#). [Zasady dotyczące danych](#) informują, w jaki sposób gromadzimy, użytkujemy i udostępniamy dane użytkowników, a [Zasady dotyczące plików cookie](#) informują jak korzystamy z plików cookie i podobnych technologii. Możesz otrzymywać powiadomienia SMS z Facebooka, z których możesz zrezygnować w dowolnej chwili.

Rejestracja

Czy to jest bezpieczna strona internetowa ? <https://pl-facebook.pl>

Zagrożenia – fałszywy e-mail

A screenshot of the real Facebook login page. The browser's address bar shows the URL <https://pl-pl.facebook.com>, which is circled in green. A green callout box points to this URL and contains the text: **TAK** wchodź
adres poprawny <https://pl-pl.facebook.com>. The page features the Facebook logo, a navigation bar with various links, and a login form with fields for 'Adres e-mail lub numer telefonu' and 'Hasło', and a blue 'Zaloguj się' button.

A screenshot of a fake Facebook login page. The browser's address bar shows the URL <https://www.facelook.com/fakepage.html>, which is circled in red. A red callout box points to this URL and contains the text: **NIE** wchodź. The page features a blue header with the Facebook logo and a login form with a field for 'Email or Phone' and a 'Keep me logged in' checkbox. The text 'Facebook helps you connect and share with the people in your life.' and 'Create' are visible at the bottom.

Zagrożenia – fałszywy e-mail

Podszywanie się pod pracowników banku



Film źródło YouTube: <https://www.youtube.com/watch?v=3C0piwRqt-o>

Zagrożenia – fałszywy e-mail

Od: [redacted]
Do: [redacted]
DW:
Temat: FW: ☹ Potwierdź szczegóły dostępu aby uniknąć zawieszenia aktywności e-mail ☹

From: Webmail Bezpieczeństwo <contact@notifysending.com>

Sent: Wednesday, December 4, 2019 8:47 AM

To: [redacted]@now.pl

Subject: ☹ Potwierdź szczegóły dostępu aby uniknąć zawieszenia aktywności e-mail ☹

roundcube
Polska Webmail Software

Drogi Kliencie umt.tarnow.pl,

Twój e-mail zostanie zawieszony z powodu kilku nieudanych prób logowania z urządzenia opisanego poniżej.

Potwierdź swoją tożsamość, naciskając przycisk poniżej. Następnie będziesz mógł wznowić swoją aktywność. Jeśli konto nie zostanie aktywowane w ciągu 48 godzin, nie będzie można się komunikować.

Powód:

Data: 2019-12-04

Powód: Logowanie nie powiodło się

Potwierdzać

NIE POTWIERDZAJ
!

SPAM – „MIELONKA” - NIECHCIANA POCZTA jak się chronić ?

- Oprogramowanie antywirusowe
- Świadome otwieranie poczty
- Filtry antyspamowe (zarządza IT)
- Adres lub domena nadawcy znajduje się na jednej z aktualizowanych codziennie list adresów wysyłających SPAM - globalne RBL (Realtime blacklist)
- Klasyfikatory , analizatory treści (zabezpiecza IT) - treść wiadomości zawiera słowa sklasyfikowane jako SPAM lub ma mały współczynnik tekstu do grafiki - w tym przypadku wszystko zależy, jak potraktują nas filtry; wysłana przez nas wiadomość może trafić do SPAMu lub nie

paradoks administracji 700 zł (opłata za bezpieczeństwo)

Kontroluj komputer - 10 przykazań

1. Będąc na stanowisku pracy nie używaj WIFI w laptopie podłączony do sieci internetowej.
2. Nie korzystaj na stanowisku z internetu smartfona.
3. Ogranicz korzystanie z Pendrive.
4. W sieci zawsze kieruj się zasadą ograniczonego zaufania i ćwicz swoją asertywność.
5. Czytaj regulaminy, komunikaty itp. – możesz tam znaleźć wiele ważnych informacji.
6. Unikaj usług ułatwiających Ci życie kosztem udostępniania Twoich danych,
7. Nie udostępniaj nikomu swoich haseł i zadbaj o ich siłę, unikalność i odpowiednie zabezpieczenie.

