Bezpieczeństwo w telekomunikacji – wyzwania dla pracowników

dr inż. Adrian Marzecki
Orange Polska

VI Forum Współpracy Edukacji i Biznesu (Edumikser 2022)
Warszawa, 19.10.2022

Agenda

- Ekosystem cyberbezpieczeństwa
- Wyzwania/zagrożenia dla pracowników - przykłady co firmy mogą robić?
- Podsumowanie

„Spiesz się powoli.”

PARP Grupa PFR

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

PTI POLSKIE TOWARZYSTWO INFORMATYCZNE

PIIT

Ewolucja cyberbezpieczeńsywa i kompetencji w Orange

1997 Abuse Polpak

2005 Abuse TP SA

2006 CERT affiliation

2010 SOC established

2011 FIRST membership

2012 Attack on DGT modems, frauds of 1 mln PLN

2013 commercial services launch (DDoS Protection)

2014 Attack on 100k+ DSL modems users

2015 CyberShield launch Live threat statistics

2015 1st annual CERT OPL Report

2016 Security Excellence Award

2016 Trusted Introducer certification

2016 Malware protection service

2017 SOC for Orange in MEA region

2017 Certificates ISO 27001 ISO 27018

2018 ISO 22301 certification MANRS certification

2019 CyberShield mobile CyberShield for business

2020 CyberShield Awarded by Broadband World Forum

2022.05 8th edition of CERT Orange Polska Report

Fundusze Europejskie Wiedza Edukacja Rozwój

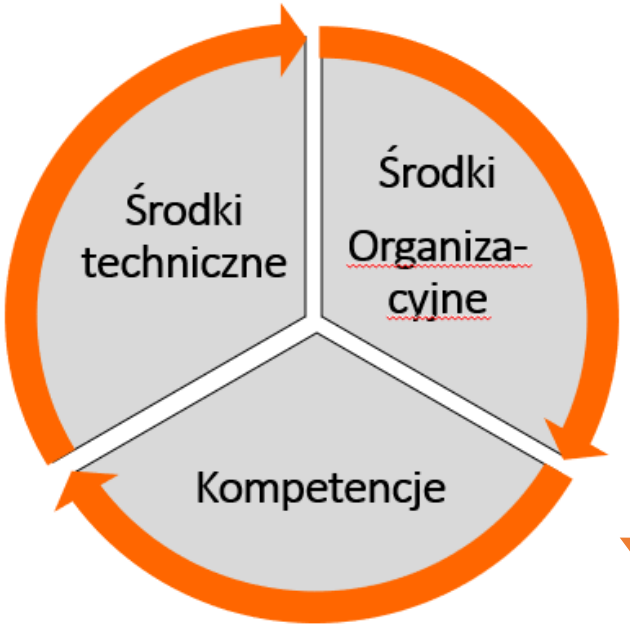
Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Społeczny

Uproszczony ekosystem cyberbezpieczeństwa

Analiza ryzyka → Zabezpieczenia → Wdrożenia → Incydent → Analiza poincydentalna

- Strategie zarządzania ryzykiem
  - Mitygacja ryzyka
  - Unikanie ryzyka
  - Transfer ryzyka
  - Akceptacja ryzyka



- Zabezpieczeń c.d.
  - Prewencja
  - Detekcja
  - Reakcja
  - Predykcja

Dostosowanie

Dodanie do analizy nowych zagrożeń

PARP Grupa PFR

Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

PTI Polskie Towarzystwo Informatyczne

PIIT

Cyber zagrożenia i wyzwania dla pracowników.

Jak firma może pomóc pracownikom poradzić sobie z tymi zagrożeniami?

„Co tak błyszczy?”

