IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

PARP Grupa PFR

Ministerstwo Rozwoju i Technologii

Podstawowe aspekty cyberbezpieczeństwa MŚP

Zuzanna Polak, 21.11.2024 r.

#IdeaRozwojuBiznesu

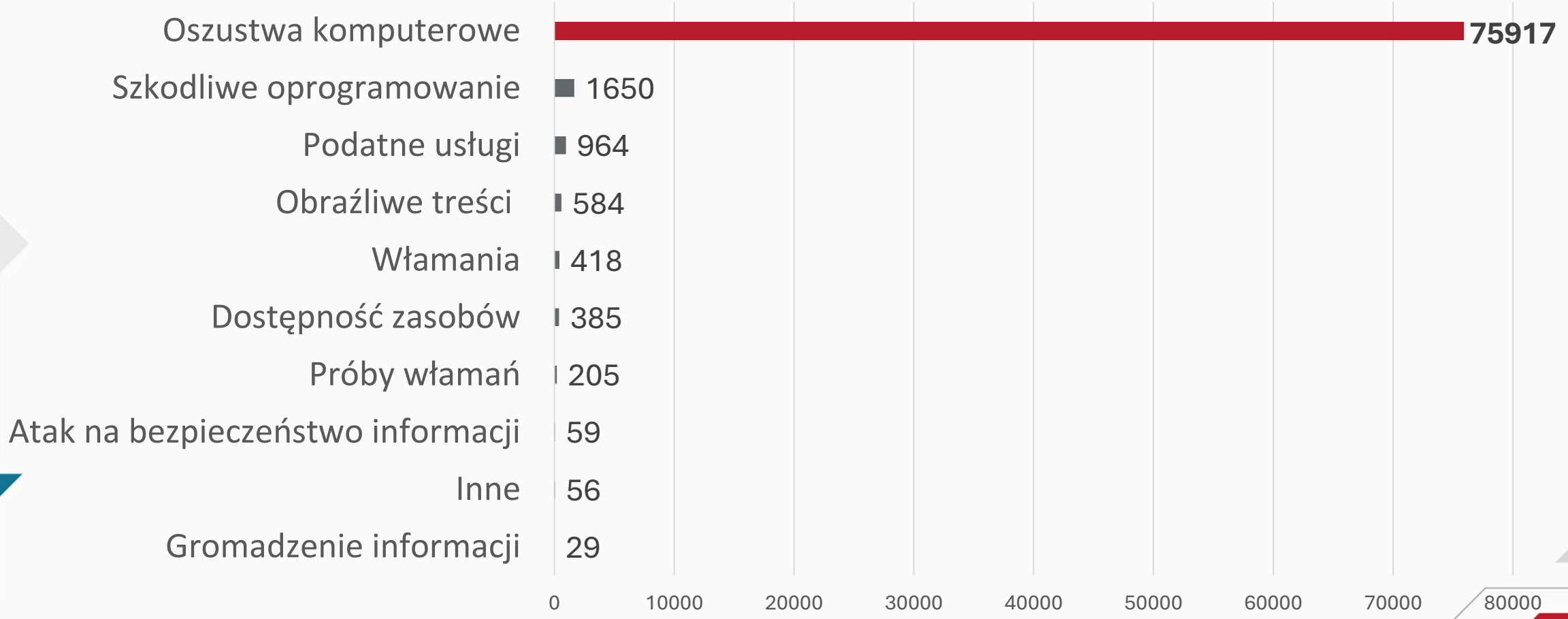
Agenda prezentacji

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

- Dane – dlaczego warto zainteresować się cyberbezpieczeństwem?
- Informacja w rękach cyberprzestępców
- Przegląd najważniejszych zagrożeń
- Cyberhigiena
- Zgłaszanie incydentów

CERT Polska: Rodzaje zarejestrowanych incydentów w 2023

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE



Najważniejsze wnioski

- DDoS oraz ransomware jako najczęstsze zagrożenia
- Phishing to nadal główny wektor początkowy
- Wzrost liczby oszustw typu BEC
- Próby wykorzystania AI

