CYBERCLUE

Cyberbezpieczeństwo w BHP – czy wirusy noszą kaski?

Organizator konferencji:

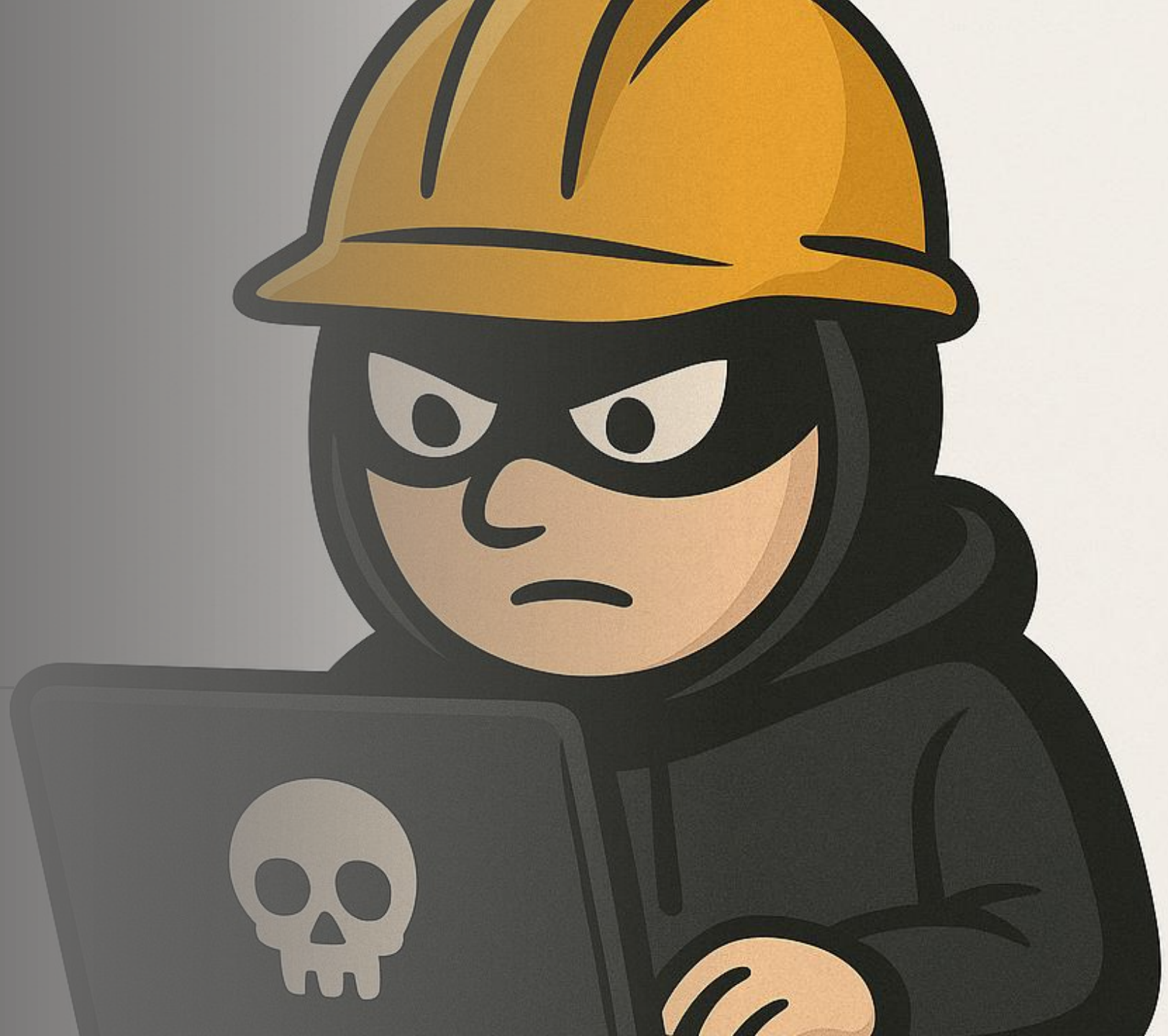
KOALICJA BEZPIECZNI W PRACY

www.cyberclue.tech | +48 606 445 156 | Izabela.taborowska@cyberclue.tech

Internal organization content

Cyberbezpieczeństwo w BHP – czy wirusy noszą kaski?