Fundusze Europejskie Wiedza Edukacja Rozwój

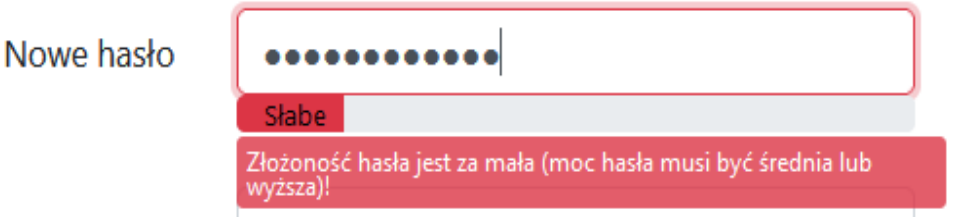
Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Społeczny

Ciągle przypominać jak tworzyć bezpieczne hasła

- częsta zmiana hasła? Nie! Hasło ma być silne i poufne.
- hasła do systemów firmowych nie mogą być powielane nigdzie indziej
- hasła do systemów firmowych nie mogą być zapamiętywane w przeglądarkach
- systemy powinny pozwalać na wykorzystywanie dłuższych fraz/wierszy w haśle
- hasło powinien znać tylko użytkownik końcowy
- hasło powinno różnić się od 20 ostatnich haseł
- hasło powinno być mocy średniej lub wyższej
- hasło powinno mieć co najmniej 12 znaków, uprzywilejowane min.15
- hasło powinno składać się z co najmniej 5 różnych znaków
- hasło nie może zawierać identyfikatora konta/użytkownika
- hasło powinno obejmować możliwie największy zestaw znaków z grup: małe litery, wielkie litery, cyfry i znaki specjalne

Prewencja: Systemy nie dopuszczają do ustawienia słabego hasła oraz hasła z internetowych baz słownikowych.



Prewencja: Stosowanie menedżera haseł np. Keepass do tworzenia i przechowywania bezpiecznych haseł

Detekcja/Reakcja: Wykrywanie hasła wpisanego w pole login i wymuszenie zmiany hasła przez SOC

Cyber odporność na Vishing

Vishing to atak phishingowy wykorzystujący kontakt telefoniczny i metody socjotechniczne w rozmowie. Atakujący często podaje się za pracownika zespołu wsparcia informatycznego IT i przekonuje użytkownika do instalacji aplikacji zdalnego pulpitu np. AnyDesk lub TeamViewer i przekazaniu później możliwości zdalnego zarządzania komputerem.

Przykłady ataków z wykorzystaniem aplikacji zdalnego pulpitu:

- https://cert.orange.pl/aktualnosci/rozmowa-z-bankowym-oszustem
- https://niebezpiecznik.pl/post/uber-zhackowany/

Reakcja: Podejrzane telefony są zgłaszane do *SOC OPL wraz z informacjami o połączeniu

Prewencja: 1) blokada aplikacji zdalnego pulpitu na proxy i uruchomienie własnego rozwiązania
2) Identyfikacja pracownika IT lub innej osoby podającej się za pracownika przez „OrangeID”

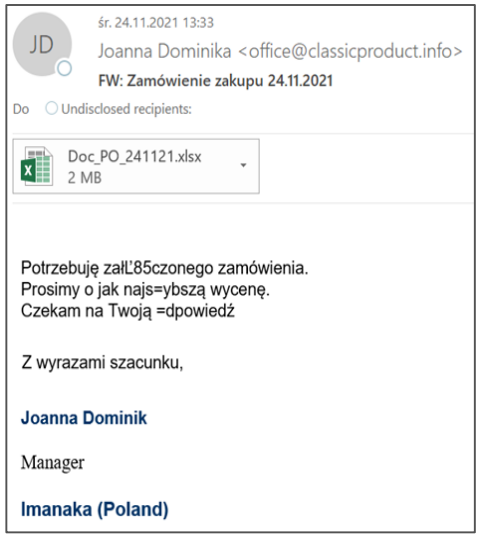
3) Już … niedługo wdrożenie blokowania CLI Spoofingu przez wszystkich operatorów w kraju

