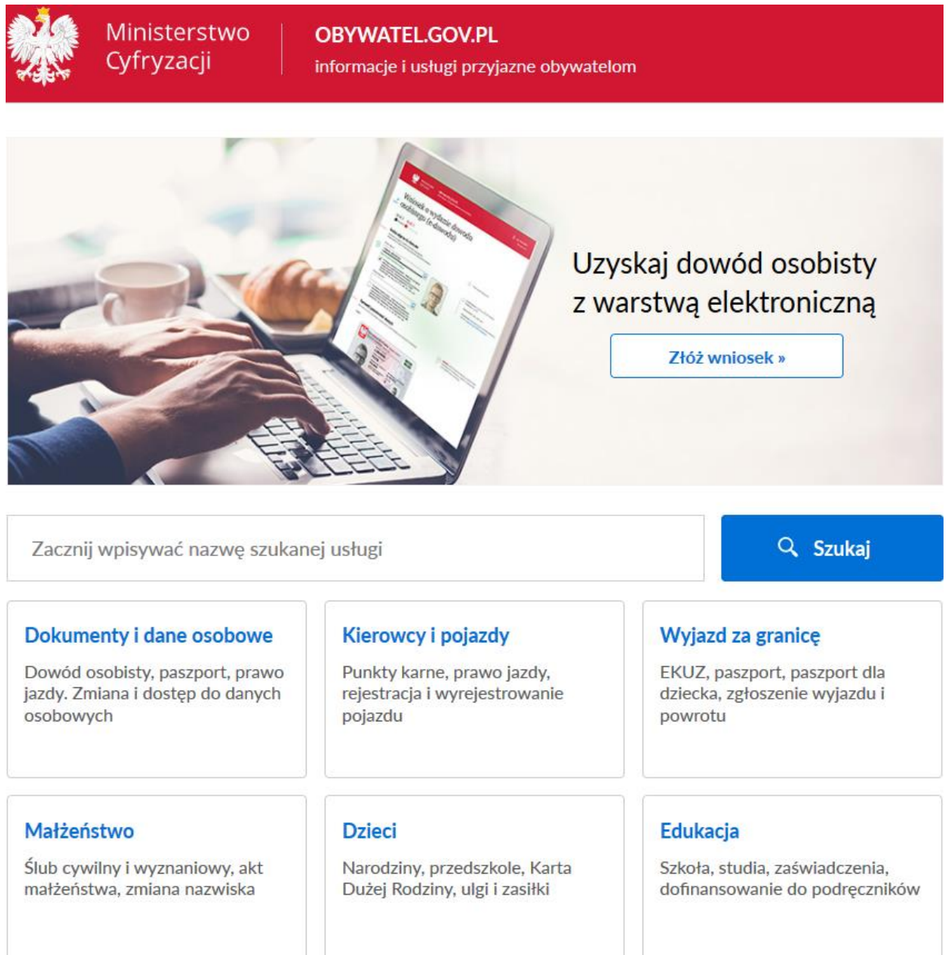
Wskazówki, profilaktyka

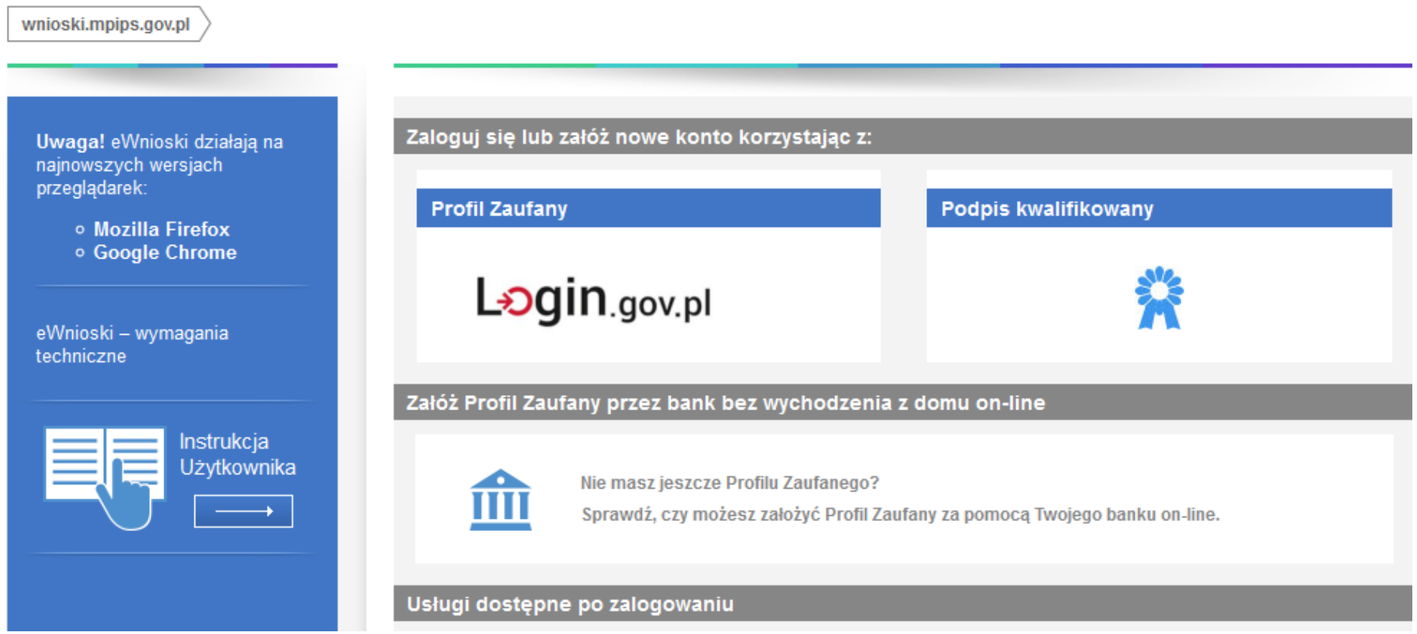
Bezpieczeństwo komunikacji

Sposób i środki komunikacji wpływają na bezpieczeństwo sieci i systemów organizacji oraz na bezpieczeństwo użytkowników korzystających z usług oferowanych przez organizację

- liczba informacji przesyłanych drogą elektroniczną będzie się zwiększała (e-Doręczenia; docelowo cała korespondencja w wersji elektronicznej)
- wzrasta podatność na atak z tego kierunku (phishing, kradzież tożsamości)
- słabo lub w ogóle niezabezpieczone kanały komunikacji, błędy ludzkie
- konieczność edukowania pracowników i obywateli (informacje na stronach, infografiki)
- załączniki i odnośniki w poczcie elektronicznej („trudna sprawa”)
- aplikacje do komunikacji i załatwiania spraw urzędowych (obywatel.gov.pl, podatki, emp@tia, ePUAP)
- korespondencja między urzędami też może się odbywać poprzez aplikacje (elektroniczne zarządzanie dokumentacją)

Bezpieczeństwo komunikacji





Bezpieczeństwo komunikacji wewnątrz organizacji

- poziom bezpieczeństwa odpowiedni do wyników analizy ryzyka (KRI, minimalne wymagania, bezpieczeństwo informacji)
- realizują zespoły bezpieczeństwa i administratorzy systemów
- podstawowe zagadnienia i zasady realizują także pracownicy
- w praktyce:
  - bezpieczeństwo komunikacji za pośrednictwem poczty elektronicznej i urządzeń mobilnych
  - bezpieczeństwo serwerów pocztowych, połączenia za pośrednictwem VPN, MFA
  - ochrona informacji niejawnych i prawnie chronionych
- rozmowy telefoniczne i SMSy (wygodne, ale nie gwarantują bezpieczeństwa informacji)
- komunikatory (własny serwer lub usługa komercyjna)

Bezpieczeństwo urządzeń – zasady dla wszystkich

