



WPROWADZENIE DO CYBERBEZPIECZEŃSTWA

KURS WSTĘPNY: WPROWADZENIE

CELE KURSU I ZARYS DZISIEJSZEGO WYKŁADU

Zdobądź podstawową wiedzę i zrozumienie terminologii i technologii związanych z cyberbezpieczeństwem.

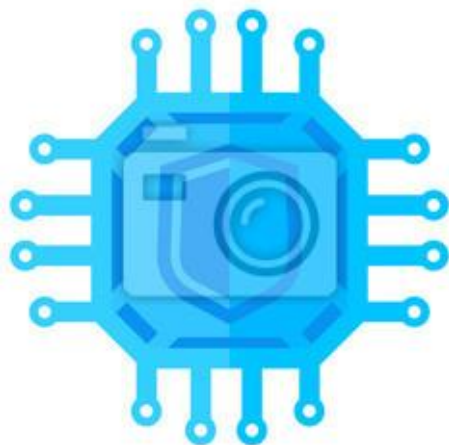
- Dlaczego cyberbezpieczeństwo?
- Zasady cyberbezpieczeństwa
- Rozwój technologii cyberbezpieczeństwa

ZALECANE PODRĘCZNIKI

1. Banasiński et al., *Cyberbezpieczeństwo*, Wolters Kluwer, Warszawa 2020.
2. Łakomy M., *Bezpieczeństwo teleinformatyczne (cyberbezpieczeństwo)*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2019.
3. Górka M. (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Difin 2014.
4. Snowden E., *Pamięć nieulotna*, Wydawnictwo Insignis, 2019.
5. Banasiński C., Rojszczak M., *Cyberbezpieczeństwo, Seria: Prawo w praktyce*, wyd. Wolters Kluwer Polska, Warszawa 2020.
6. Kowalewski J., *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017.
7. Bednarek J., Andrzejewska A., *Zagrożenia cyberprzestrzeni i świata wirtualnego*, Difin, Warszawa 2014.
8. Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni*, Wydawnictwo CeDeWu, Warszawa 2016.
9. Unold J., *Zarządzanie informacją w cyberprzestrzeni*, PWN, Warszawa 2021.
10. Kraśniewski A., *Cybersecurity Research, Education and Management: University Perspective*, Oficyna Wydawnicza Politechniki Warszawskiej.

DLACZEGO CYBERBEZPIECZEŃSTWO?

DLACZEGO CYBERBEZPIECZEŃSTWO?



Kluczowa globalna konieczność
Ciągły rozwój technologiczny
Ciekawa i satysfakcjonująca dziedzina
Ciągłe kształcenie w zawodzie

BLUE TEAM



Utrzymuje bezpieczeństwo systemów
Zapobiega naruszeniom bezpieczeństwa
Monitoruje systemy pod kątem potencjalnych zagrożeń
Rozwija technologię zabezpieczeń

STANOWISKA MONITOROWANIA SIECI



Technik Centrum Operacji Sieciowych

Odpowiedzialny za monitorowanie i pomoc
w zakresie wsparcia technicznego i rutynowej konserwacji



Analitik Centrum Operacji Bezpieczeństwa

Monitoruje i zarządza sieciami;
korzysta z systemów wykrywania / zapobiegania włamaniom



Administrator Bezpieczeństwa Sieci

Odpowiedzialny za zarządzanie i monitorowanie
bezpieczeństwa sieci przedsiębiorstwa

STANOWISKA IT DOTYCZĄCE CYBERBEZPIECZEŃSTWA



Technik Cyberbezpieczeństwa

Zapewnia bezpieczeństwo komputerowych systemów informatycznych i kontroluje dostęp do systemów w oparciu o klasyfikacje użytkowników



Inżynier Wsparcia IT

Rozwiązuje problemy techniczne klientów i personelu w przedsiębiorstwie

STANOWISKA BADAWCZE DOTYCZĄCE CYBERBEZPIECZEŃSTWA



Analitik ds. Cyberbezpieczeństwa Defensywnego

Bada i ocenia zagrożenia związane z cyberbezpieczeństwem;
zaleca modyfikacje cyberobrony przedsiębiorstwa



Inżynier Adaptacyjnej Replikacji Zagrożeń

Odtwarza rzeczywiste zagrożenia,
aby zrozumieć ich działanie i je neutralizować

STANOWISKA BADANIA ZAGROŻEŃ



Badacz Przestępstw Związanych z Cyberbezpieczeństwem
Gromadzi dowody i ślady informacji cyfrowych w systemach informatycznych aby ustalić w jaki sposób popełniono cyberprzestępstwa



Analityk Oceny Podatności

Wyszukuje krytyczne wady i luki w sieciach, często jako zewnętrzny konsultant

CYBERSEEK

Zawiera szczegółowe informacje na temat stanowisk związanych z cyberbezpieczeństwem dostępnych na rynku pracy.

