

[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>



21-05-2026

[Nowy wzór elektronicznej legitymacji studenckiej](#)

Resort nauki udostępnił go.



21-05-2026

[Kleszcz to tylko pośrednik](#)

Krętki Borrelia to częściowo „prezent” od gryzoni i ptaków.



21-05-2026

[Pod względem leczenia czerniaka Polska w](#)

czołowce Europy

W ciągu 8 lat przeżywalność pacjentów z tym nowotworem wzrosła o 20 proc.



21-05-2026

Przyszłość pszczół zależy od ochrony ich naturalnych siedlisk

Bez zapylaczy nie ma części produkcji żywności.



21-05-2026

Powstała niewidzialna elektroda dla podczerwieni

Elektrodę, która przepuszcza aż 94 proc. promieniowania podczerwonego.



21-05-2026

Choroby serca mogą zaczynać się już w czasie życia płodowego

To wynik badania, w którym brało ponad tysiąc par matka-dziecko.



21-05-2026

Problemy ze snem związane z ryzykiem choroby Alzheimera u kobiet

Informuje „Journal of Prevention of Alzheimer's Disease”.



21-05-2026

Zespół policystycznych jajników zmienił nazwę

Informuje "The Lancet".

Informacje dnia: [Nowy wzór elektronicznej legitymacji studenckiej Kleszcz to tylko pośrednik Pod względem leczenia czerniaka Polska w czołówce Europy Przyszłość pszczół zależy od ochrony ich naturalnych siedlisk Powstała niewidzialna elektroda dla podczerwieni Choroby serca mogą zaczynać się już w czasie życia płodowego Nowy wzór elektronicznej legitymacji studenckiej Kleszcz to tylko pośrednik Pod względem leczenia czerniaka Polska w czołówce Europy Przyszłość pszczół zależy od ochrony ich naturalnych siedlisk Powstała niewidzialna elektroda dla podczerwieni Choroby serca mogą zaczynać się już w czasie życia płodowego Nowy wzór elektronicznej legitymacji studenckiej Kleszcz to tylko pośrednik Pod względem leczenia czerniaka Polska w czołówce Europy Przyszłość pszczół zależy od ochrony ich naturalnych siedlisk Powstała niewidzialna elektroda dla podczerwieni Choroby serca mogą zaczynać się już w czasie życia płodowego](#)

Partnerzy