Ochrona urządzeń powierzonych nam przez pracodawcę, albo prywatnych dopuszczonych do użycia w pracy, polega na stosowaniu się do wewnętrznych polityk bezpieczeństwa, wytycznych lub rekomendacji zespołów informatycznych i bezpieczeństwa

W każdym urzędzie taka polityka bezpieczeństwa powinna istnieć

Warto także stworzyć pracownikom uproszczoną wersję z wypisanymi najważniejszymi zasadami (np. infografika albo lista)

Pracodawca zabezpiecza urządzenia technicznie

Bezpieczeństwo urządzeń – podsumowanie

1. Twórz kopie zapasowe!
2. Używaj sprawdzonego oprogramowania antywirusowego
3. Aktualizuj na bieżąco swoje oprogramowanie
4. W sieci nie ufaj nikomu – dosłownie
5. Włącz opcję "Pokaż rozszerzenia nazw plików" w ustawieniach systemu Windows
6. Jeśli odkryjesz podejrzany lub nieznany proces na Twojej maszynie, odłącz ją natychmiast od internetu i innych połączeń sieciowych (takich jak domowe Wi-Fi)

Jeśli padłeś ofiarą ataku, zgłoś incydent do zespołu bezpieczeństwa w swojej firmie

Jeżeli zaatakowane zostało Twoje prywatne urządzenie, zgłoś incydent do CERT Polska wypełniając formularz na stronie https://incydent.cert.pl

Bezpieczeństwo urządzeń – materiały dodatkowe

https://nomoreransom.org

NO MORE RANSOM!

Polski

Crypto Sheriff | Ransomware: FAQ | Jak zapobiegać | Narzędzia deszyfrujące | Zgłoś przestępstwo | Partnerzy | O Projekcie

JAK ZAPOBIEGAĆ

Dodatkowe zalecenia w przypadku WannaCry

1. **Wyłącz smb v1**, aby zapobiec rozprzestrzenianiu się WannaCry w twojej sieci.
2. **Zainstaluj łaty bezpieczeństwa Microsoft**, co również zapobiegnie rozprzestrzenianiu się infekcji w obrębie sieci. Więcej informacji znajdziesz **tutaj**.

Jak zapobiegać atakom ransomware?