Pomaga znaleźć osoby poszukujące pracy, pracodawców, nauczycieli i doradców zawodowych.

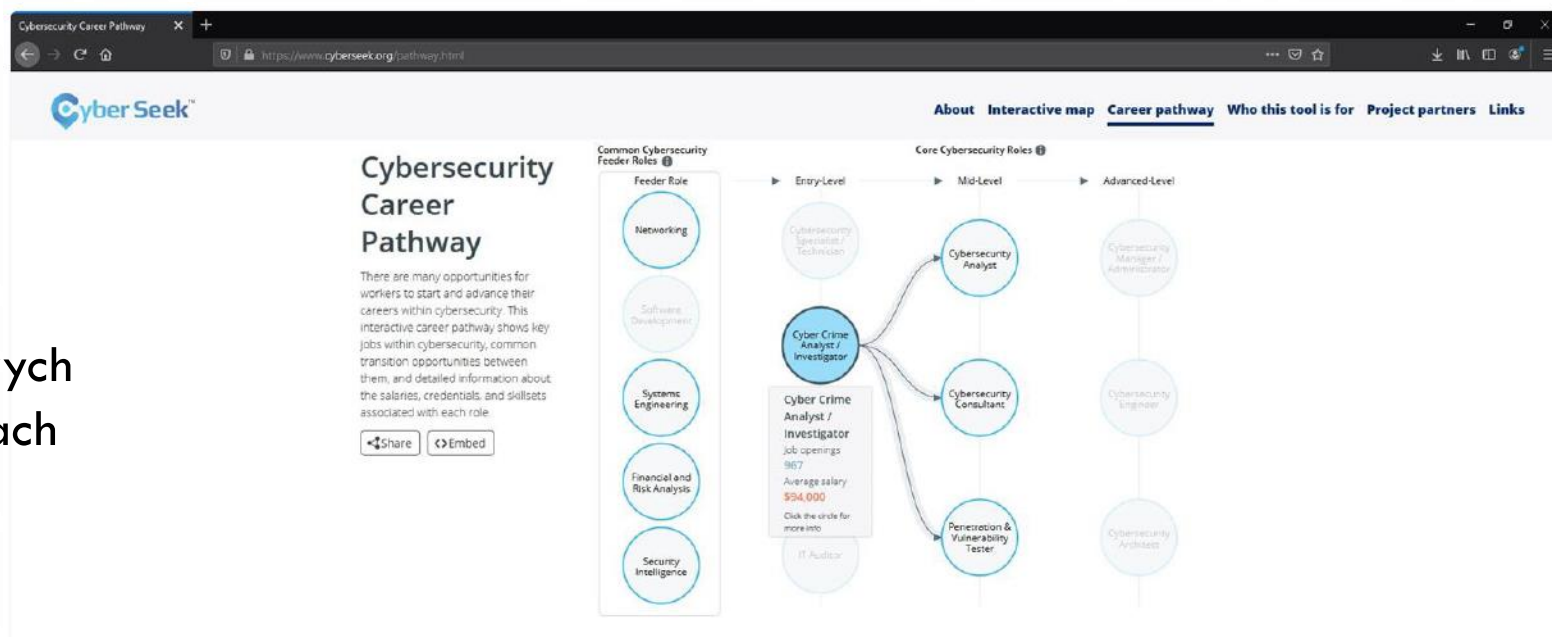
<https://www.cyberseek.org/>



ŚCIEŻKI KARIERY W CYBERSEEK

Dostarcza informacje o możliwych ścieżkach kariery i możliwościach zatrudnienia w obszarze cyberbezpieczeństwa.

Zawiera również szczegółowe informacje, takie jak średnie wynagrodzenia i dostępne stanowiska



ZASADY CYBERBEZPIECZEŃSTWA

POJĘCIA



Bezpieczeństwo informacji

Obrona i ochrona samych informacji, zarówno cyfrowych, jak i fizycznych



Bezpieczeństwo cybernetyczne (cyberbezpieczeństwo)

