Honeypots: Czy to my gonimy króliczka, czy króliczek goni nas?

Zrozumienie honeypotów i ich zastosowanie w bezpieczeństwie

Beata Zalewa, ISSA Poland Lublin, 15.04.2025

O mnie

Security Architect

Consultant

Microsoft Certified Trainer

AI & Cybersecurity Practitioner

Developer

Freelancer

Azure

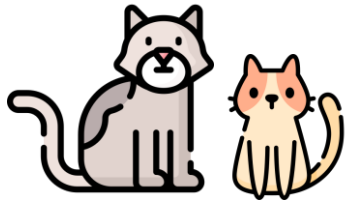
Azure @ ❤

aws

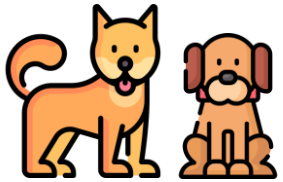
Google Cloud

1 Mąż

1 Córka



2 Koty



2 Psy

Kryminały

Fotografia

zalnet BEATA ZALEWA

https://www.linkedin.com/in/beatazalewa/

beata@zalnet.pl

BLOG https://zalnet.pl/

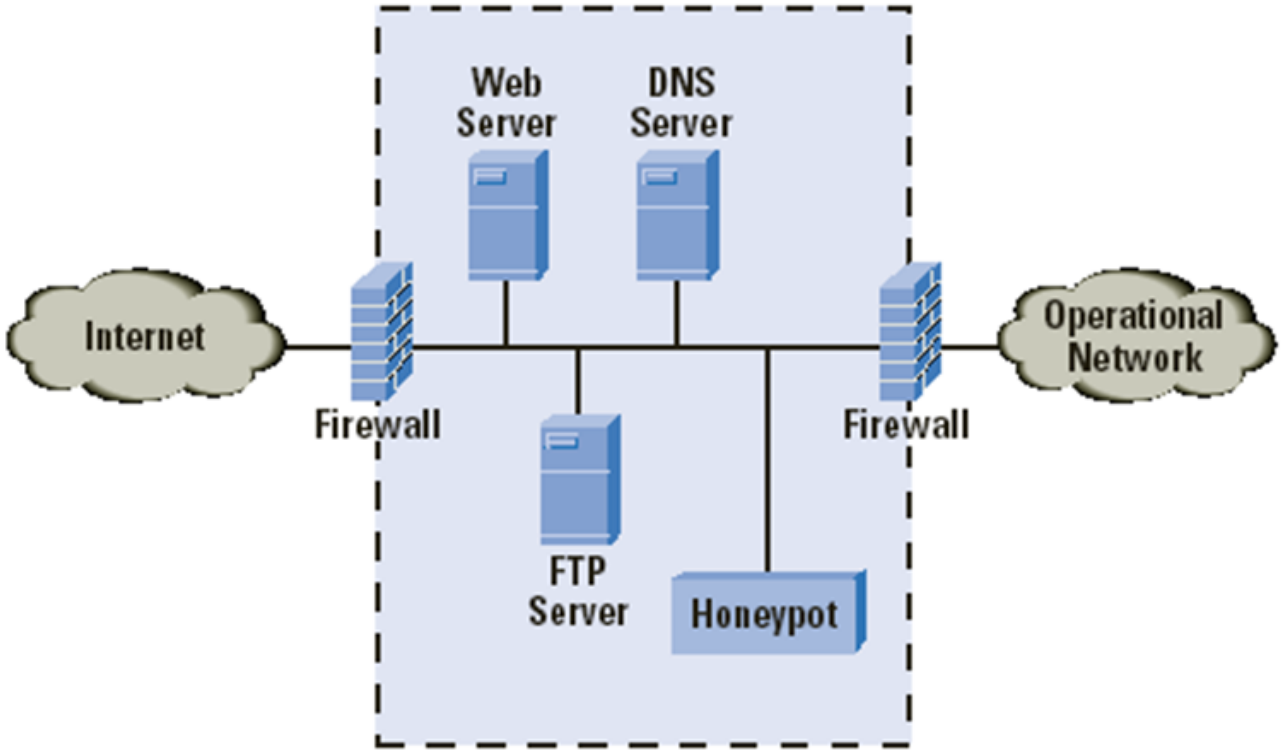
Agenda

- Podstawy honeypotów
- Dlaczego honeypoty są ważne w cybersecurity?
- Jak zacząć z honeypotami?
- Praktyczne zastosowania honeypotów
- Przyszłość honeypotów w cybersecurity