1. **Backup! Backup! Backup!** Jeśli będziesz stosował kopie zapasowe jako mechanizm odzyskiwania danych, ransomware nie będzie w stanie całkowicie zniszczyć Twoich danych. Najlepiej tworzyć dwie kopie: jedną umieszczoną w chmurze (najlepiej z wykorzystaniem usługi, która będzie wykonywać tę kopię automatycznie) i jedną przechowywaną fizycznie (np. na przenośnym dysku twardym, pendrive, dodatkowym laptopie itp.). Pamiętaj, aby po wykonaniu kopii zapasowej, odłączyć urządzenie od komputera. Kopie zapasowe są pomocne również, gdy przypadkiem usuniesz istotny plik lub przy niespodziewanej awarii dysku twardego.
2. **Używaj sprawdzonego oprogramowania antywirusowego**, aby chronić komputer przed infekcją złośliwym oprogramowaniem. Nie wyłączaj funkcji heurystycznych, mogących pomóc w wykryciu oprogramowania ransomware, którego nie ma jeszcze w bazie sygnatur.
3. **Aktualizuj na bieżąco swoje oprogramowanie**. Jeśli została wydana aktualizacja systemu operacyjnego (OS) lub aplikacji, zainstaluj ją. Jeśli oprogramowanie oferuje opcję automatycznych aktualizacji, warto mieć ją włączoną.
4. **Nie ufaj nikomu. Dosłownie.** Dowolne konto może zostać skompromitowane! Złośliwe linki mogą być wysyłane nawet z kont przyjaciół z portali społecznościowych, kolegów lub partnerów w **grach online**. Nigdy nie otwieraj załączników w mailach od nieznanej osoby. Przestępcy często rozsyłają fałszywe e-maile, które wyglądają jak powiadomienia ze sklepu online, banku, sądu, od policji czy komornika. Oszuści spróbują nakłonić Cię do kliknięcia w złośliwy link i tym samym zainfekowania systemu złośliwym oprogramowiem.
5. **Włącz opcję "Pokaż rozszerzenia nazw plików" w ustawieniach systemu Windows na Twoim komputerze**. Dzięki temu łatwiej zauważysz pliki, które mogą być potencjalnie złośliwe. Trzymaj się z dala od takich rozszerzeń jak '.exe', '.vbs' czy '.scr'. Scammerzy mogą używać wielu rozszerzeń, aby złośliwy plik wyglądał na film, zdjęcie lub dokument (np. hot-chics.avi.exe lub doc.scr).
6. Jeśli odkryjesz podejrzany lub nieznany proces na Twojej maszynie, **odłącz ją natychmiast od internetu i innych połączeń sieciowych (takich jak domowe Wi-Fi)** - zapobiegniesz w ten sposób dalszemu rozprzestrzenieniu się infekcji.

https://cert.pl/news

CERT.PL

Home > Aktualności > Bez kategorii > Przeciwdziałanie phishingowi wykorzystującemu technikę man-in-the-middle

Przeciwdziałanie phishingowi wykorzystującemu technikę man-in-the-middle

Data publikacji: 21/01/2019, Michał Leszczyński

Zespół CERT Polska zaobserwował interesującą technikę phishingową zastosowaną wobec użytkowników popularnego polskiego agregatora treści. W sieci zrobiło się również głośno za sprawą pojawienia się nowego narzędzia Modlishka służącego do automatyzacji tego typu ataków. Artykuł opisuje mechanizm ataku oraz przedstawia nasze rekomendacje dla twórców stron internetowych.

Mechanizm ataku

Zaobserwowany atak polega na skierowaniu użytkownika na fałszywą domenę, która często nazywa się bardzo podobnie do prawdziwej usługi. Odmiennie od obserwowanych wcześniej technik phishingowych, fałszywy serwer nie przesyła użytkownikowi podrobionej wersji strony, tylko pośredniczy w komunikacji z prawdziwą usługą.