ENISA Threat Landscape 2024 https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

Top 5 obszarów wymagających pilnych inwestycji wg ekspertów

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

33% Narzędzia do wykrywania, analizy i reagowania (EDR/XDR)

34% Tworzenie kopii bezpieczeństwa

36% Ochrona sieci (firewalle, UTM)

37% Monitorowanie i reagowanie (SIEM, SOAR)

48% Szkolenia

Cyberportret polskiego biznesu. 2024. Raport Bezpieczeństwo cyfrowe oczami ekspertów i pracowników ESET i DAGMA Bezpieczeństwo IT

#IdeaRozwojuBiznesu

Jak działają cyberprzestępcy?

Jak działają cyberprzestępcy?

Jakie informacje są intersujące?

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

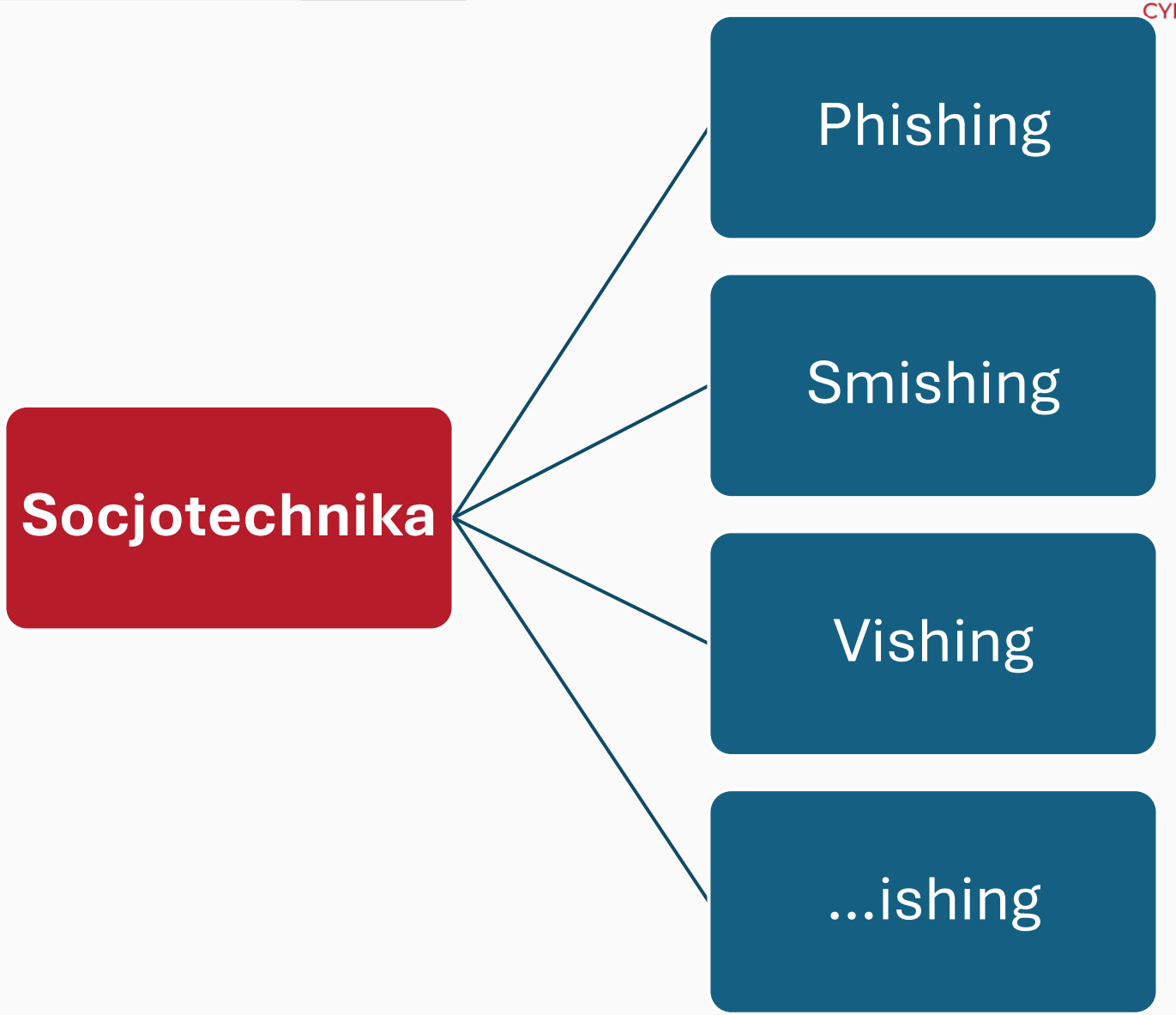
- Informacje finansowe
- Strona internetowa
- Technologie
- Klienci
- Zarząd i pracownicy