Obrona i ochrona cyberprzestrzeni* przed wszelkiego rodzaju przestępstwami

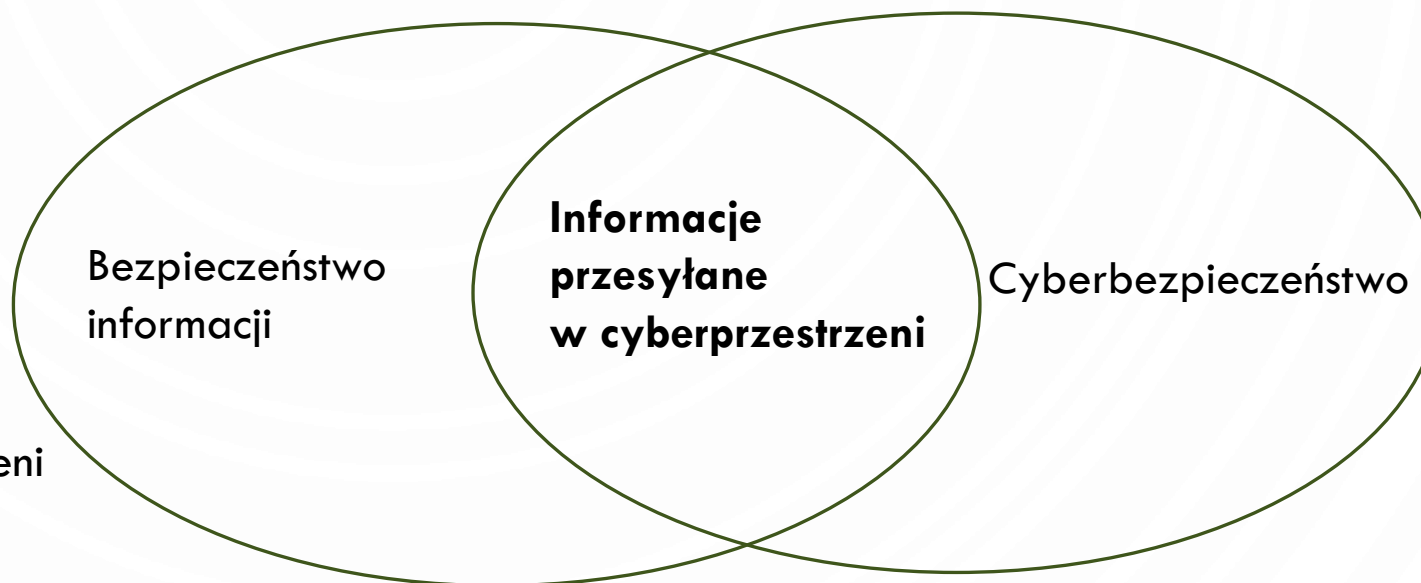
*Iluzja świata rzeczywistego stworzona za pomocą metod teleinformatycznych. Ułatwia wymianę, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikację między człowiekiem i komputerem.

CYBERPRZESTRZEŃ: OBSZAR WSPÓLNY

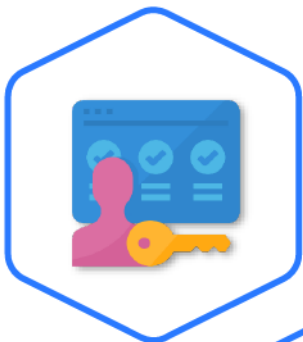
Bezpieczeństwo informacji
odnosi się do ochrony
wszelkiego rodzaju informacji

Cyberbezpieczeństwo
odnosi się do obrony cyberprzestrzeni
i zapewnienia jej integralności

**Informacje przesyłane
w cyberprzestrzeni**
odnoszą się do informacji
udostępnianych przez sieci komputerowe



CIA



Confidentiality (Poufność)

Akt udostępniania lub ujawniania informacji wyłącznie upoważnionemu personelowi



Integrity (Integralność)

Zdolność do zapewnienia, że informacje lub dane pozostaną niezmienione



Availability (Dostępność)

Zapewnienie dostępności danych lub usług tym, którzy ich potrzebują, wtedy, gdy ich potrzebują

TERMINOLOGIA STOSOWANA W CYBERBEZPIECZEŃSTWIE



Zasób
(Asset)



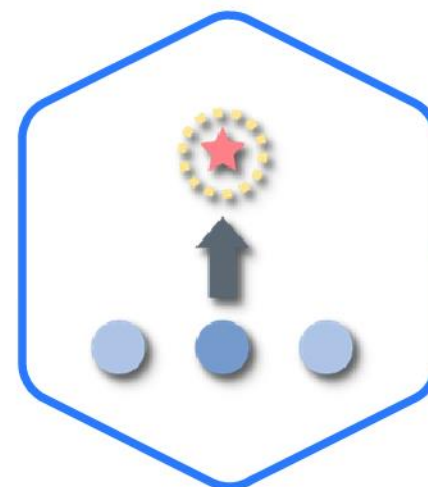
Zagrożenie
(Threat)



Ryzyko
(Risk)