Zwiększanie świadomości pracowników

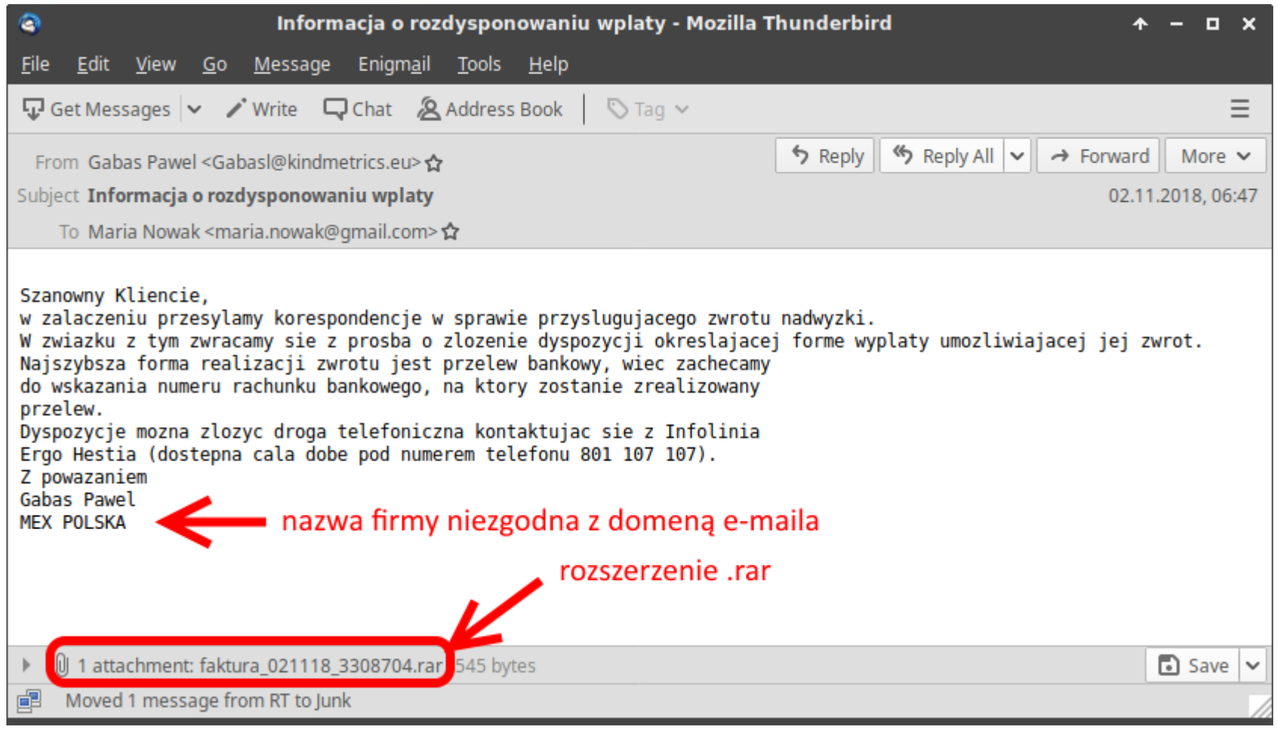
Zwiększanie świadomości

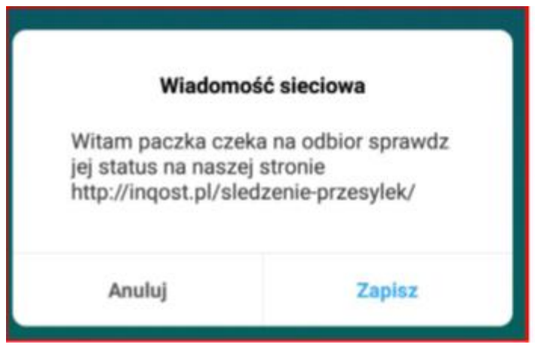
- Same zabezpieczenia techniczne do zapewnienia bezpieczeństwa nie są wystarczające
- Jesteśmy w stanie zabezpieczyć sieci i systemy w dobrym stopniu (biorąc pod uwagę analizę ryzyka i model zagrożeń)
- **Atakujący obierają za cel ataku użytkownika – pracownika**
- Zwiększanie świadomości użytkowników o zagrożeniach jest istotnym elementem zapewnienia bezpieczeństwa