IDEA ROZWOJU
TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Jak cyberprzestępcy wykorzystują znalezione informacje?

#IdeaRozwojuBiznesu

Najłatwiej dostępna metoda



IDEA ROZWOJU
TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Otrzymałeś powiadomienie od Krajowej Administracji Skarbowej - Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages | Write | Tag

Krajowa Administracja Skarbowa
???rajowaAdministracja???karbowa@[redacted].com.br

Reply | Reply All | Forward | Archive | Junk | Delete | More

To [redacted] 09:58

Otrzymałeś powiadomienie od Krajowej Administracji Skarbowej

Informujemy, że dostępna jest nowa **notyfikacja** o następujących danych:

- [redacted] z numerem PESEL: ***295*** jako Właściciel
- Organ wydający: Krajowa Administracja Skarbowa, z numerem NIP: PL0028512
- Identyfikator: 87655235
- Termin upływa dnia: 02/10/2024
- Koncepcja: Powiadomienie o rozbieżnościach w samoopodatkowaniu od majątku (formularz PIT-17)

Jak uzyskać dostęp:

Tę notyfikację można pobrać w Elektronicznej Skrzynce Podawczej Krajowej Administracji Skarbowej (ESP) za pośrednictwem platformy ePUAP

Dla Twojej wygody, udostępniamy bezpośredni link do notyfikacji: Notyfikacje Oczekujace 87655235

Proszę pamiętać, że:

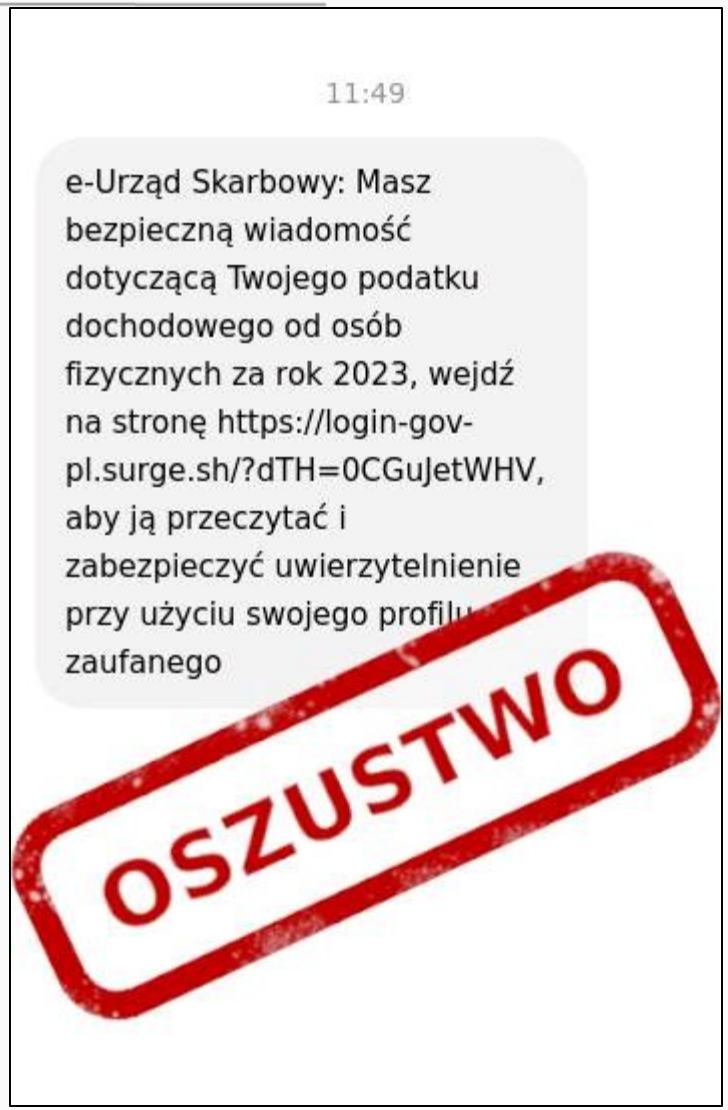
Zgodnie z przepisami art. 41 i 43 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, przyjęcie notyfikacji, wyraźne odrzucenie notyfikacji lub domniemanie odrzucenia z powodu nieuzyskania dostępu do notyfikacji w okresie jej udostępnienia, uznawane jest za skuteczne dostarczenie i procedura będzie kont