Prelekcja: Izabela Taborowska



CYBERCLUE

Uwaga Materiał Wybuchowy!

(brak tematu)

Od [redacted] dniu 2020-09-08 16:51

Szczegóły Zwykły tekst

Zrekrutowana przeze mnie osoba ukryła w budynku, w którym prowadzona jest Twoja firma, potężny materiał wybuchowy (PETN), który został zmontowany zgodnie z moimi instrukcjami.

Jest niewielka i bardzo dobrze zakryta, możliwe jest rozbicie konstrukcji budynku tym ładunkiem wybuchowym, ale w przypadku jego wybuchu będzie wiele rannych i martwych ludzi.
Mój człowiek kontroluje sytuację wokół budynku. Jeśli zauważy podejrzane działania lub zaangażowanie Policjantów, cała firma zostanie wysadzona w powietrze.

Mogę odwołać najemnika, jeśli zapłacisz. Płacisz mi 50 000 $ w Bitcoinie, a materiał wybuchowy zdetonuje, ale nie próbuj oszukiwać. Zapewniam, że odwołam najemnika dopiero po trzech potwierdzeniach w mojej sieci blockchain bitcoin.

Oto mój adres Bitcoin: 560eeedc-dfc3-4094-b761-93a54af55666

Jeśli będziesz próbował oszukiwać lub grać mądrze, zapewniam cię, że materiał wybuchowy nie wybuchnie.

Musisz mi zapłacić do końca dnia roboczego. Jeśli spóźnisz się z transakcją, wybuchną materiały wybuchowe.

Nic osobistego, jeśli nie otrzymam bitcoina i bomba wybuchnie, następnym razem inne komercyjne przedsiębiorstwa zapłacą mi dużo więcej, ponieważ nie jest to jednorazowa akcja.

Ze względów bezpieczeństwa i anonimowości nie zaloguję się na to konto e-mail, monitoruję swój adres co trzydzieści pięć minut i po zobaczeniu pieniędzy rozkazuję mojemu najemnikowi opuścić twój okręg.

Jeśli wybuchnie bomba i władze zobaczą następujący komunikat: Nie jesteśmy społeczeństwem terrorystycznym i nie bierzemy odpowiedzialności za wybuchy w innych miejscach.

Internal organization content

Czy hakerzy przestrzegają zasad bezpieczeństwa?

Haker w kasku? Brzmi absurdalnie… a jednak:

👉 Cyberzagrożenia mają wpływ na fizyczne bezpieczeństwo pracy.

👉 „Zabezpieczenia" to nie tylko kask i gaśnica, ale też firewall i silne hasła.

👉 Jeśli haker „zabezpieczy" system – pracownicy tracą dostęp do hali, maszyn czy wyjść ewakuacyjnych.

BHP i cyber to dwie strony tego samego medalu – chronią ludzi i organizację.

Internal organization content

Dlaczego cyber w BHP?

👉 Pracujemy w cyfrowym środowisku – nawet w fabryce czy na budowie.

👉 Awaria IT = realne ryzyko dla ludzi.

👉 Nowe źródło „wypadków przy pracy" → kliknięcia, phishing, blokada systemu.

„Tak jak mokra podłoga jest ryzykiem, tak samo ryzykiem jest mail z załącznikiem. Jedno i drugie może skończyć się 'wypadkiem przy pracy' – tylko innym."

Internal organization content

Ocena ryzyka 2.0

👉 Klasyczne ryzyka: hałas, pył, upadki.
👉 Nowe ryzyka: ransomware, phishing, sabotaż IT.
👉 Karta oceny ryzyka musi się rozszerzyć.

„Kiedyś w karcie oceny ryzyka wpisywało się: ‘śliska podłoga’.
Dziś warto dopisać: ‘email phishingowy’.”

Cyber w ocenie ryzyka:

👉 Phishing → stres, utrata danych.
👉 Sabotaż IT → zagrożenie życia (np. brak alarmu).
👉 Atak = ryzyko zawodowe tak samo realne jak hałas.

Kiedy ryzyko wpisujemy w karcie, często zapominamy, że komputer też może być źródłem wypadku.

Internal organization content

Przykłady ataków hakerskich wpływających na BHP

Atak na system kontroli dostępu

Hakerzy blokują karty wejściowe do budynku lub hali.
Pracownicy nie mogą się ewakuować w sytuacji zagrożenia.
Ryzyko: bezpośrednie zagrożenie życia, chaos podczas kryzysu.