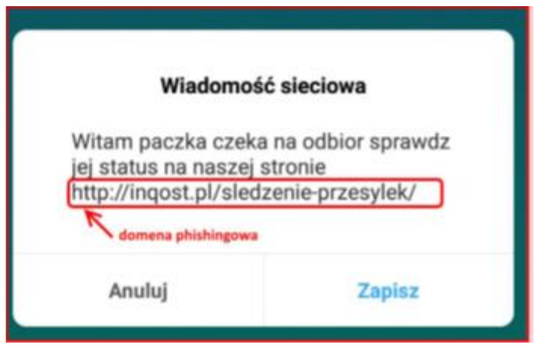
Zwiększanie świadomości – szkolenia

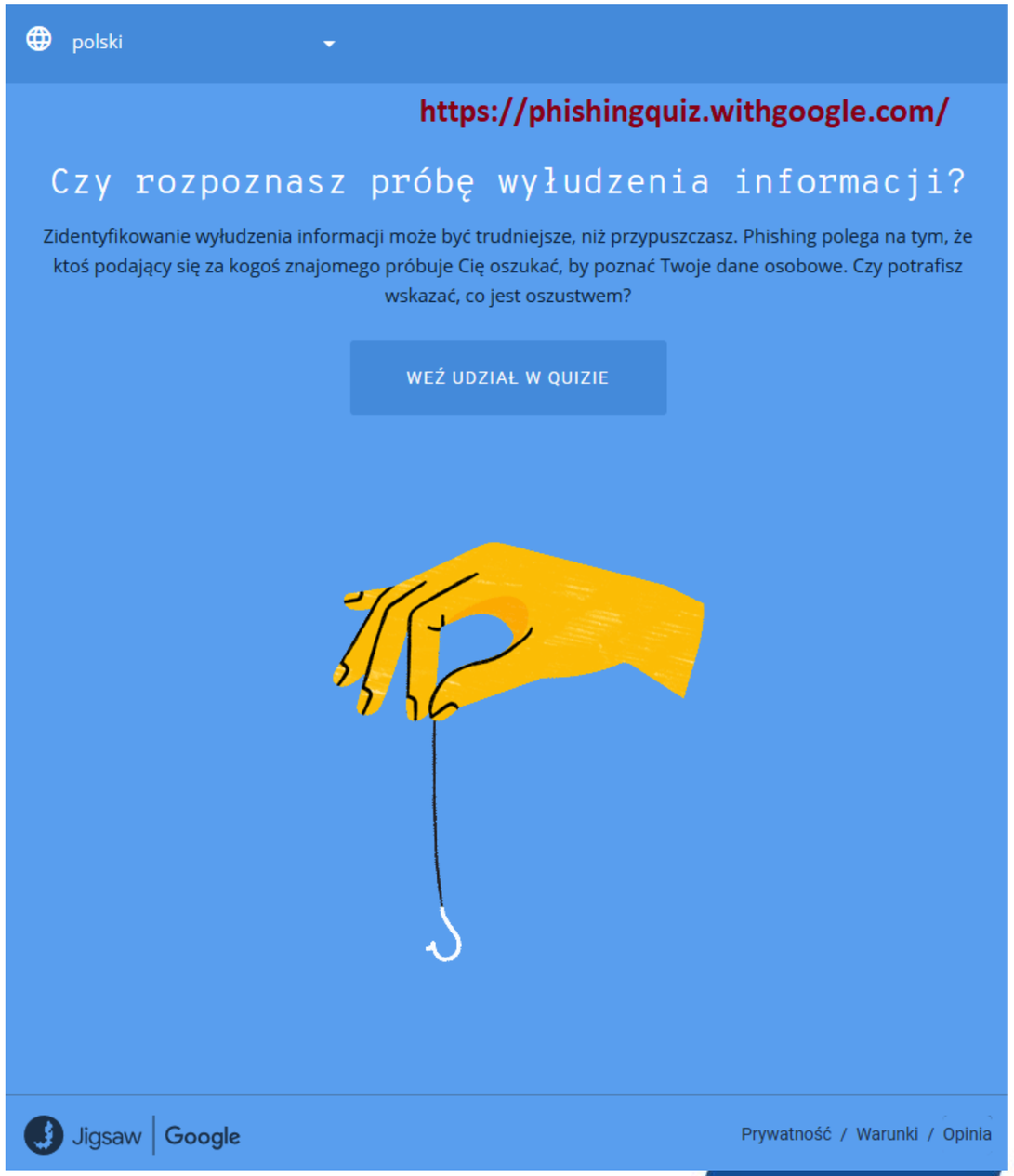
- Dla określonej grupy słuchaczy na wybrany temat
- Szkolenia wstępne – podstawowe zagadnienia, polityki i procedury firmowe, zgłaszanie incydentów
- Szkolenia przypominające – uzupełnienie i utrwalenie wiedzy, aktualne trendy
- Warsztaty – element dodatkowy szkoleń
- Szkolenia specjalistyczne – dla wybranych grup zawodowych
- Kursy online – intranet, internet, usługi komercyjne

Zwiększanie świadomości – szkolenia





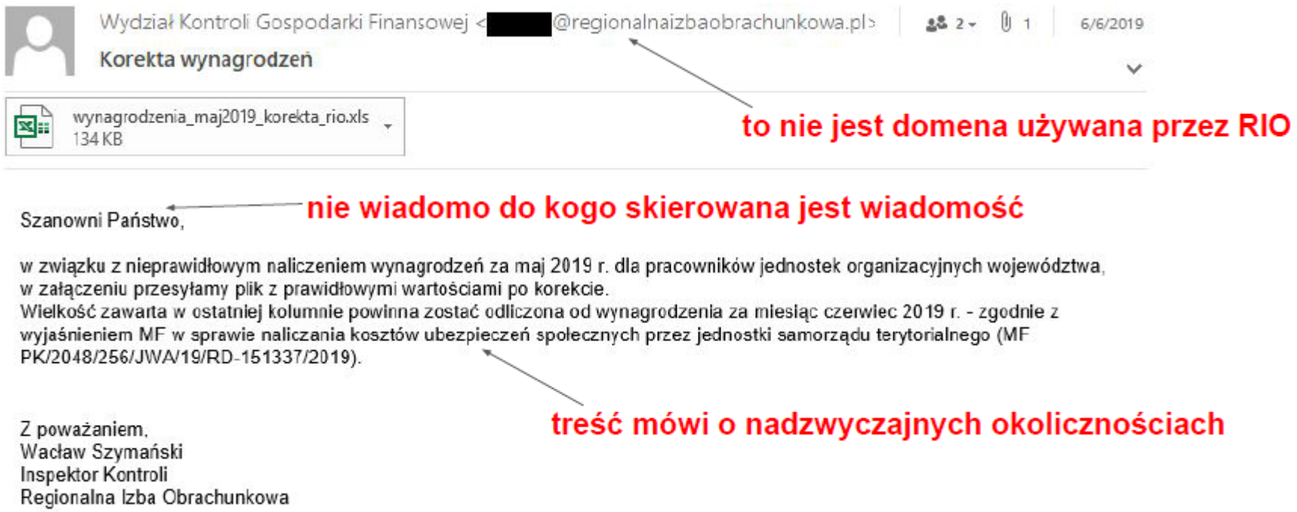




Zwiększanie świadomości – ćwiczenia

- Ćwiczenia dla pracowników – ukierunkowane na indywidualnego pracownika
- Sektorowe, w organizacji lub dla określonych komórek organizacyjnych
- W miejscu pracy, w czasie pracy
- Scenariusz realny i aktualny
- Przygotowanie i uodpornienie użytkownika na atak
- Sprawdzenie i utrwalenie umiejętności nabytych na szkoleniach