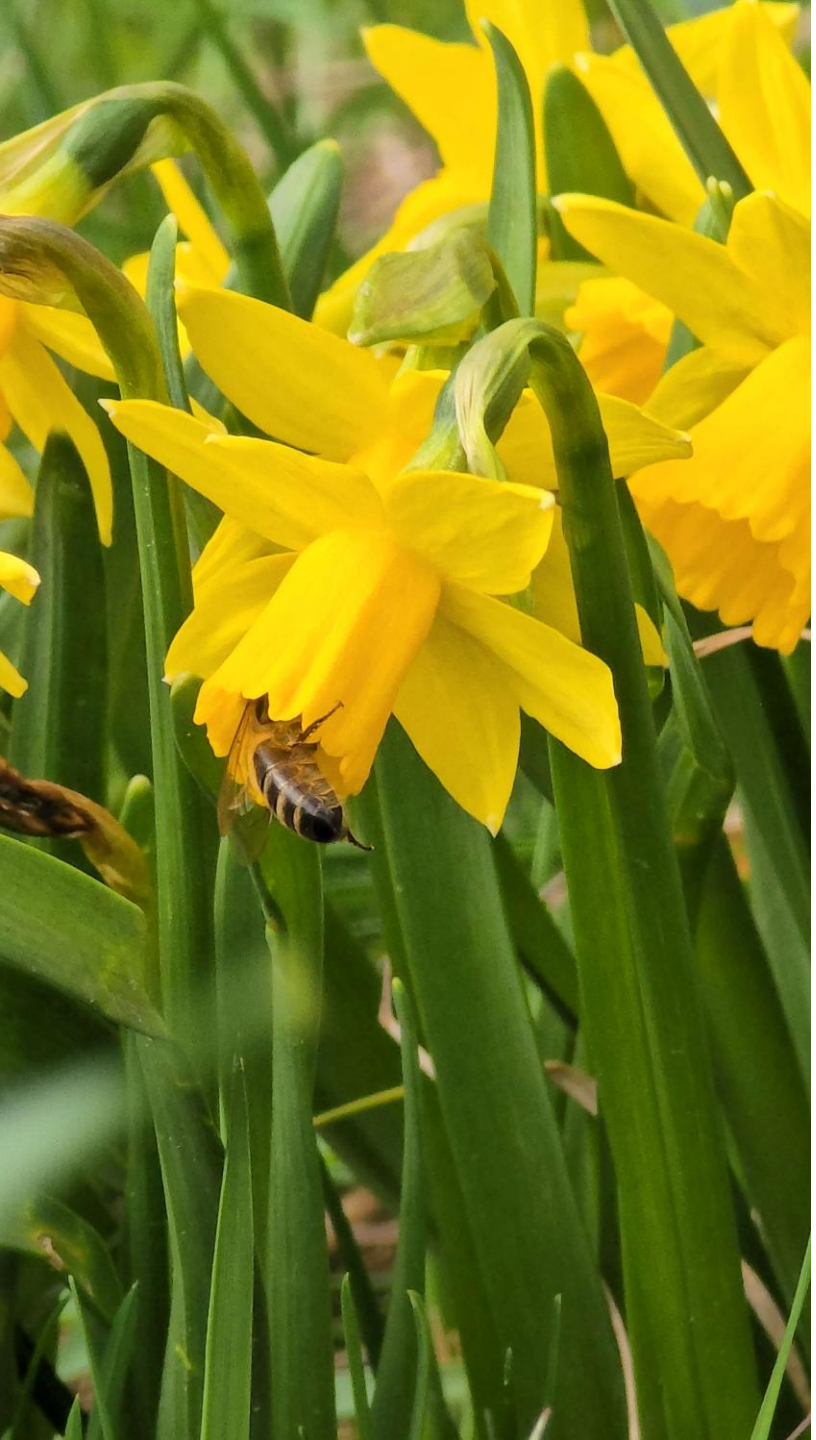
PODSTAWY HONEYPOTÓW

CZYM SĄ HONEYPOTY?