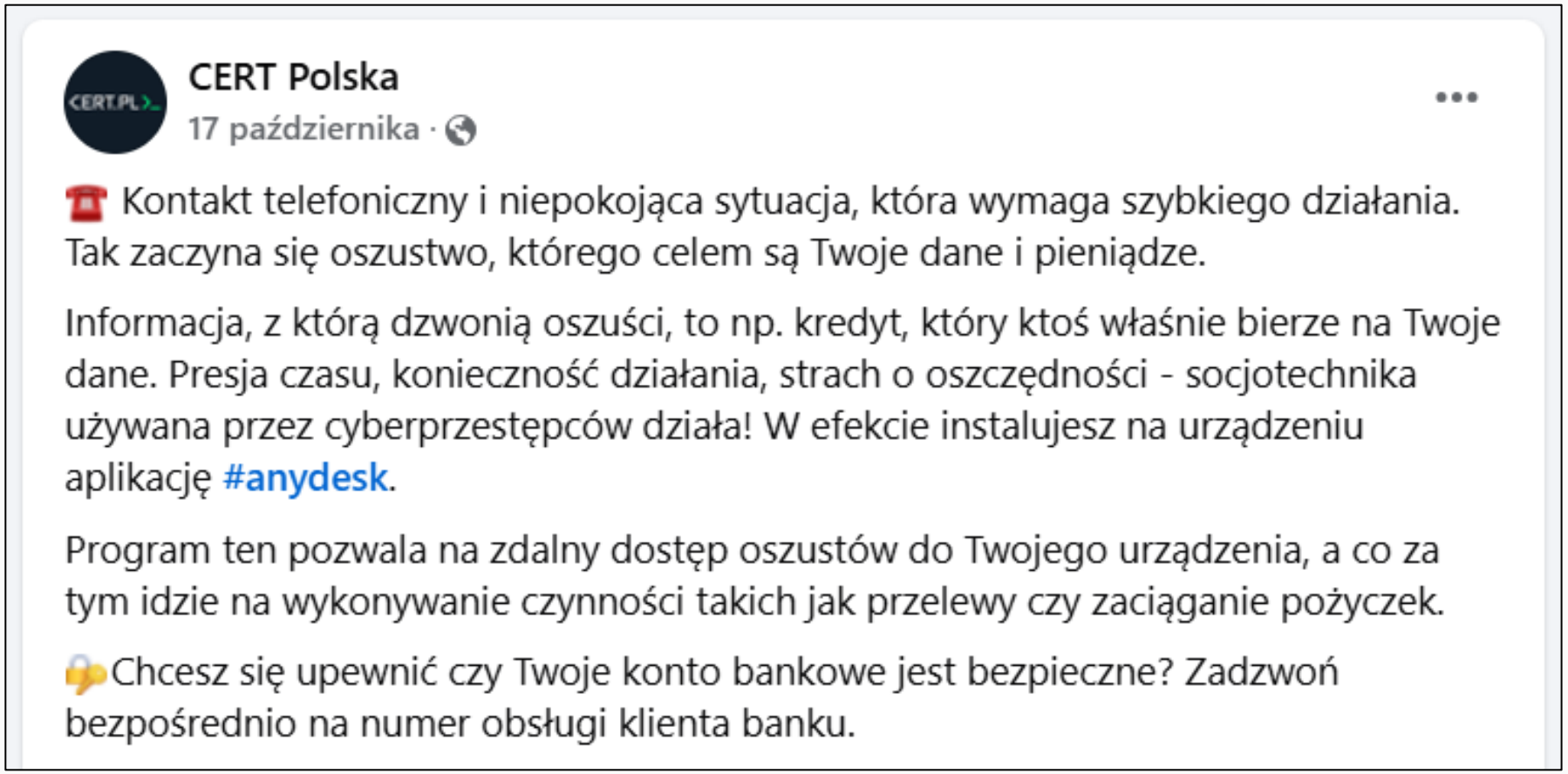
Można otrzymać tę notyfikację różnymi kanałami elektronicznymi lub nawet w formie papierowej drogą pocztową. Jeżeli dostęp do treś anie uzyskan ej niż jedną drogą, proszę pamiętać, że skutki prawne, o ile takie wystąpią, zawsze będą liczone od momentu pierwszego uzyskania dost