Zwiększanie świadomości – ćwiczenia


Wydział Kontroli Gospodarki Finansowej <[redacted]@regionalnaizbaobrachunkowa.pl> 2 1 6/6/2019

Korekta wynagrodzeń

wynagrodzenia_maj2019_korekta_rio.xls
134 KB

to nie jest domena używana przez RIO

Szanowni Państwo,

nie wiadomo do kogo skierowana jest wiadomość

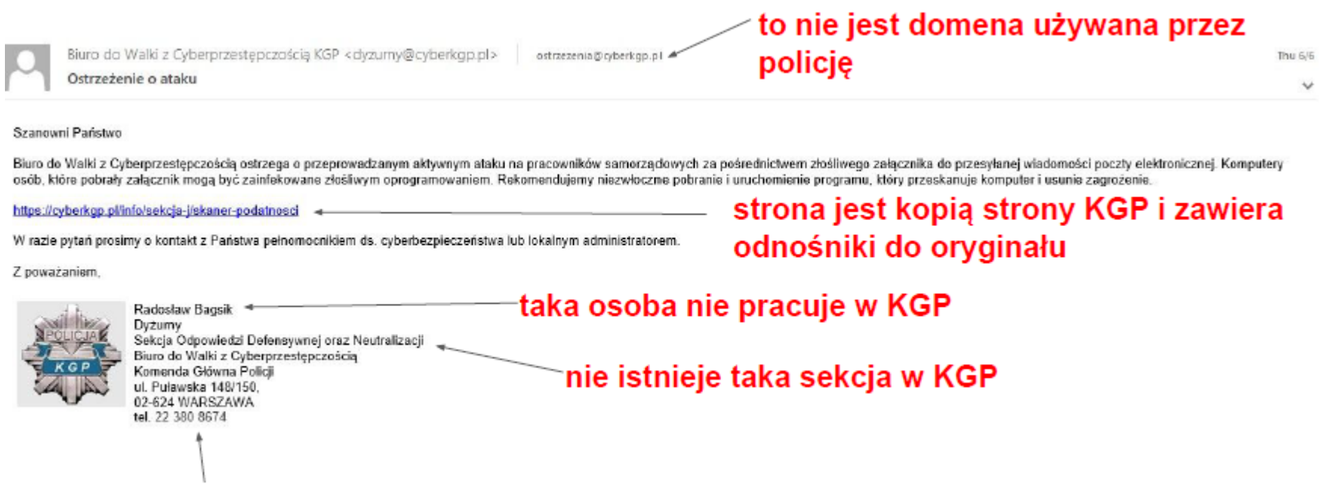
w związku z nieprawidłowym naliczeniem wynagrodzeń za maj 2019 r. dla pracowników jednostek organizacyjnych województwa, w załączeniu przesyłamy plik z prawidłowymi wartościami po korekcie.
Wielkość zawarta w ostatniej kolumnie powinna zostać odliczona od wynagrodzenia za miesiąc czerwiec 2019 r. - zgodnie z wyjaśnieniem MF w sprawie naliczania kosztów ubezpieczeń społecznych przez jednostki samorządu terytorialnego (MF PK/2048/256/JWA/19/RD-151337/2019).

treść mówi o nadzwyczajnych okolicznościach

Z poważaniem,
Wacław Szymański
Inspektor Kontroli
Regionalna Izba Obrachunkowa

sugestii w ankiecie, która zostanie przesłana Państwu odrębną korespondencją w czasie późniejszym.

Z poważaniem,
Karol Okoński
Sekretarz Stanu
w Ministerstwie Cyfryzacji


Biuro do Walki z Cyberprzestępczością KGP <dyzurny@cyberkgp.pl> ostrzezenia@cyberkgp.pl Thu 6/6

Ostrzeżenie o ataku

to nie jest domena używana przez policję

Szanowni Państwo

Biuro do Walki z Cyberprzestępczością ostrzega o przeprowadzanym aktywnym ataku na pracowników samorządowych za pośrednictwem złośliwego załącznika do przesyłanej wiadomości poczty elektronicznej. Komputery osób, które pobrały załącznik mogą być zainfekowane złośliwym oprogramowaniem. Rekomendujemy niezwłoczne pobranie i uruchomienie programu, który przeskanuje komputer i usunie zagrożenie.

https://cyberkgp.pl/info/sekcja-j/skaner-podatnosci

strona jest kopią strony KGP i zawiera odnośniki do oryginału

W razie pytań prosimy o kontakt z Państwa pełnomocnikiem ds. cyberbezpieczeństwa lub lokalnym administratorem.