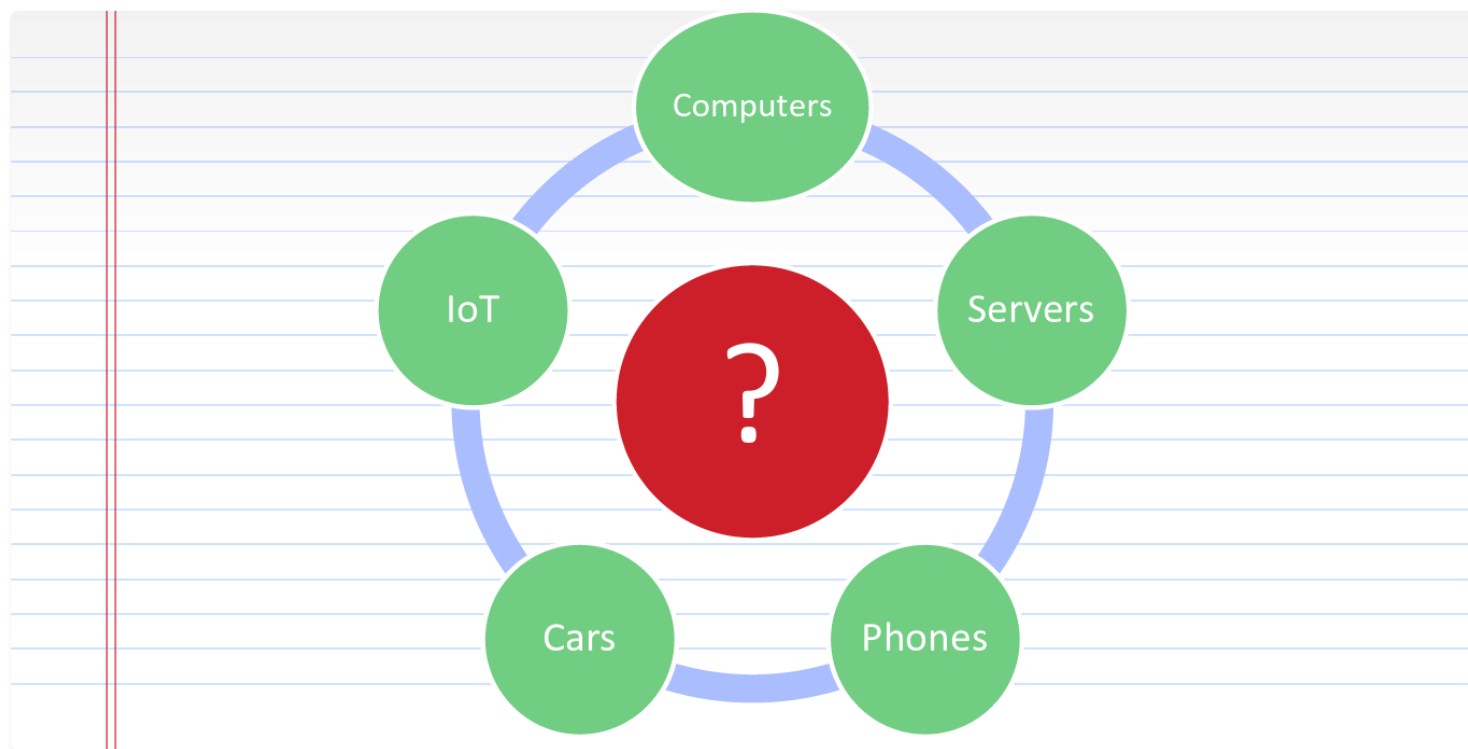


Podatność
(Vulnerability)



Wykorzystanie
(Exploit)

CO CHCEMY CHRONIĆ?



Jest wiele rzeczy do ochrony, ale jedna z nich jest najważniejsza!

TECHNOLOGIE STOSOWANE W CYBERBEZPIECZEŃSTWIE



Firewall

Sprawdza, wykrywa i blokuje ruch w oparciu o zasady i parametry (IP, port itp.)