To jest uprzejme powiadomienie wysłane z Elektronicznej Skrzynki Podawczej Krajowej Administrac każdej chwili można uzyskać dostęp, popra ub usunąć adresy email za pomocą odpowiedniego formularza.

Rząd Polski

OSZUSTWO


11:49
e-Urząd Skarbowy: Masz bezpieczną wiadomość dotyczącą Twojego podatku dochodowego od osób fizycznych za rok 2023, wejdź na stronę https://login-gov-pl.surge.sh/?dTH=0CGuJetWHV, aby ją przeczytać i zabezpieczyć uwierzytelnienie przy użyciu swojego profilu zaufanego
OSZUSTWO



CERT Polska
17 października ·

☎ Kontakt telefoniczny i niepokojąca sytuacja, która wymaga szybkiego działania. Tak zaczyna się oszustwo, którego celem są Twoje dane i pieniądze.

Informacja, z którą dzwonią oszuści, to np. kredyt, który ktoś właśnie bierze na Twoje dane. Presja czasu, konieczność działania, strach o oszczędności - socjotechnika używana przez cyberprzestępców działa! W efekcie instalujesz na urządzeniu aplikację #anydesk.

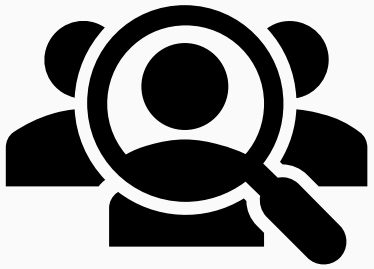
Program ten pozwala na zdalny dostęp oszustów do Twojego urządzenia, a co za tym idzie na wykonywanie czynności takich jak przelewy czy zaciąganie pożyczek.

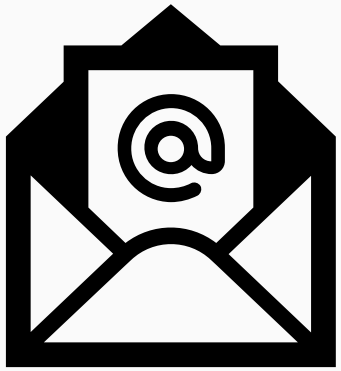
🔐Chcesz się upewnić czy Twoje konto bankowe jest bezpieczne? Zadzwoń bezpośrednio na numer obsługi klienta banku.

