

[Akceptuje](#)

W ramach naszej witryny stosujemy pliki cookies w celu świadczenia państwu usług na najwyższym poziomie, w tym w sposób dostosowany do indywidualnych potrzeb. Korzystanie z witryny bez zmiany ustawień dotyczących cookies oznacza, że będą one zamieszczone w Państwa urządzeniu końcowym. Możecie Państwo dokonać w każdym czasie zmiany ustawień dotyczących cookies. Więcej szczegółów w naszej [Polityce Prywatności](#)

[Portal](#) [Informacje](#) [Katalog firm](#) [Praca](#) [Szkolenia](#) [Wydarzenia](#) [Porównania międzylaboratoryjne](#)
[Kontakt](#)



[Laboratoria](#)
[.net](#)
[Innowacje](#)
[Nauka](#)
[Technologie](#)



[Logowanie](#) [Rejestracja](#) [pl](#)

Newsletter

zapisz się

Naukowy styl życia

Nauka i biznes

- [Nowe technologie](#)
- [Felieton](#)
- [Tygodnik "Nature"](#)
- [Edukacja](#)
- [Artykuły](#)
- [Przemysł](#)

[Strona główna](#) > [Informacje](#)

Polski CERT zbadał pułapki na cyberprzestępców



Użyteczność tzw. honeypotów, czyli zastawianych w sieci pułapek na cyberprzestępców, zbadał zespół CERT Polska działający w ramach instytutu badawczego NASK. Polacy szczególnie zbadali 30 różnych darmowych pułapek, z których korzystają eksperci od bezpieczeństwa internetowego.

Jak wyjaśnili przedstawiciele CERT Polska w przesłanym PAP komunikacie, honeypot (z ang. „garnek miodu”), jest zasobem umieszczonym w sieci, którego jedynym zadaniem jest to, by dostać się w ręce hakerów czy cyberprzestępców i zostać wykorzystanym w nieautoryzowany sposób. Zasobem-pułapką może być np. specjalnie przygotowany serwis, aplikacja, system czy nawet jakaś informacja. Wszystko to kusić ma cyberprzestępców do ataku.

Podstawowym założeniem jest to, że każdy, kto próbuje się połączyć lub korzystać z honeypota w jakikolwiek sposób jest z definicji podejrzany. Cała interakcja pomiędzy honeypotem i podmiotem, który się z nim łączy jest monitorowana i analizowana, aby wykryć złośliwe działania i zrozumieć ich mechanizmy.

Honeypoty mogą być stosowane m.in. do monitorowania aktywności botnetów i robaków w Internecie, zbierania informacji o zainfekowanych komputerach w sieci, wykrywania i zbierania złośliwego oprogramowania, badania zachowań hakerów oraz szukania wewnętrznych infekcji w sieci lub ataków wewnętrznych.

Jak podkreślają specjaliści z CERT Polska, honeypoty, dzięki wczesnemu ostrzeganiu o infekcji i zachowaniu złośliwego oprogramowania, pozostają bardzo dobrą platformą do pozyskiwania informacji o zmianach w taktyce cyberprzestępców.

"W związku z dużą ilością dostępnych honeypotów warto było zbadać i wskazać te systemy, które mogą być najbardziej przydatne w praktyce dla ekspertów od cyberbezpieczeństwa na całym świecie, działających na przykład w krajowych zespołach reagowania na zagrożenia sieciowe. Mamy nadzieję, że nasze zestawienie przyczyni się do wyboru najlepszych narzędzi oraz metod zwalczania złośliwego oprogramowania i działalności cyberprzestępców" - mówi Piotr Kijewski, kierownik CERT Polska.

W badaniu, opublikowanym przez Europejską Agencję ds. Bezpieczeństwa Informacji, specjaliści z CERT Polska przeanalizowali pod kątem praktyczności 30 istniejących, darmowych honeypotów, które można samodzielnie zainstalować w sieci. Bezpośrednim celem było zestawienie dostępnych rozwiązań, analiza ich zalet i wad oraz wskazanie podmiotom zajmującym się cyberbezpieczeństwem najskuteczniejszych narzędzi do walki z zagrożeniami sieciowymi.

Wśród czynników branych pod uwagę były m.in. zakres wykrywania, jakość dostarczanych danych, wydajność i niezawodność oraz łatwość instalacji i obsługi. Cztery z badanych systemów - Dionaea, Glastopf, Kippo oraz Honeyd, zostały zidentyfikowane jako najbardziej użyteczne i najłatwiejsze do zainstalowania.

Więcej informacji na temat raportu CERT Polska o zastosowaniu honeypotów do wykrywania zagrożeń sieciowych (ang. „Proactive Detection of Security Incidents: Honeypots”) dla Europejskiej Agencji ds. Bezpieczeństwa Informacji, dostępnych jest na stronie: <http://www.cert.pl/news/6609>

źródło: www.naukawpolsce.pap.pl

<https://laboratoria.net/aktualnosci/15827.html>



30-03-2026

[Stypendia ministra nauki za znaczące osiągnięcia](#)

Przyznał je 402 osobom.



30-03-2026

[Doktor z TikToka: fajnie by było, gdyby w sieci to jednak naukowcy...](#)

Aby chronić pisklęta przed pasożytami.



30-03-2026

[Kierownik wyprawy polarnej](#)

Zmiany klimatu widać gołym okiem.



30-03-2026

[Mikrolasery mogą wykrywać pojedyncze cząsteczki](#)

Informuje pismo „Nature Photonics”.



30-03-2026

[Duże teleskopy sfotografowały dwie formujące się planety](#)

Ogłosiło Europejskie Obserwatorium Południowe (ESO).



30-03-2026

[Bakteriofagi mogą chronić żywność przed salmonellą](#)

Informuje pismo „Applied and Environmental Microbiology”.



30-03-2026

Rękawiczki mogą zawyżać wyniki pomiarów mikroplastiku

Informuje specjalistyczne pismo „Analytical Methods”.



30-03-2026

Problem dezinformacji medycznej będzie narastał

Szkolenia na UMB dla przyszłych lekarzy

Informacje dnia: [Stypendia ministra nauki za znaczące osiągnięcia Doktor z TikToka: fajnie by było, gdyby w sieci to jednak naukowcy mówili o nauce](#) [Kierownik wyprawy polarnej Mikrolasery mogą wykrywać pojedyncze cząsteczki](#) [Duże teleskopy sfotografowały dwie formujące się planety](#) [Bakteriofagi mogą chronić żywność przed salmonellą](#) [Stypendia ministra nauki za znaczące osiągnięcia Doktor z TikToka: fajnie by było, gdyby w sieci to jednak naukowcy mówili o nauce](#) [Kierownik wyprawy polarnej Mikrolasery mogą wykrywać pojedyncze cząsteczki](#) [Duże teleskopy sfotografowały dwie formujące się planety](#) [Bakteriofagi mogą chronić żywność przed salmonellą](#) [Stypendia ministra nauki za znaczące osiągnięcia Doktor z TikToka: fajnie by było, gdyby w sieci to jednak naukowcy mówili o nauce](#) [Kierownik wyprawy polarnej Mikrolasery mogą wykrywać pojedyncze cząsteczki](#) [Duże teleskopy sfotografowały dwie formujące się planety](#) [Bakteriofagi mogą chronić żywność przed salmonellą](#)

Partnerzy