Z poważaniem,

Radosław Bagsik
Dyżurny
Sekcja Odpowiedzi Defensywnej oraz Neutralizacji
Biuro do Walki z Cyberprzestępczością
Komenda Główna Policji
ul. Puławska 148/150,
02-624 WARSZAWA
tel. 22 380 8674

taka osoba nie pracuje w KGP

nie istnieje taka sekcja w KGP

to nie jest numer związany z KGP

Zwiększanie świadomości – wewnętrzne procedury zgłaszania incydentów

Utrwalanie w organizacji sposobu obsługi incydentów

- Pracownicy przekazują zgłoszenie do konkretnej osoby odpowiedzialnej za obsługę incydentów wewnątrz instytucji
- Zespoły IT / bezpieczeństwa przekazują zgłoszenie do CERT Polska lub innego właściwego dla siebie zespołu CSIRT oraz na policję jeżeli zgłoszone działanie jest przestępstwem
- Przypominamy pracownikom o nieprzekazywaniu informacji poza organizację na własną rękę (np. do prasy lub na portale społecznościowe) – informacje o ataku pojawiające się na zewnątrz organizacji ułatwiają atakującemu ocenę sytuacji i utrudniają obronę

Zwiększanie świadomości – wewnętrzne procedury zgłaszania incydentów

Dziwny atak – nie atak trafia na skrzynki polskich urzędów

[redacted] dodał [redacted] kategorii Złośniki z tagami: atak • Polska • skaner

Dzisiaj koło południa do skrzynek polskich urzędników trafiły dwa dziwne e-maile. Na pierwszy rzut oka wyglądały na bardzo sprytny atak, ale nie widać celu atakujących innego niż testowanie świadomości urzędników. Ktoś się zatem bawi – lub pracuje.

Otrzymaliśmy zgłoszenie od jednego z Czytelników, który otrzymał dwa e-maile, jednego po drugim. Czytelnik pracuje w administracji rządowej, a e-maile były faktycznie ciekawe. Przeanalizowaliśmy je – jeśli to atak, to chyba nieudany, choć bardzo ładny.

Dwa e-maile

Pierwsza wiadomość, która dotarła do Czytelnika, wyglądała następująco:

Ważne - ostrzeżenie o fałszywym portalu
Dyżurny PCC <dyzurny@plcyber.pl>
Odpowiedź na tę wiadomość wysłano w dniu 2018-11-27
Wysłano: Wt 2018-11-27
Do: rozdzielnik-ostrzezenia@plcyber.pl

Szanowni Państwo,

Zwiększanie świadomości – schemat przeprowadzania ćwiczenia

- Szkolenie z bezpieczeństwa sieci i systemów, w tym zgłaszania incydentów (najpóźniej na miesiąc przed symulacją)
- Uprzedzenie pracowników o ćwiczeniu (może być wykonane razem ze szkoleniem)
- Przeprowadzenie symulacji
- Zebranie statystyk
- Przygotowanie i przesłanie raportów z ćwiczeń
- Informacja zwrotna dla pracowników – indywidualna lub szkolenie z podsumowaniem ćwiczeń

Zwiększanie świadomości – schemat przeprowadzania ćwiczenia

CERT.PL

SZaZa 2019: Raport ogólny z ćwiczenia

Przebieg ćwiczenia

Etap 1: cybertest2019

Administratorzy IT z podmiotów ćwiczących dystrybuowali swoim użytkownikom wiadomość e-mail zachęcającą do wypełnienia testu rozpoznawania phishingów. Test składał się z 12 pytań, a każde z nich zawierało zrzut ekranu wiadomości e-mail, SMS lub strony internetowej. Zadaniem użytkownika było dokonanie klasyfikacji, czy treść prezentowana na zrzucie ekranu pochodzi od prawdziwej, czy fałszywej organizacji.

Etap 2: korekta płac

Organizatorzy ćwiczenia posługując się adresem e-mail według schematu `<miasto>@regionalnaizbaobrachunkowa.pl` rozdystrybuowali do użytkowników z podmiotów ćwiczących wiadomość e-mail.