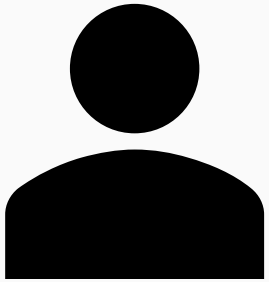
Jak działa socjotechnika?

Bussiness Email Compromise

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE







BEC - skutki

- Przelew na konto cyberprzestępcy
- Ujawnienie poufnych danych
- Zainfekowanie urządzenia, zaszyfrowanie lub kradzież danych

Phishing – jak się chronić?

- Weryfikacja nadawcy!
- Uważność na szczegóły (logo, stopki, formatu i kolorystyka maili)
- Nie klikanie w hiperłącza/linki
- Nie podawanie poufnych danych w mailu
- Tajne hasło rozpoznawcze
- Ustalenie bezpiecznego kanału komunikacji
- **Ostrożność wobec załączników**

Podejrzane załączniki

- przypominają dokumenty PDF, Microsoft Word lub Excel
- PODEJRZENIA powinny wzbudzać jednak ich rozszerzenia, takie jak **.exe, js,.iso, .img, .htm, .html,.dll,** lub pliki archiwów typu**: .rar, .gz, .tar i .zip**
- w tym archiwa dzielone na części np. **.r00, .r01**
- oraz pliki skryptów o rozszerzeniach **.vbs, .wsf, .js,**

Wirtualna Polska Media

Cześć ,

Jesteśmy prawnymi przedstawicielami Wirtualna Polska Media. Zauważyliśmy, że ta treść została użyta lub rozpowszechniona bezprawnie na Państwa stronie internetowej bez naszej zgody. Narusza to przepisy dotyczące ochrony praw autorskich zgodnie z obowiązującym prawem własności intelektualnej.

Szczegóły dotyczące naruszenia:

Akta dowodowe naruszenia praw autorskich.pdf

- Nazwa strony:
- ID Facebook:
- Właściciel: Wirtualna Polska Media
- Data naruszenia: 5 października 2024 roku

Proszę niezwłocznie usunąć naruszenie treści i potwierdzić to w ciągu 48 godzin od otrzymania tego powiadomienia. W przeciwnym razie podejmiemy odpowiednie kroki prawne w celu ochrony naszych praw.

Żądanie natychmiastowego działania:

1. Jesteś odpowiedzialny za zapewnienie, że wszystkie treści na Twojej stronie internetowej są zgodne z obowiązującym prawem autorskim.
2. Niezastosowanie się do naszych żądań może prowadzić do działań prawnych, w tym żądania odszkodowania.
3. Zastrzegamy sobie prawo do żądania odszkodowania za wszelkie szkody spowodowane naruszeniem praw autorskich.
4. Jeśli uważasz, że treść została usunięta przez stronę trzecią, prosimy o dostarczenie dowodów w celu naszego rozpatrzenia.

Doceniamy współpracę z Państwem w zakresie ochrony praw własności intelektualnej. W przypadku jakichkolwiek pytań prosimy o kontakt z nami za pośrednictwem poniższego adresu e-mail lub strony internetowej.

Z poważaniem, Wirtualna Polska Media

+48 22 57 67 900 | wp@grupawp.pl | ul. Żwirki i Wigury 16, 02-092 Warszawa

Ransomware

#IdeaRozwojuBiznesu

Ransomware – jak postępować w przypadku incydentu?

- Izolacja maszyn(y) od sieci
- Identyfikacja oraz eliminacja źródła infekcji (Phishing? Nośnik? Podatność? Usługa dostępna z Internetu?)
- Identyfikacja rodziny ransomware – http://nomoreransom.org
- Przywrócenie działania systemów – z czystej kopii, na czystej maszynie
- Zgłoszenie incydentu do CSIRT NASK (https://incydent.cert.pl/)

Więcej: https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

Dlaczego nie warto płacić okupu?