Antywirus

Sprawdza, wykrywa i usuwa złośliwe programy

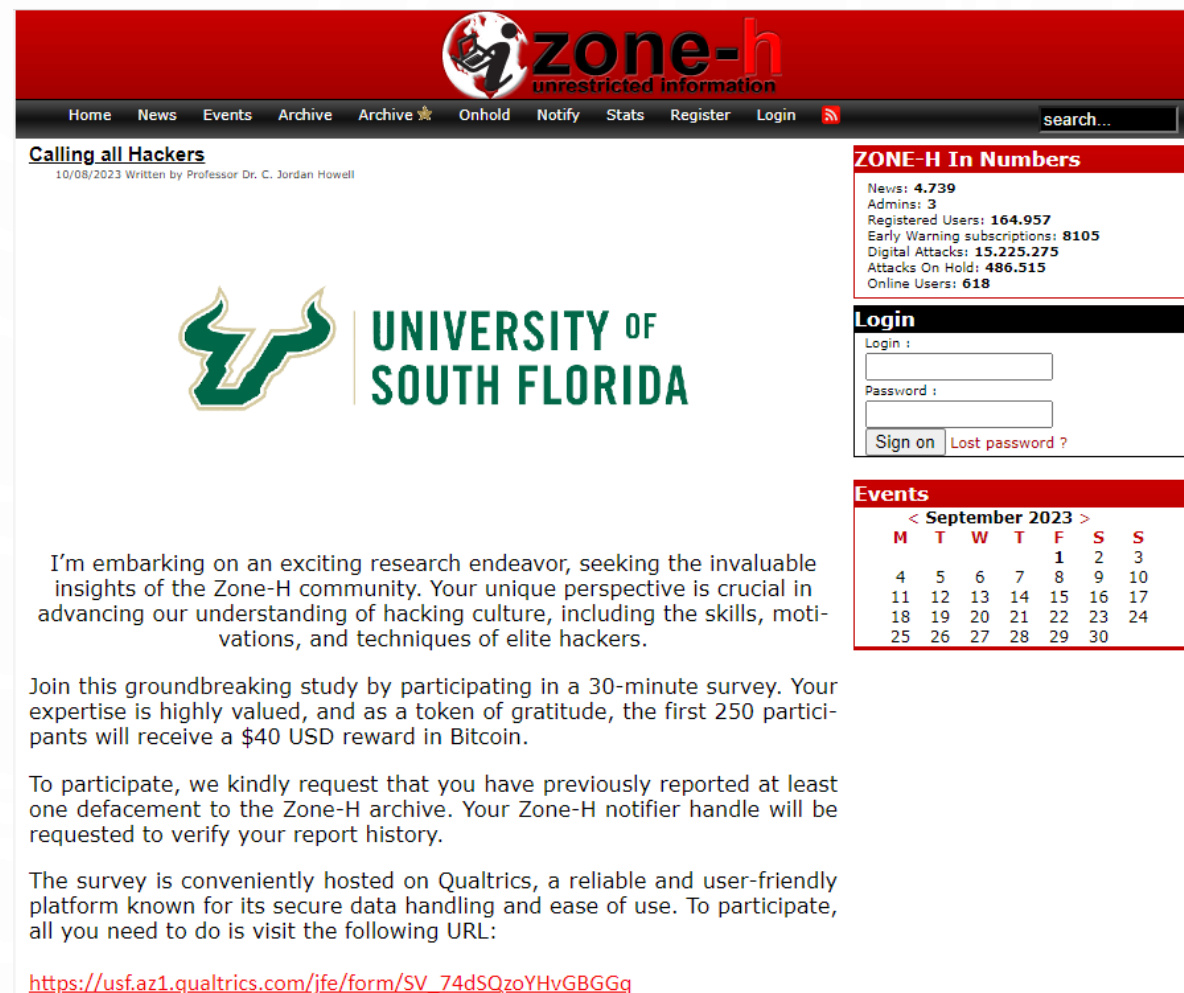
MAPY ATAKÓW (W CZASIE RZECZYWISTYM)

Zone-H to jedna z kilku stron internetowych dokumentujących cyberataki na całym świecie.

Pokazywane są tylko udokumentowane ataki

Dane wyświetlane na takich stronach jak Zone-H obejmują liczbę ataków w danym momencie

<https://www.zone-h.org/>



The screenshot shows the Zone-H website interface. At the top is a red header with the 'zone-h' logo and the tagline 'unrestricted information'. Below the header is a navigation bar with links: Home, News, Events, Archive, Archive (with a star icon), Onhold, Notify, Stats, Register, Login, and a search bar. The main content area features a large green logo of the University of South Florida and a text announcement from Professor Dr. C. Jordan Howell dated 10/08/2023. The announcement describes a research endeavor to study hacking culture and offers a \$40 USD reward in Bitcoin for participants. It also includes a survey URL. On the right side, there is a 'ZONE-H In Numbers' section with statistics: News: 4,739, Admins: 3, Registered Users: 164,957, Early Warning subscriptions: 8105, Digital Attacks: 15,225,275, Attacks On Hold: 486,515, and Online Users: 618. Below this is a 'Login' section with fields for 'Login :' and 'Password :', and buttons for 'Sign on' and 'Lost password ?'. At the bottom right, there is an 'Events' section with a calendar for September 2023.

zone-h
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login search...

Calling all Hackers
10/08/2023 Written by Professor Dr. C. Jordan Howell

UNIVERSITY OF SOUTH FLORIDA

I'm embarking on an exciting research endeavor, seeking the invaluable insights of the Zone-H community. Your unique perspective is crucial in advancing our understanding of hacking culture, including the skills, motivations, and techniques of elite hackers.

Join this groundbreaking study by participating in a 30-minute survey. Your expertise is highly valued, and as a token of gratitude, the first 250 participants will receive a \$40 USD reward in Bitcoin.

To participate, we kindly request that you have previously reported at least one defacement to the Zone-H archive. Your Zone-H notifier handle will be requested to verify your report history.