„Głęboki oddech” przed otwarciem załączników z poczty

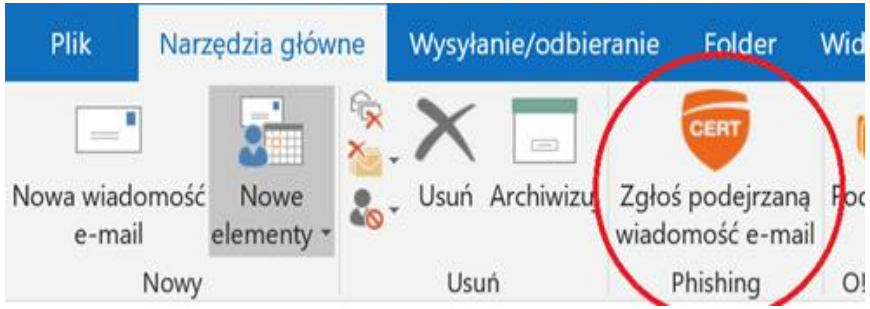
Najczęstszym źródłem infekcji komputerów przez szkodliwe oprogramowanie (malware), jest otwieranie podejrzanych załączników otrzymanych w poczcie oraz korzystanie z zewnętrznych zasobów plikowych.
Po otwarciu załącznika, zazwyczaj pyta on użytkownika o zgodę na uruchomienie makra, a potem zaczyna zachowywać się jak program typu „downloader” i pobiera z Internetu resztę szkodliwego kodu.

Prewencja: 1) kampanie kontrolowanego rozsyłania phishingu
2) blokada IoC na Cybertarczy
3) implementacja Zero Tust – dostęp tylko VPN z min. uprawnień

Reakcja: 1) ikonka w systemie pocztowym do zgłaszania podejrzanych emaili do CERT OPL 2) obniżanie uprawnień pracowników przez SOC OPL



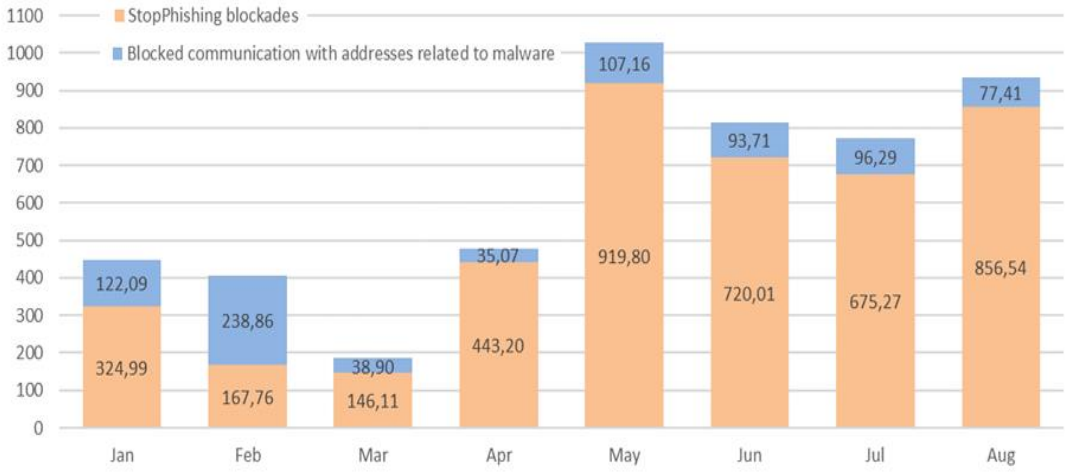
Przykład kampanii Formbook wykorzystującej exploit na Microsoft Excel, CVE-2017-11882.
Formbook to złośliwe oprogramowanie wykradające dane.