Kontroluj komputer - 13 przykazań

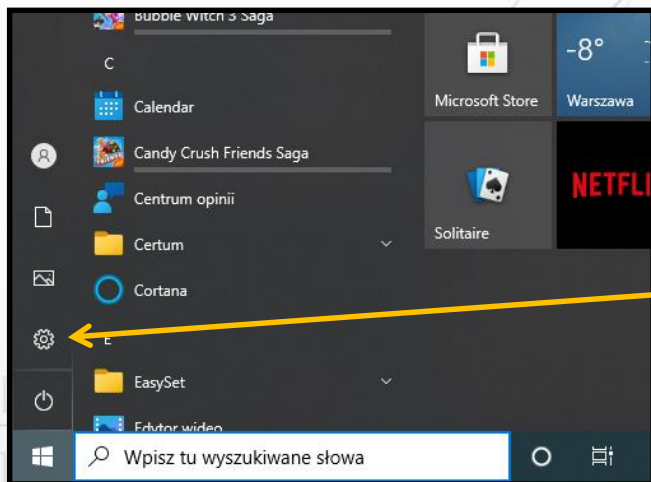
8. Nie udostępniaj nikomu swoich haseł i zadbaj o ich siłę, unikalność i odpowiednie zabezpieczenie.
9. Nie używaj w haśle swojego imienia i nazwiska ani związanych z Tobą informacji, np. daty urodzin, nr PESEL
10. Pamiętaj o zmianie hasła co pewien czas.
11. Nigdy nie używaj swojego imienia, identyfikatorów ani nicków jako hasła (nawet ze zmianą wielkości liter, pisane wspak). Nie używaj samych cyfr ani prostych pojedynczych słów.
12. Używaj wielkich liter, znaków specjalnych (.,*#@!^& etc.) i cyfr (najlepiej równocześnie).
13. Nie ignoruj informacji o wyciekach danych z serwisów, z których korzystasz. W razie wątpliwości zmień hasło.

Kontroluj „alerty” programu antywirusowego

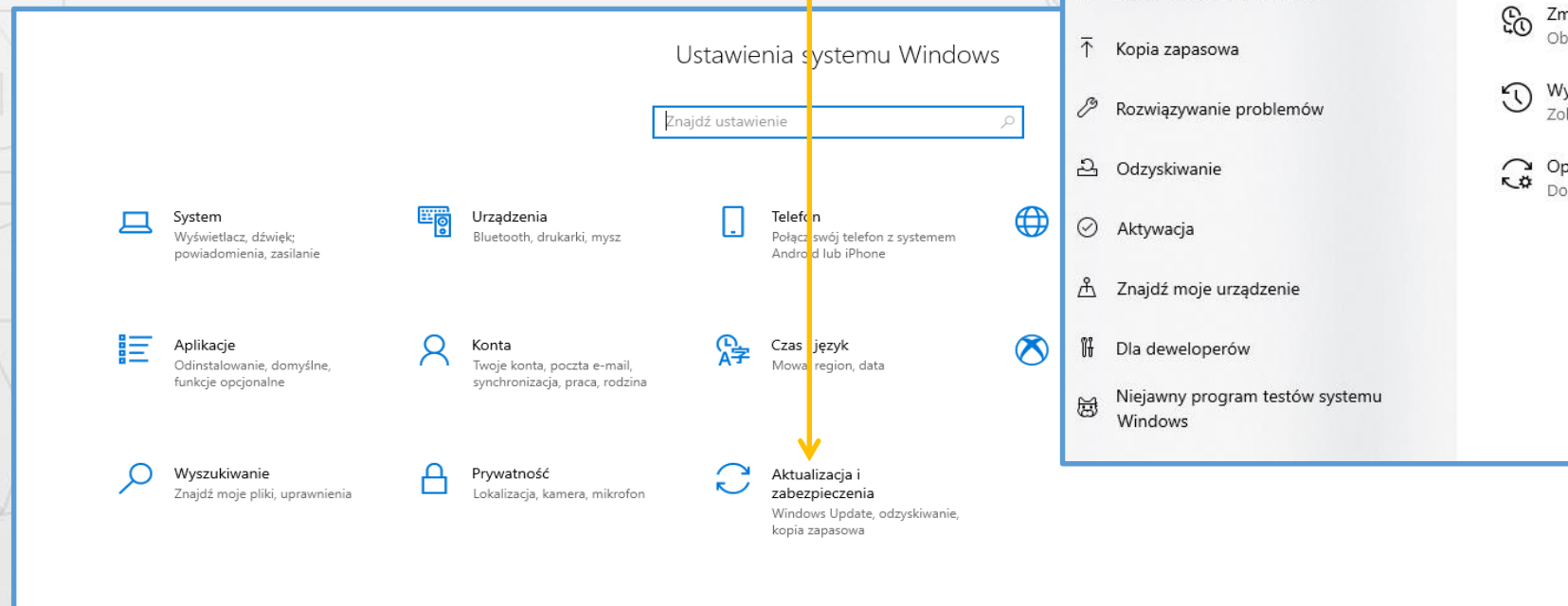
The image displays the ESET Endpoint Antivirus interface. The main window shows a green checkmark and the text "Maksymalna ochrona". Below this, it indicates "Licencja" with a validity date of 13.09.2021 and "Moduły są aktualne" with the last update on 18.02.2021 at 06:02:50. A sidebar on the left lists navigation options: STAN OCHRONY, SKANOWANIE KOMPUTERA, AKTUALIZACJA, USTAWIENIA, NARZĘDZIA, and POMOC I OBSŁUGA. An inset window titled "Stan ochrony" shows a warning icon and the text "ESET Endpoint Antivirus wymaga uwagi". It lists protection status for "Komputer" and "Internet i poczta e-mail", both at "Maksymalna ochrona". A red box highlights a warning: "System operacyjny nie jest aktualny" (The operating system is not up to date), with a message advising to install missing updates via Windows Update. Another inset shows the Windows taskbar with the system tray containing the ESET icon, the date 18.02.2021, and the time 08:20.