Sabotaż systemu alarmowego / ewakuacyjnego

Atak ransomware blokuje serwery sterujące alarmami przeciwpożarowymi.
Alarm nie włącza się w razie zagrożenia, a procedury ewakuacyjne nie działają.
Ryzyko: opóźniona reakcja, panika, większa liczba poszkodowanych.

Atak na infrastrukturę przemysłową (ICS/SCADA)

Przejęcie kontroli nad maszynami (np. linia produkcyjna, roboty, zawory).
Maszyny zaczynają działać w sposób niebezpieczny dla operatorów.
Przykład realny: Stuxnet (Iran, 2010) – wirus, który zmieniał parametry pracy wirówek.

Cyberatak na system wentylacji i klimatyzacji

Hakerzy podnoszą temperaturę w serwerowni albo w biurowcu.
Ludzie narażeni są na przegrzanie, a sprzęt na awarie.
Ryzyko: zagrożenie zdrowia pracowników i przerwy w pracy.

Internal organization content

Przykłady ataków hakerskich wpływających na BHP

Manipulacja tablicami informacyjnymi w zakładzie

Wyświetlanie fałszywych komunikatów o zagrożeniu lub bezpieczeństwie.
Pracownicy mogą np. ignorować realne ryzyko, bo system został zmanipulowany.
Skutek: błędne decyzje w sytuacjach kryzysowych.

Atak na system medyczny w zakładzie pracy / szpitalu

Ransomware blokuje dostęp do dokumentacji medycznej i urządzeń (np. respiratorów).
Pracownicy służby zdrowia nie mogą leczyć pacjentów.
Przykład realny: ataki ransomware na szpitale w Niemczech, Francji, Czechach.

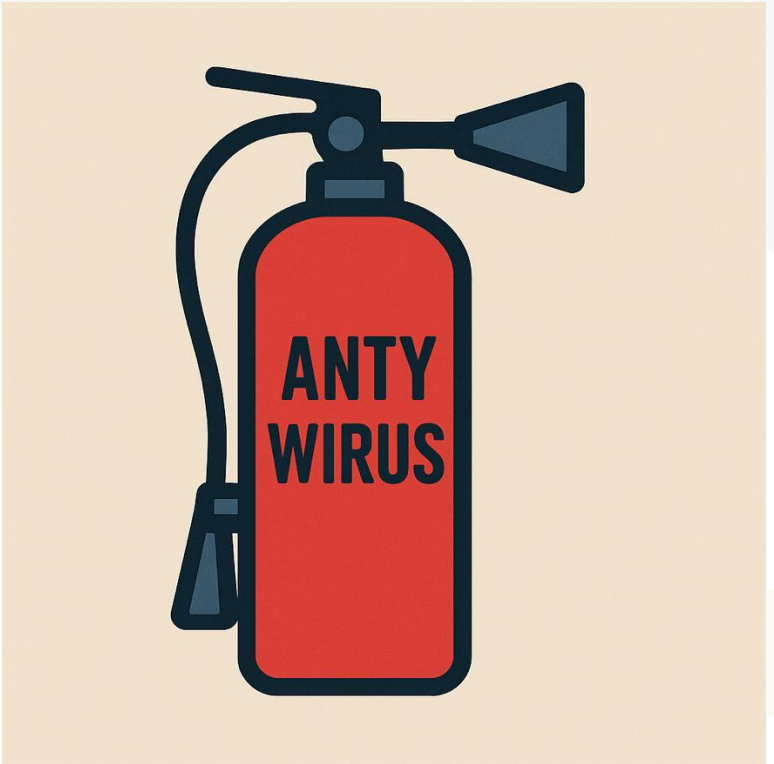
Sabotaż przez urządzenia IoT (np. kamery, czujniki dymu)

Hakerzy wyłączają kamery bezpieczeństwa i czujniki przeciwpożarowe.
Fałszywe poczucie bezpieczeństwa → brak reakcji na prawdziwe zagrożenie.

Cyberataki to nie tylko „kradzież danych". One przekładają się na życie i zdrowie ludzi, a BHP musi brać to pod uwagę.