A Honey Pot is an intrusion detection technique used to study hackers' movements.



Źródło: internet



CZYM SĄ HONEYPOTY?

Cel honeypotów

Honeypoty są pułapkami zaprojektowanymi w celu przyciągania atakujących i zbierania informacji o ich działaniach.

Badanie technik ataków

Honeypoty służą do analizy technik ataków, co pozwala lepiej zrozumieć zagrożenia w sieci.

Identyfikacja luk w zabezpieczeniach

Honeypoty pomagają w identyfikacji potencjalnych luk w zabezpieczeniach, co jest kluczowe dla ochrony systemów.

RODZAJE HONEYPOTÓW

Honeypoty niskiej interakcji

Honeypoty niskiej interakcji symulują usługi, aby przyciągnąć atakujących i zbierać dane o ich działaniach.

Honeypoty wysokiej interakcji

Honeypoty wysokiej interakcji oferują pełną funkcjonalność systemu, co pozwala na bardziej zaawansowane badania i analizę ataków.

Zastosowania honeypotów

Każdy typ honeypota ma swoje specyficzne zastosowanie w ochronie przed cyberatakami i w badaniach nad bezpieczeństwem sieci.


HISTORIA
ZAKŁADANIA
PUŁAPEK


HISTORIA
ZAKŁADANIA
PUŁAPEK

HISTORIA ZAKŁADANIA PUŁAPEK


HISTORIA
ZAKŁADANIA
PUŁAPEK

HISTORIA I ROZWÓJ HONEYPOTÓW

- Honeypoty zaczynały jako proste pułapki na wirusy, pomagające w badaniu zagrożeń w sieci.
- Honeypoty ewoluowały w odpowiedzi na zmieniające się zagrożenia w sieci, stając się bardziej zaawansowanymi systemami obrony.
- Dziś honeypoty są kluczowymi elementami strategii bezpieczeństwa, służąc do wykrywania i analizowania zagrożeń.

DLACZEGO HONEYPOTY SĄ WAŻNE W CYBERSECURITY?

WYKRYWANIE I ANALIZA ZAGROŻEŃ

- Honeypoty są używane do zbierania cennych informacji o metodach ataków, co zwiększa bezpieczeństwo systemów.
- Analiza danych z honeypotów pozwala na identyfikację najnowszych trendów w cyberzagrożeniach, co jest kluczowe dla ochrony.
- W oparciu o zebrane dane, organizacje mogą tworzyć skuteczne strategie obronne, aby chronić swoje systemy przed zagrożeniami.

OCHRONA PRZED ATAKAMI I DEZINFORMACJĄ

- Honeypoty pełnią rolę pułapek, wciągając atakujących do fałszywych systemów, co zwiększa bezpieczeństwo.
- Dzięki honeypotom możemy zbierać cenne dane o atakach, co umożliwia lepsze zabezpieczenie systemów.
- Wprowadzenie dezinformacji może zniechęcić i rozproszyć uwagę atakujących, co chroni prawdziwe systemy.

WZMOCNIENIE SYSTEMÓW OBRONNYCH

Dane z honeypotów

Dane uzyskane z honeypotów pomagają w identyfikacji i zrozumieniu zachowań zagrożeń, co wzmacnia systemy bezpieczeństwa.

Analiza luk w zabezpieczeniach

Analiza działania systemów obronnych pozwala na identyfikację luk, które mogą być wykorzystane przez cyberprzestępców.

Wzmocnienie polityk bezpieczeństwa

Wzmocnienie polityk bezpieczeństwa jest kluczowe dla skutecznej obrony przed nowymi zagrożeniami w cyberprzestrzeni.

JAK ZACZĄĆ Z HONEYPOTAMI?