nie instaluj kilku programów antywirusowych, część stron/programów automatycznie proponuje instalację

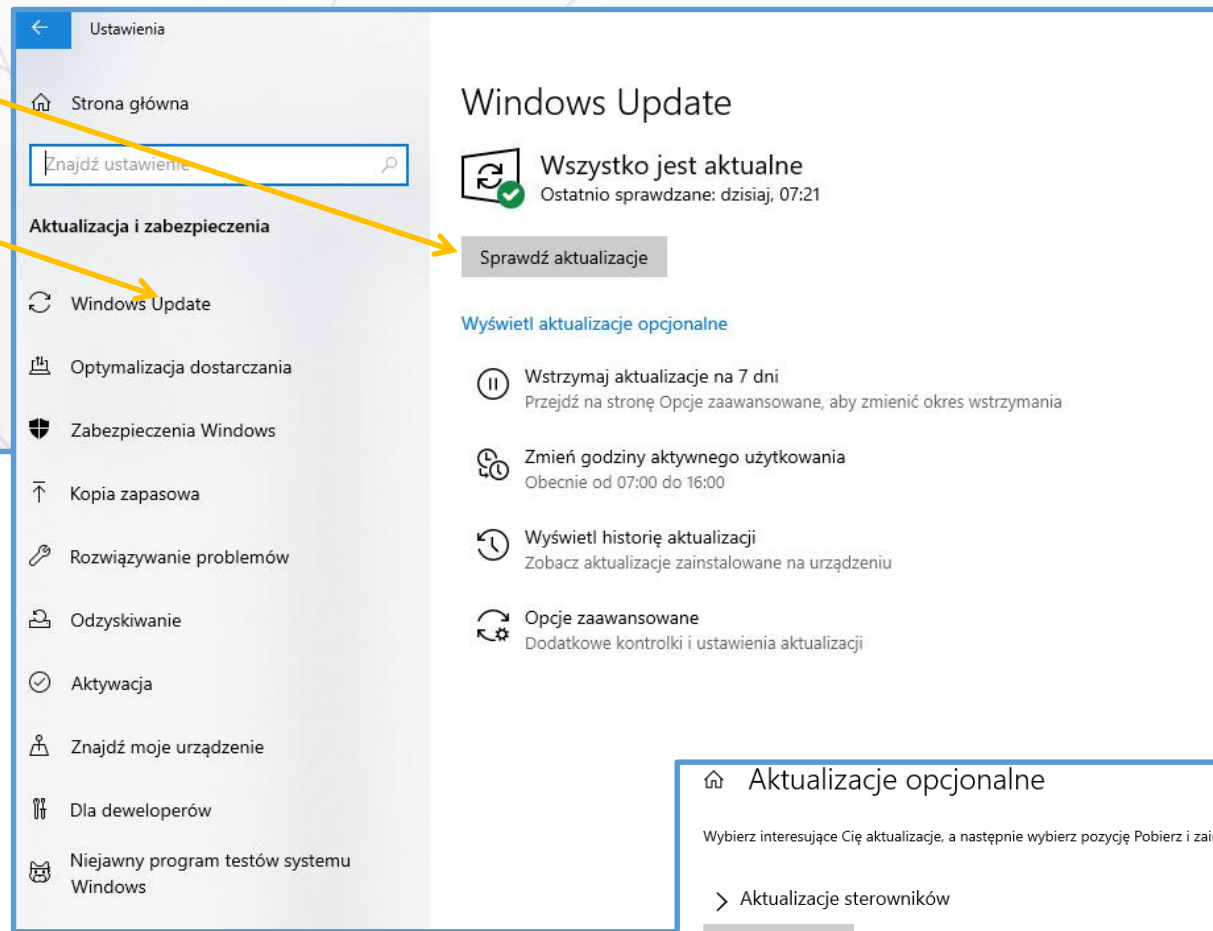
Kontroluj aktualizacje Windows 10 (menu Start)