Internal organization content

BHP-owiec = edukator



- 👉 Szkolenia z bezpiecznych zachowań → także przy komputerze.
- 👉 Zagrożenia cyber muszą wejść do katalogu BHP.
- 👉 Profilaktyka = mniejsze ryzyko incydentu.

„Specjalista BHP mówi: ‘Nie wkładaj ręki do maszyny’.
A dziś dodaje: ‘Nie klikaj w maila od księcia z Nigerii’.”

Internal organization content

Nowe procedury BHP

- Instrukcje: rękawice ochronne + aktualizacje systemu.
- Szkolenie: kask + silne hasło.
- Procedura ewakuacji: drzwi + backup IT.

„Tak, można uczyć obsługi wózka widłowego i… Outlooka w jednej sali.”

„Szkolenie wstępne?
Obok gaśnicy powinna być instrukcja ‘Jak nie dać się phishingowi’.”

Most IT – BHP

👉 IT zna technikalia.
👉 BHP zna ludzi.
👉 Razem → odporność organizacji.

To jak Batman i Robin – sami coś zrobią, ale w duecie są nie do zatrzymania.”

„IT może ustawić firewall, ale to BHP wie, że pracownik zawsze kliknie ‘dalej’. Dlatego muszą współpracować.”

Najczęstsze błędy pracowników

- 👉 Karteczki samoprzylepne z hasłami na monitorze.
- 👉 To samo hasło do wszystkiego.
- 👉 Klikanie ‘Tak, akceptuję’ bez czytania.

„To trochę jak w BHP: ‘Tak, wiem jak obsługiwać maszynę’.
I potem gips na 6 tygodni.”

Internal organization content

Co może zrobić BHP?

👉 Włączyć cyberbezpieczeństwo do szkoleń.
👉 Monitorować i zgłaszać incydenty.
👉 Tłumaczyć język IT na język pracownika.

„Bo IT mówi: ‘phishing’, a pracownik pyta: ‘To mogę otworzyć tego Excela od szefa, czy nie?’.”

Internal organization content

Cyber + BHP = duet idealny

👉 Firewalle i kaski.
👉 Antywirusy i gaśnice.
👉 Silne hasła i kamizelki odblaskowe.

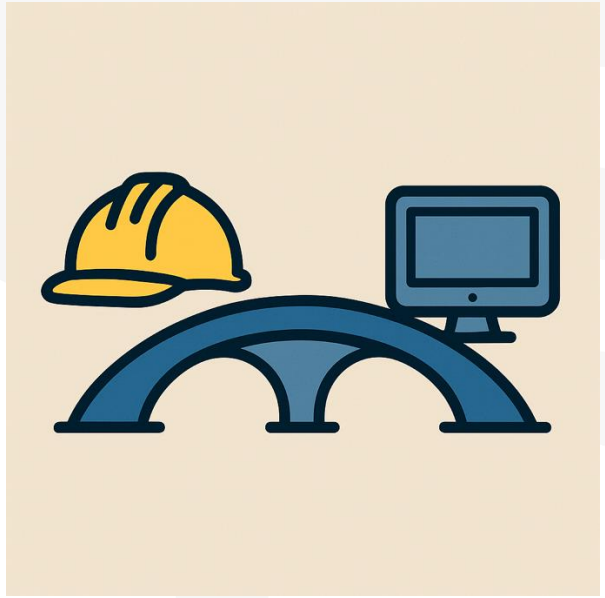
„Jedno chroni ciało, drugie dane – a bez jednego i drugiego, praca nie idzie.”

„I jedno, i drugie chroni nas przed bólem głowy. Tylko trochę innym.”

Internal organization content

CYBERCLUE

Podsumowanie



👉 Bezpieczeństwo = cyber + fizyczne.
👉 Zagrożenie może spaść z sufitu albo wyskoczyć z maila.
👉 Rola BHP-owców = rośnie w świecie cyfrowym.

💡 Bezpieczeństwo to nie tylko ochrona przeciw spadającej cegle,
ale również przed mailem, który może zablokować działanie całej firmy.

„Łączymy dwa światy – i dzięki temu mamy pełne bezpieczeństwo.
Od kasku po firewall.”

Internal organization content

CYBERCLUE

Zacznij od szkoleń!

Tylko dla uczestników konferencji Koalicji Bezpieczni w Pracy!