The survey is conveniently hosted on Qualtrics, a reliable and user-friendly platform known for its secure data handling and ease of use. To participate, all you need to do is visit the following URL:

https://usf.az1.qualtrics.com/jfe/form/SV_74dSQzoYHvGBGGq

ZONE-H In Numbers

News: **4,739**
Admins: **3**
Registered Users: **164,957**
Early Warning subscriptions: **8105**
Digital Attacks: **15,225,275**
Attacks On Hold: **486,515**
Online Users: **618**

Login

Login :

Password :

Events

< September 2023 >

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

ĆWICZENIE

Dla każdej wymienionej poniżej technologii lub określenia wybierz odpowiednie terminy CIA: poufność, integralność i/lub dostępność.

- Naruszenie danych
- Uwierzytelnianie dwuskładnikowe
- Bezpieczeństwo cybernetyczne
- DoS/DDoS
- Uprawnienia do plików

Uwaga: technologia lub określenie może odpowiadać więcej niż jednemu elementowi CIA.

ROZWÓJ TECHNOLOGII CYBERBEZPIECZEŃSTWA

RODZAJE ZŁOŚLIWEGO OPROGRAMOWANIA - „MALWARE”



Virus



Worm



Trojan Horse



Spyware



Ransomware

WIRUS VS ROBAK

WIRUS

Cel ataku:

Modyfikuje lub uszkadza system komputerowy

Sposób replikacji:

Pliki wykonywalne

Zależność:

Program hostujący

ROBAK

Cel ataku:

Zużywa zasoby systemu(ów) komputerowego(ych)

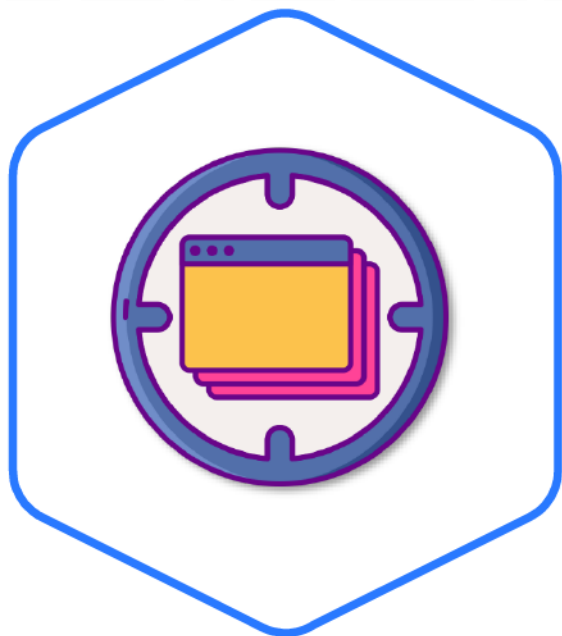
Sposób replikacji:

Słabo zabezpieczone sieci komputerowe

Zależność:

Brak

CYBERATAKI



- Cyberataki nieustannie ewoluują
- Pojedynczy atak może spowodować ogromne szkody
- Zagrożenia realizują wykwalifikowani i zdeterminowani hakerzy
- Przedsiębiorstwa muszą inwestować w środki bezpieczeństwa wysokiego poziomu, aby chronić swoje zasoby cybernetyczne

Środki bezpieczeństwa są wymagane do zapobiegania, wykrywania, reagowania i odzyskiwania.

NIEKTÓRE RODZAJE CYBERATAKÓW



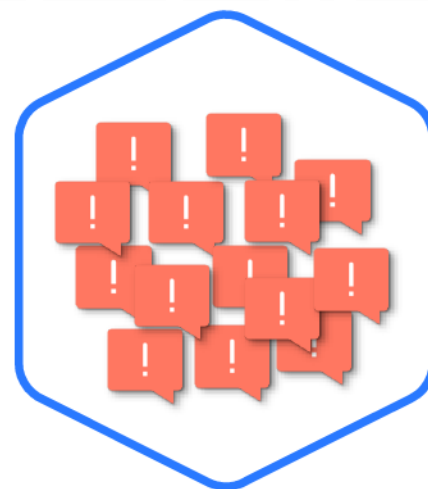
Social
Engineering



Malware



DoS



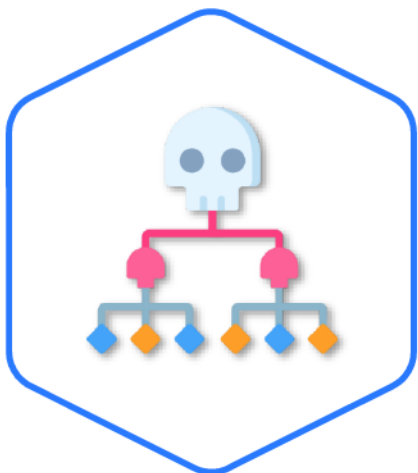
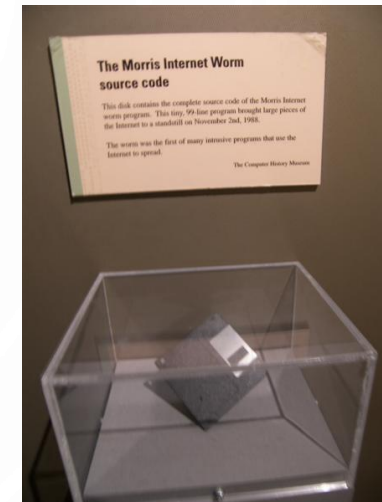
DDoS