- Potencjalnie nielegalne (uczestnictwo z zorganizowanej grupie przestępczej; pranie pieniędzy; wspieranie terrorystów)
- Brak gwarancji
- Współudział w działaniach przestępczych – zachęta do dalszych ataków
- Zwiększenie ryzyka powtórnego ataku

Cyberhigiena od ręki

- Bezwzględne oddzielenie **spraw <u>służbowych i prywatnych</u>**:
- **Jeden użytkownik/domownik = jedno konto na urządzeniu.**
- **Aktualizacje!** systemu operacyjnego na urządzeniu oraz posiadanych aplikacji.
- Instalacja sprawdzonego oprogramowania **z zaufanych źródeł**.

Cyberhigiena cd.

- **Szyfrowanie** urządzeń – wszystkich.
- **Szyfrowanie** komunikacji oraz przegląd korespondencji.
- Niekorzystanie z **niezaufanych nośników.**
- Korzystanie z **filtrów ekranowych.**
- Niezostawianie **sprzętu bez nadzoru!**

Pracownicy…

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Podejmują ryzykowne działania na sprzęcie służbowym

65%

Ignorują powiadomienia o potrzebie aktualizacji oprogramowania

24%

Posiadają jedno/podobne hasło do większości swoich służbowych kont

29%

Zapisują hasła do swoich kont z miejsc, z których łatwo jej wykraść

20%

Cyberportret polskiego biznesu. 2024. Raport Bezpieczeństwo cyfrowe oczami ekspertów i pracowników ESET i DAGMA Bezpieczeństwo IT

Zacznij od hasła…

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

1. Długie (co najmniej 14 znaków).
2. Unikatowe (do każdego konta inne).
3. Łatwe do zapamiętania, ale trudne do odgadnięcia!!!
4. Zmiana tylko w wyjątkowych przypadkach.
5. Menedżer haseł

Silne hasło?

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

Zasada pełnego zdania (ale nie cytatu/powiedzenia)

- Wlazł**Kostek**Na**Mostek**I**Stuka**
- zielony**ParkingDla**3malych**Samolotow**
- DwaBialeLatajace**Sophisticated**Kroliki

Więcej o bezpiecznych hasłach: https://cert.pl/hasla/

Dwuskładnikowe uwierzytelnienie

- Kod generowany przez aplikację
- Fizyczny klucz zabezpieczeń
- Wiadomość z kodem
- Lista kodów

Gdzie zgłaszać?

- **Wewnętrzne komórki** bezpieczeństwa IT
- **Jako osoby prywatne:** https://incydent.cert.pl/
- **mObywatel**
- **Fałszywe SMSy:** 8080
- **Oszustwa, wyłudzenia:** bank, policja, CERT Polska

Dlaczego warto zgłaszać incydenty do CERT Polska

Dbasz o bezpieczeństwo innych

Umieszczenie strony na naszej liście ostrzeżeń ochroni przed niebezpieczeństwem osoby, którym nie udało się rozpoznać zagrożenia.

Pomagasz nam tworzyć obraz zagrożeń w internecie

Mając informacje o zagrożeniu, pochodzące od kilku osób, możemy lepiej zrozumieć incydent i cel działania cyberprzestępców.

Pozwalasz nam lepiej poznać niebezpieczeństwo

Większość projektów w których bierzemy udział jest bezpośrednią odpowiedzią na realne zagrożenia. Im lepszy mamy obraz, tym skuteczniej możemy działać, w tym na polu prawnym.

Umożliwiasz nam ostrzeganie innych o działaniach przestępców

Posiadając informacje o aktualnych niebezpieczeństwach możemy zwracać na nie uwagę szerszej grupie odbiorców.