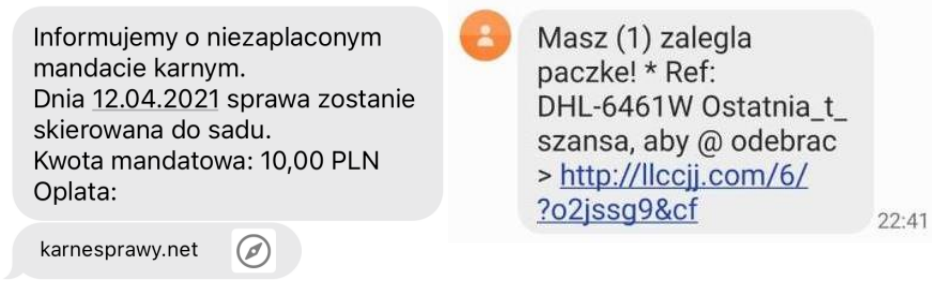
„Siła spokoju” przy czytaniu phishingowej komunikacji

Phishing, czyli podszywanie się w komunikacji pod inna osobę lub instytucję. Wykorzystując w korespondencji (email, SMS, media społecznościowe, etc.) techniki socjotechniczne, atakujący próbuje nakłonić odbiorcę do wykonania jakiejś czynności np. otworzenia linku i wykonania podanej instrukcji. Dużo przykładów kampanii phishingowych opisuje CERT OPL:
https://cert.orange.pl/ostrzezenia/uwazajcie-na-kwarantanne
https://cert.orange.pl/aktualnosci/phishing-inny-niz-wszystkie

Blokady na Cybertarczy w tyś. unikatowych użytkowników



Prewencja: 1) Cybertarcza blokuje domeny phishingowe
2) kampanie kontrolowanego phishingu
3) podnoszenie świadomości cyberzagrożeń i nauka nawyków np. samodzielnego wpisywania do logowania adresu internetowego lub wykorzystania własnych linków zapisanych w zakładkach przeglądarki



Rozwaga przy instalacji aplikacji oraz pobieraniu plików

Instalacja aplikacji z innych źródeł niż producenci może zakończyć się pobraniem aplikacji zainfekowanej złośliwym oprogramowaniem.
Większość hostowni aplikacji wykorzystuje własne aplikacje wspomagające instalację hostowanych programów, które przy instalacji poszukiwanej aplikacji, instalują dodatkowo inne aplikacje, które mogą stanowić zagrożenie.
Darmowe aplikacje – zarówno te na komputery jak i na smartfony mogą zawierać ukryte funkcjonalności np. „residential proxy", które po instalacji będą pozwalały innym użytkownikom na zdalne wykorzystywanie tych urządzeń.
Pobieranie z Internetu nielegalnie udostępnionych plików multimedialnych oraz korzystanie z nielegalnych streamingów często wiąże się z infekcją urządzenia

Prewencja: 1) wszystkie aplikacje dopuszczone do użytkowania w firmie znajdują się na Liście Aplikacji Dopuszczonych do instalacji na Stacjach Roboczych OPL tzw. LAD
2) instalowanie i uruchamianie niebezpiecznych aplikacji jest blokowane przez Firewall na stacjach roboczych

Detekcja: monitorowanie ruchu sieciowego ze stacji roboczych do Internetu: 1) wykrywanie komunikacji do C&C
2) wykrywanie urządzeń „residential proxy" w sieci