„HISTORYCZNE” ZŁOŚLIWE OPROGRAMOWANIE



The Morris Worm

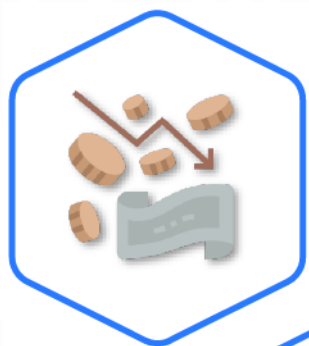
Pierwszy robak komputerowy.
Spowodował ogromne uszkodzenia
komputerów i sieci



Elk cloner

Jeden z pierwszych wirusów.
Rozprzestrzenia się na komputery osobiste
za pośrednictwem dyskietki

„SŁYNNNE” CYBERATAKI



2000: Cyberatak na Yahoo!, Amazon, eBay i CNN spowodował szkody gospodarcze o wartości 1,2 miliarda dolarów



2007: Estońska cyberwojna wycelowała w rządowe i finansowe strony internetowe



2010: Stuxnet obrał za cel irański program nuklearny i spowodował jego niepowodzenie operacyjne

ĆWICZENIE

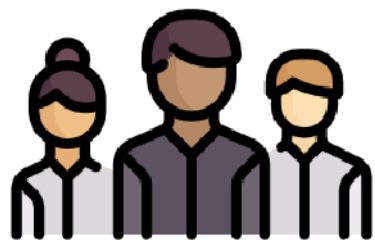
- Przeanalizuj jeden z dobrze znanych ataków i omów z innymi osobami w sali.
- Wyjaśnij co było jego przyczyną.

<https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks>



TECHNIKI OBRONY CYBERNETYCZNEJ

ŚWIADOMOŚĆ ZAGROŻEŃ



Wykłady i szkolenia

Treści wizualne (na ścianie, ekranie komputera itp.)

Okresowe kontrole

Czynnik ludzki jest zazwyczaj „najłabszym ogniwem” cyberbezpieczeństwa w przedsiębiorstwie ze względu na brak świadomości zagrożeń w cyberprzestrzeni

ŚWIADOMOŚĆ ZAGROŻEŃ



security awareness



Security Awareness Episode 1: Passwords

<https://www.youtube.com/watch?v=0Wd3JoUHXno&list=PL7QHbjPSF0r6qJonaROlxVaMLzwDnZyOL>

ŚWIADOMOŚĆ ZAGROZEŃ

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

ŚWIADOMOŚĆ ZAGROZEŃ



Using ChatGPT hardware to brute force your password in 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	instantly	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	instantly	instantly
7	instantly	instantly	instantly	instantly	instantly
8	instantly	instantly	instantly	instantly	1 sec
9	instantly	instantly	4 secs	21 secs	1 min
10	instantly	instantly	4 mins	22 mins	1 hour
11	instantly	6 secs	3 hours	22 hours	4 days
12	instantly	2 mins	7 days	2 months	8 months
13	instantly	1 hour	12 months	10 years	47 years
14	instantly	1 day	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Source: hivesystems.io