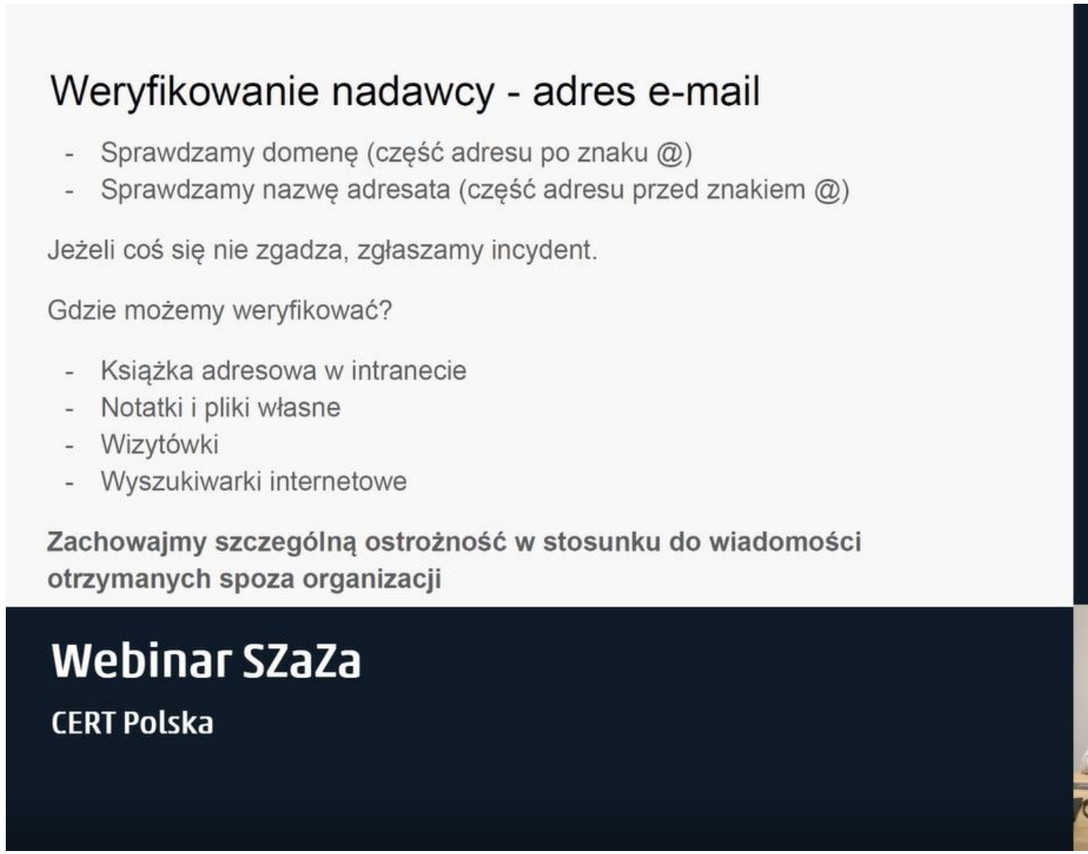

Wydział Kontroli Gospodarki Finansowej <[redacted]@regionalnaizbaobrachunkowa.pl>
[redacted]@regionalnaizbaobrachunkowa.pl
Wed 6/5
Korekta wynagrodzeń

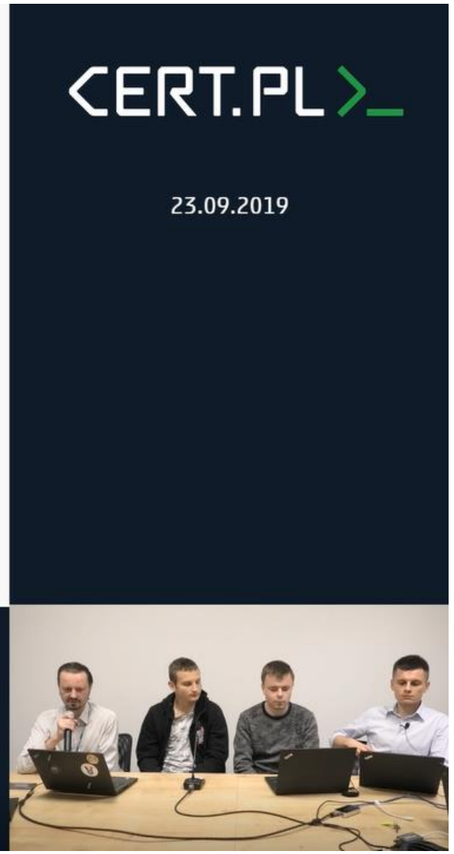
Szanowni Państwo,

w związku z nieprawidłowym naliczeniem wynagrodzeń za maj 2019 r. dla pracowników jednostek organizacyjnych województwa, w załączeniu przesyłamy plik z prawidłowymi wartościami po korekcie.
Wielkość zawarta w ostatniej kolumnie powinna zostać odliczona od wynagrodzenia za miesiąc czerwiec 2019 r. - zgodnie z wyjaśnieniem MF w sprawie naliczania kosztów ubezpieczeń społecznych przez jednostki samorządu terytorialnego (MF PK/20&8/256/JWA/19/RD-101337/2019).

Z poważaniem,
Wacław Szymański
Inspektor Kontroli
Regionalnej Izby Obrachunkowej

Do wiadomości załączony był arkusz kalkulacyjny programu Microsoft Office Excel (plik .xls) zawierający "złośliwe" makro. Uruchomienie makra powodowało wysłanie na serwer organizatorów ćwiczenia następujących informacji:





NASK

Dlaczego warto ćwiczyć?

Wystarczy jedna uruchomiona próbka na całą organizację, by zwiększyć uprawnienia atakującego w infiltrowanej sieci

Wystarczy jeden zgłoszony incydent, żeby uratować organizację

Wiedza i umiejętności pracowników zwiększają szansę na obronę