WYBÓR ODPOWIEDNIEGO TYPU HONEYPOTA

- Właściwy wybór honeypota wpływa na skuteczność strategii bezpieczeństwa. Różne typy honeypotów służą różnym celom.
- Różne typy honeypotów mogą lepiej odpowiadać na specyficzne potrzeby organizacji w zakresie bezpieczeństwa.
- Zanim podejmiemy decyzję, ważne jest, aby jasno określić cele, które chcemy osiągnąć za pomocą honeypotów.

KONFIGURACJA I WDROŻENIE HONEYPOTA

- Dokładna konfiguracja honeypota jest kluczowa dla jego skuteczności w identyfikacji i analizie zagrożeń.
- Honeypot musi być odpowiednio zabezpieczony, aby nie stał się celem ataków i nie zagrażał sieci.

MONITOROWANIE I ANALIZA DANYCH

- Monitorowanie honeypotów jest kluczowe, aby zapewnić ich skuteczność w wykrywaniu ataków i zabezpieczaniu systemów.
- Regularna analiza danych pozwala na szybkie reagowanie na incydenty oraz na poprawę strategii obronnych.
- Analiza danych z honeypotów umożliwia zbieranie cennych informacji o metodach ataku, co wzmacnia ochronę systemów.

PRAKTYCZNE ZASTOSOWANIA HONEYPOTÓW

PRZYKŁADY UDANYCH WDROŻEŃ

- Honeypoty są skutecznym narzędziem w wykrywaniu zagrożeń i podejrzanej aktywności w sieciach organizacji.
- Honeypoty pomagają w zabezpieczaniu systemów, odwracając uwagę atakujących i zbierając cenne dane o zagrożeniach.

https://www.controleng.com/throwback-attack-chinese-hackers-fall-for-a-honeypot-trap/

NAJLEPSZE PRAKTYKI I ZALECENIA

- Honeypoty powinny być starannie integrowane z istniejącą infrastrukturą bezpieczeństwa, aby były efektywne w wykrywaniu zagrożeń.
- Regularne zarządzanie i monitorowanie honeypotów jest kluczowe dla maksymalizacji ich skuteczności w wykrywaniu ataków.
- Analiza danych zbieranych przez honeypoty dostarcza cennych informacji o zachowaniach atakujących i pozwala na lepsze zabezpieczenie systemów.

DEMO

https://github.com/paralax/awesome-honeypots

PRZYSZŁOŚĆ HONEYPOTÓW W CYBERSECURITY

NOWE TECHNOLOGIE I INNOWACJE

- Honeypoty mogą korzystać z najnowszych narzędzi do zarządzania i wykrywania zagrożeń, poprawiając swoją skuteczność.
- Wprowadzenie nowych metod operacyjnych może zwiększyć zdolność honeypotów do zwalczania cyberzagrożeń i wyzwań.
- Honeypoty mogą przyjąć nowe formy, takie jak inteligentne systemy, które uczą się i adaptują do zmieniającego się środowiska zagrożeń.

ADAPTACJA DO ZMIENIAJĄCYCH SIĘ ZAGROŻEŃ

- Zagrożenia w cyberprzestrzeni stale się zmieniają, co wymaga innowacyjnych strategii obrony.
- Honeypoty muszą być elastyczne i przystosowane do nowych technik ataków, aby zapewnić skuteczną ochronę.
- Rozwój nowych metod działania honeypotów pozwala na lepszą identyfikację i analizę ataków.

WNIOSKI

Honeypoty jako narzędzie bezpieczeństwa

Honeypoty wykrywają ataki i zbierają cenne dane na temat zagrożeń, co czyni je kluczowym elementem obrony.

Wsparcie strategii obronnych

Honeypoty dostarczają informacji, które pomagają w opracowywaniu efektywnych strategii obronnych przeciwko cyberatakom.

Zwiększenie bezpieczeństwa systemów

Właściwe wdrożenie honeypotów zwiększa ogólne bezpieczeństwo systemów, zmniejszając ryzyko udanych ataków.