- 👉 Napisz na: info@cyberclue.tech
- 👉 Podaj hasło „Koalicja Bezpieczni w Pracy”
- 👉 Zgarnij rabat 20% na szkolenia z cyberbezpieczeństwa

KOALICJA BEZPIECZNI W PRACY

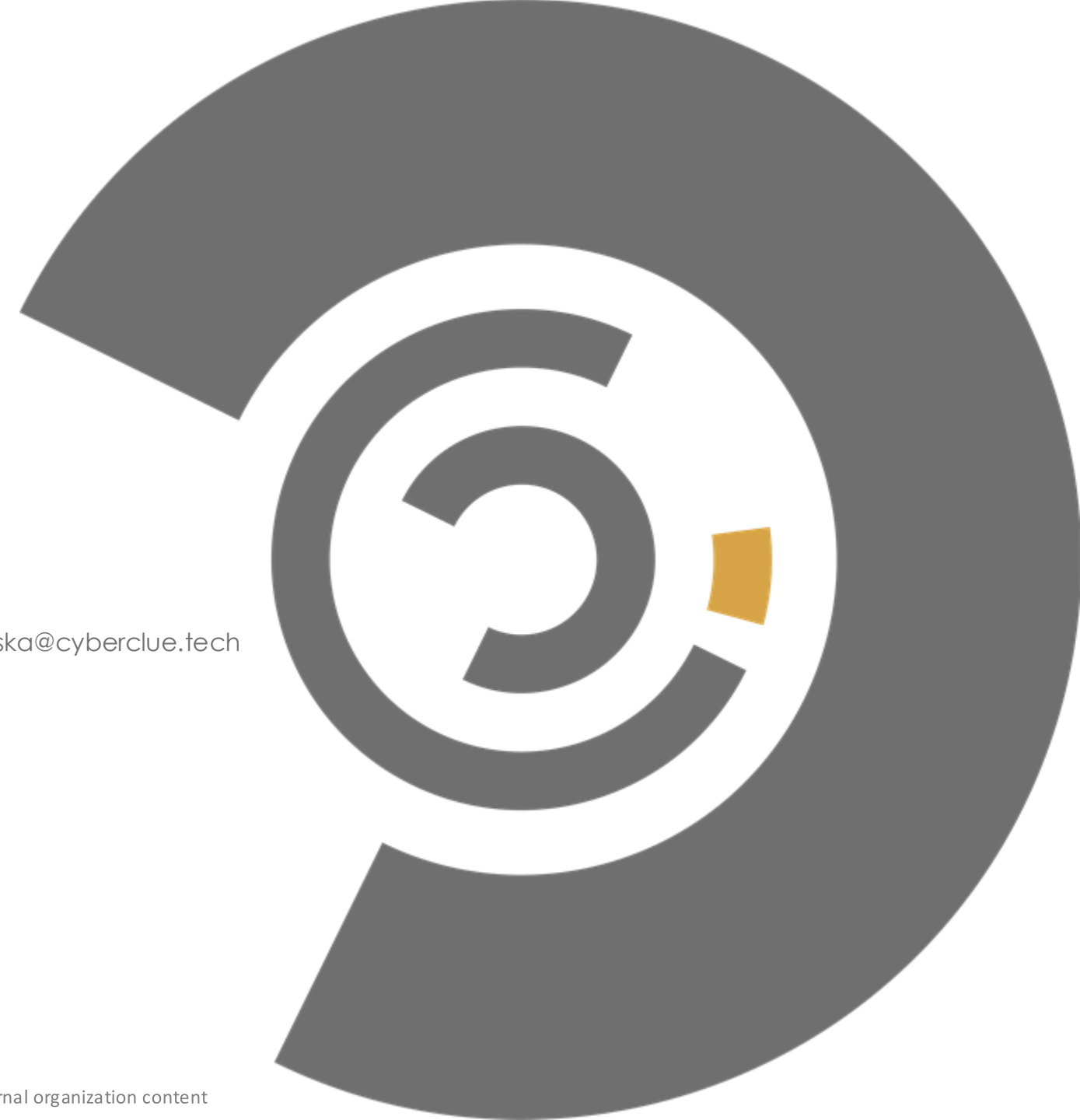
Internal organization content

CyberClue Sp. z o.o.

Izabela Taborowska
Prezeska

+48 606 445 156

Izabela.taborowska@cyberclue.tech



Internal organization content