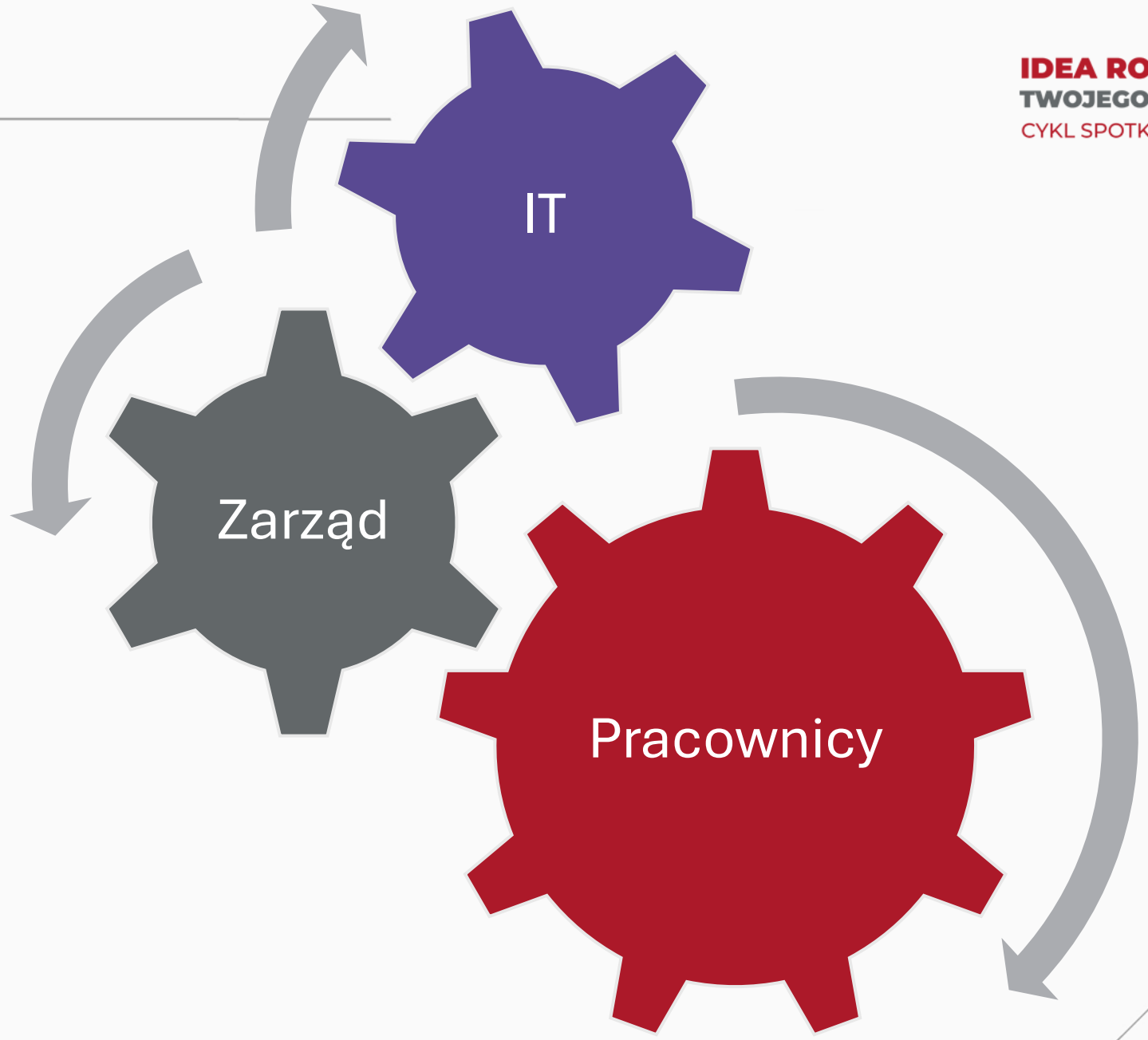
CERT.PL
NASK

Edukacja!

- https://cert.pl/
- https://bezpiecznymiesiac.pl/bm/baza-wiedzy

Szkolenia

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE



#IdeaRozwojuBiznesu


Świadomość
Szkolenia
Kanały zgłoszeń
Praktyka
Poczucie odpowiedzialności

IDEA ROZWOJU TWOJEGO BIZNESU
CYKL SPOTKAŃ ONLINE

PARP Grupa PFR

Ministerstwo Rozwoju i Technologii

Dziękuję za uwagę!

Zuzanna.polak@nask.pl

#IdeaRozwojuBiznesu