Stale poszukuję nowych możliwości i ekscytujących wyzwań. Jeśli chcesz się ze mną skontaktować, proszę, skorzystaj z poniższych kanałów:

zalnet
BEATA ZALEWA

Email: beata@zalnet.pl

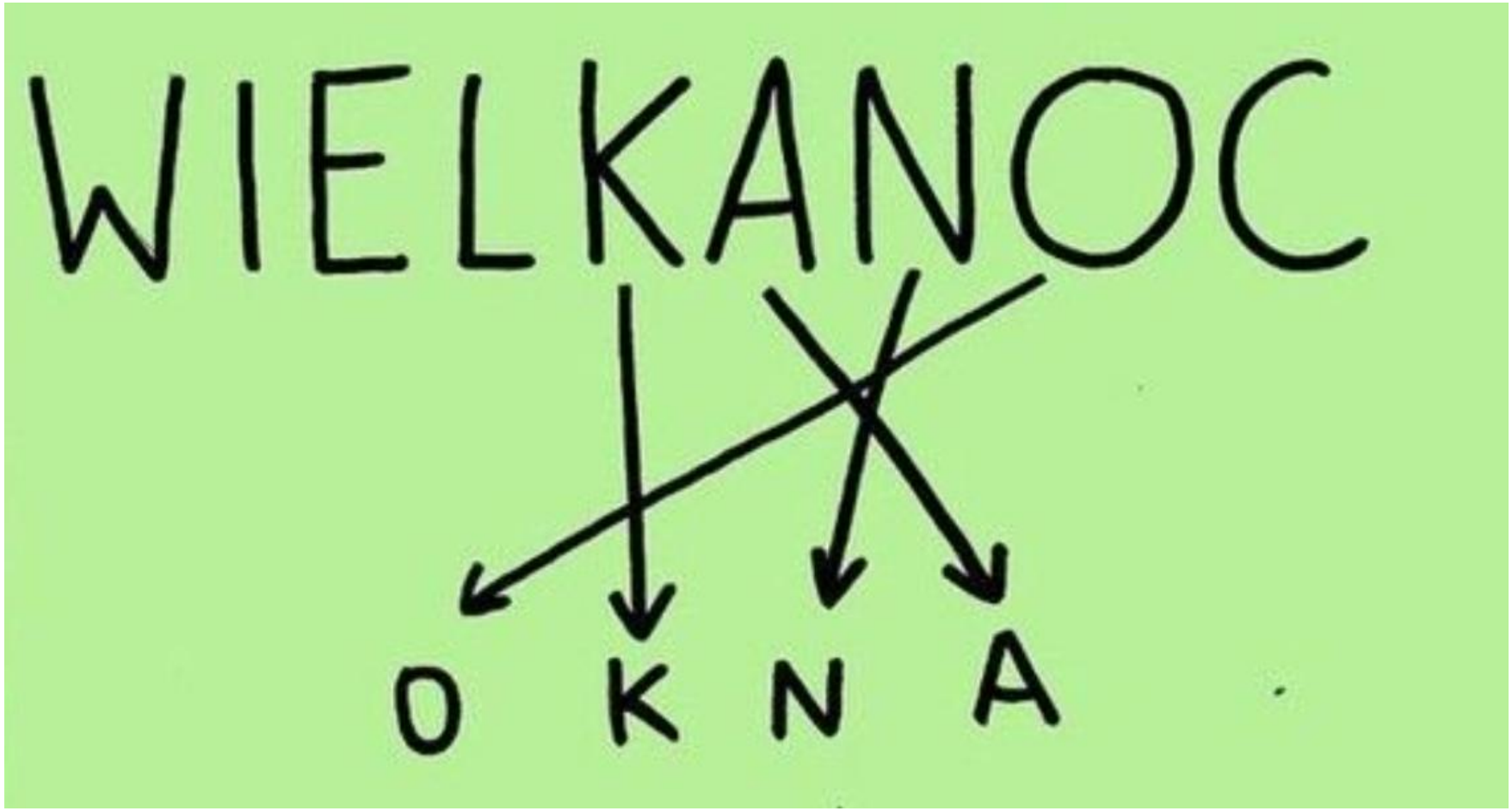
LinkedIn: https://www.linkedin.com/in/beatazalewa/

Blog: https://zalnet.pl/blog/

X: https://x.com/beatazalewa

GitHub: https://github.com/beatazalewa/Conferences/

Wesołych Świąt



Źródło: https://gloswielkopolski.pl/