1

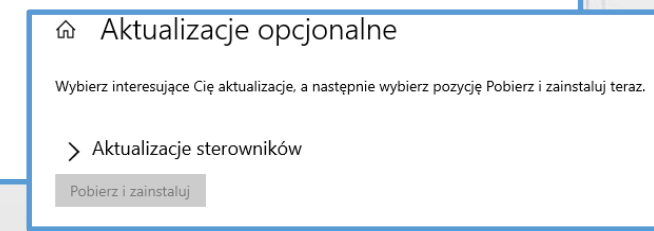


2



4

3



Aktualizacje opcjonalne

Wybierz interesujące Cię aktualizacje, a następnie wybierz pozycję Pobierz i zainstaluj teraz.

> Aktualizacje sterowników

Pobierz i zainstaluj

Aktualizuj przeglądarki internetowe (Google)

The image illustrates the process of updating Google Chrome. It features a main screenshot of the Chrome browser window with the Google logo and a menu open. Four numbered yellow circles (1-4) indicate the steps: 1. Clicking the menu icon (three dots) in the top right corner. 2. Selecting 'Ustawienia' (Settings) from the menu. 3. Selecting 'Pomoc' (Help) from the menu. 4. Clicking on the 'Masz aktualną wersję Google Chrome' (You have the latest version of Google Chrome) notification in the Windows Settings 'Ustawienia' (Settings) app. The 'Ustawienia' app is shown with the 'Potwierdzenie bezpieczeństwa' (Security) section highlighted in a yellow circle. The 'Chrome - informacje' (Chrome - About) page in the Settings app shows the current version as 88.0.4324.182 (Official version) and confirms it is the latest.

1

2

3

4

Ustawienia

Przeszukaj ustawienia

Ty i Google

Autouzupełnianie

Potwierdzenie bezpieczeństwa

Prywatność i bezpieczeństwo

Wyświetl

Wyszukiwarka

Domyślna przeglądarka

Po uruchomieniu

Zaawansowane

Rozszerzenia

Chrome - informacje

Chrome - informacje

Przeszukaj ustawienia

Google Chrome

Masz aktualną wersję Google Chrome

Wersja 88.0.4324.182 (Oficjalna wersja) (64-bitowa)

Pomoc do Chrome

Zgłoś problem

Google Chrome

Copyright 2021 Google LLC. Wszelkie prawa zastrzeżone.

Stworzenie przeglądarki Google Chrome było możliwe dzięki programom o otwartym kodzie źródłowym.

Warunki korzystania z usługi

Nowa karta Ctrl+T

Nowe okno Ctrl+N

Nowe okno incognito Ctrl+Shift+N

Historia

Pobrane pliki Ctrl+J

Zakładki

Powiększ - 100% +

Drukuj... Ctrl+P

Przesyłaj...

Znajdź Ctrl+F

Więcej narzędzi

Edytuj Wyciagnij Kopiuj Wklej

Ustawienia

Pomoc

Zakończ

Google Chrome - informacje

Centrum pomocy

Zgłoś problem Alt+Shift+I

Kontroluj w zakładce „ustawienia” zapisane hasła (Google)

1

2

3

4

skopiuj hasło
edytuj hasło
usuń

Ustawienia

Ty i Google

Autouzupełnianie

Potwierdzenie bezpieczeństwa

Prywatność i bezpieczeństwo

Wygląd

Wyszukiwarka

Domyślna przeglądarka

Po uruchomieniu

Zaawansowane

Rozszerzenia

Chrome – informacje

Przeszukaj ustawienia

Inteligentne rozwiązania

Synchronizacja i usługi Google

Nazwa i zdjęcie w Chrome

Importuj zakładki i ustawienia

Autouzupełnianie

Hasła

Formy płatności

Adresy i ustawienia

Ustawienia

Nowa karta Ctrl+T

Nowe okno Ctrl+N

Nowe okno incognito Ctrl+Shift+N

Historia

Pobrane pliki Ctrl+J

Zakładki

Powiększ - 100% +

Drukuj... Ctrl+P

Przesyłaj...

Znajdź Ctrl+F

Więcej narzędzi

Edytuj Wytnij Kopiuj Wklej

Ustawienia

Zakończ

Ustawienia

Szukaj haseł

Włączony

Włączony

Włączony

Zapisane hasła

Strona internetowa	Nazwa użytkownika	Hasło
🌐 [Redacted]	
Nigdy nie zapisane		
🌐 goonline.bnpparibas.pl		✕
🌐 login.microsoftonline.com		✕
🌐 pz.gov.pl		✕



Dziękuję za uwagę

Janusz Różycki - Inspektor Ochrony Danych Urzędu Miasta Tarnowa,

iod@umt.tarnow.pl