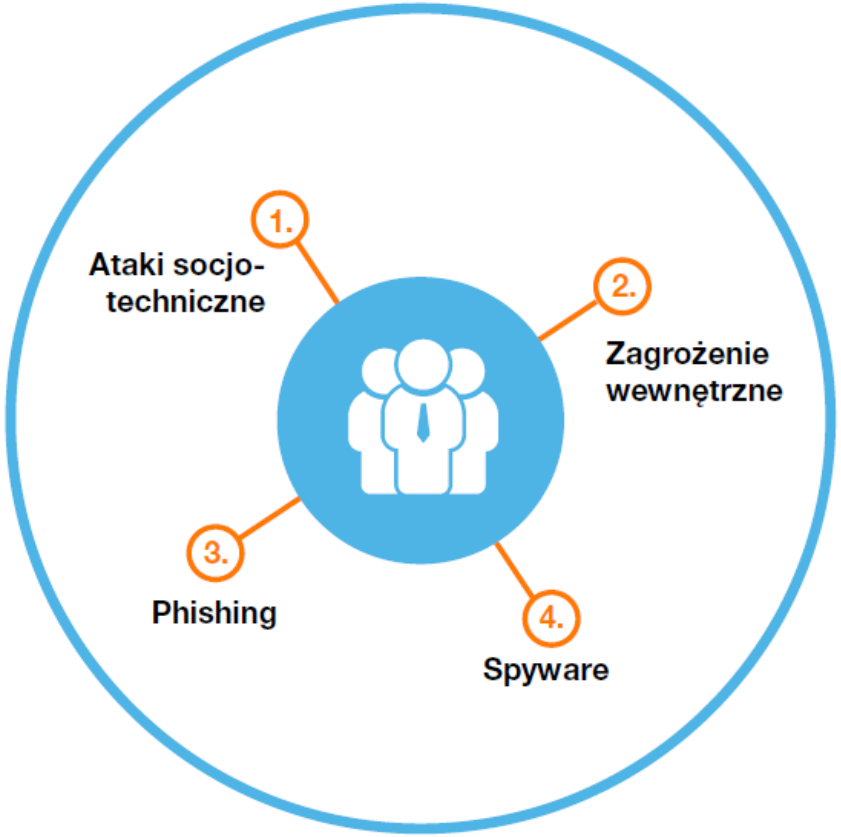
PODSUMOWANIE: Cyber zagrożenia dla pracowników

1.

- vishing
- znaleziony USB
- dla najlepszych smartphone lub tablet w prezencie
- „zmęczyć ofiarę” – przypadek Uber

3.

- phishing
- smishing



2.

- słabe hasła
- nawyki np. usypianie notebooka w podróży
- kradzież danych np. technikami steganograficznymi
- przekazanie „kredek” - przypadek Lapsus

4.

- otwieranie podejrzanych załączników z korespondencji
- instalacja „darmowych” aplikacji np. z ukrytym „residential proxy”
- urządzenia w „prezencie” do testów

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Społeczny

PODSUMOWANIE: ciągłe podnoszenie kompetencji

1. CERTYFIKACJE I SZKOLENIA

- utrzymanie certyfikatów potrzebnych do funkcjonowania certyfikacji firmy oraz partnerstwa z dostawcami rozwiązań i urządzeń
- szkolenia/warsztaty/laboratoria cyberbezpieczeństwa/ PoC z nowych, złożonych technologii

2. DOKTORATY WDROŻENIOWE

- jeden dr inż. z pierwszej edycji programu oraz dwóch doktorantów w trakcie realizacji doktoratu wdrożeniowego

3. STUDIA MIĘDZYNARODOWE

- trzech studentów na podyplomowych studiach online „Cyberbezpieczeństwo” w Dublinie w Irlandii

4. PROJEKTY MIĘDZYNARODOWE

- udział ekspertów w projektach finansowanych z UE np. SIMARGL „Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware”

SIMARGL

PODSUMOWANIE: Konieczna zmiana nawyków i budowanie nowych

Nie ma osób perfekcyjnych, grających bezbłędnie. Trzeba cały czas ćwiczyć.

Paweł Zagumny

Motywacja jest tym, co pozwala Ci zacząć. Nawyk jest tym, co pozwala Ci wytrwać.

Jim Ryun

Zaczynajmy budowanie świadomości cyberbezpieczeństwa od „dlaczego?”

https://thetrainingthinking.com/en/the-golden-circle-by-simon-sinek/

PARP
Grupa PFR

POLSKIE TOWARZYSTWO INFORMATYCZNE

PIIT

Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

Zapraszam do kontaktu:

e-mail: adrian.marzecki@orange.com

Cyberbezpieczeństwo Orange Polska

www.radasektorowa.pl

Fundusze Europejskie Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Społeczny