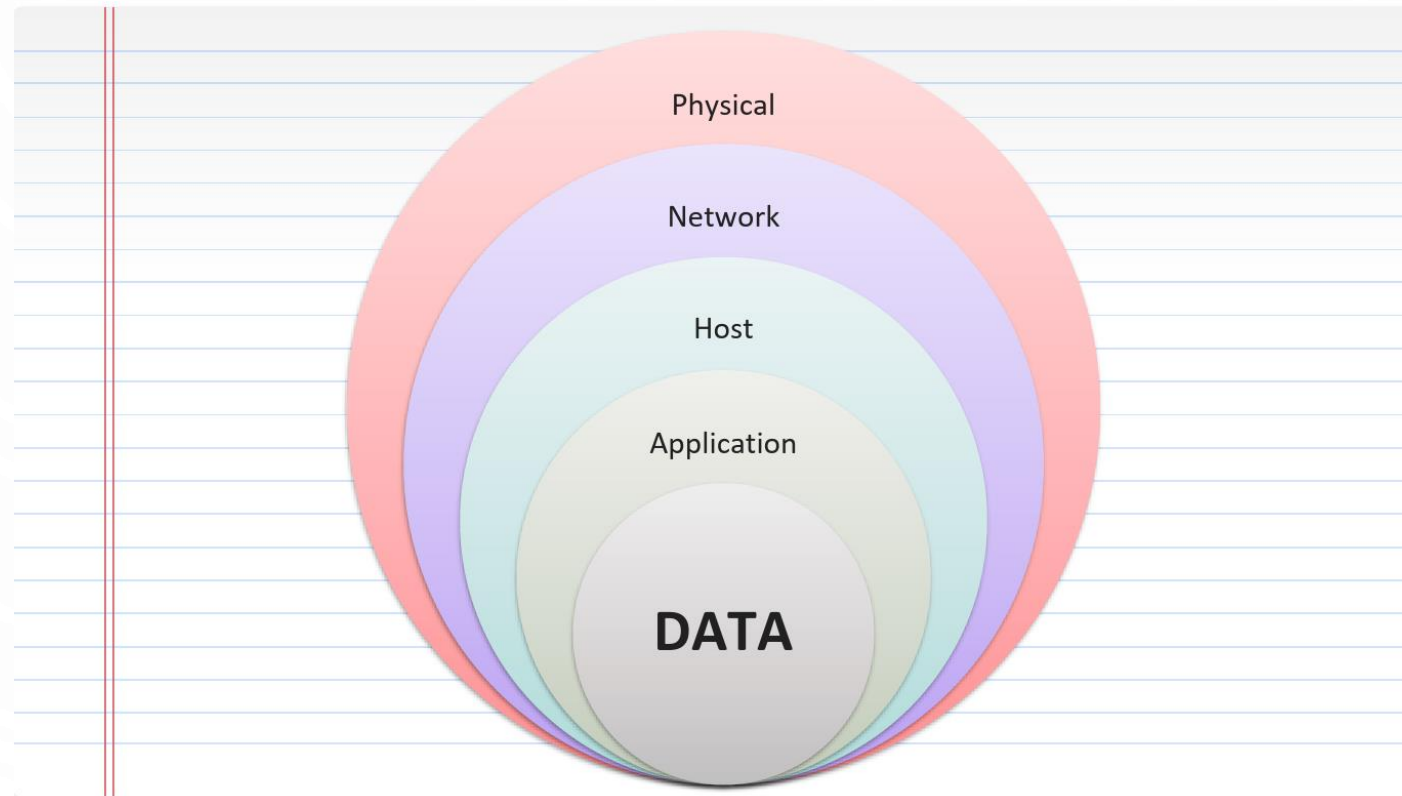
<https://www.hivesystems.io/password>

DEFENSE IN DEPTH (DID)

DiD odnosi się do wielowarstwowej struktury bezpieczeństwa.

W strukturze wielowarstwowej różne zabezpieczenia są rozproszone pomiędzy systemami informatycznymi.

DiD zapewnia kompleksowe zabezpieczenie przed różnorodnymi atakami.



KONTROLA DID

Fizyczna

Ogrodzenie

Drzwi

CCTV

Techniczna

Firewall

Uwierzytelnianie

Ochrona przed włamaniami

Administracyjna

Procedury

Świadomość zagrożeń

Przeglądy dzienników dostępu

KOSZTY ATAKU CYBERNETYCZNEGO



Niski koszt ataku

Niektórzy napastnicy próbują przeprowadzić jak najwięcej ataków, wykorzystując jak najmniej pieniędzy, wysiłku i zasobów. Niższe koszty oznaczają **więcej** ataków.



Wysoki koszt ataku

Ataki wymagające więcej pieniędzy, wysiłku i zasobów oznaczają **mniej** ataków

Dobrze chronione przedsiębiorstwa rzadziej są celem ataków niż organizacje z mniejszą ochroną

The background is a blue gradient with decorative white circuit-like lines in the corners. These lines consist of straight segments and small circles, resembling a stylized electronic circuit board.

TYPY HAKERÓW

KLASYFIKACJA HAKERÓW (1)



Etyczni hakerzy
Eksperci, którzy wykorzystują swoje umiejętności
do celów etycznych i zgodnych z prawem



„Szare Kapelusze”
Czasem działają legalnie, czasem nielegalnie



Nieetyczni hakerzy
Działają dla korzyści osobistych, takich jak pieniądze
lub czynienie innym szkody; nielegalnie, bez zezwolenia

KLASYFIKACJA HAKERÓW (2)



Hakerzy sponsorowani przez państwo/naród

Zatrudnieni przez rząd krajowy lub stanowy



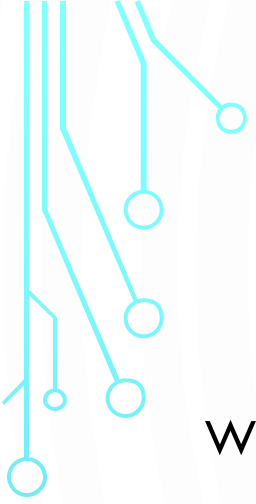
Haktywiści

Zwykle działają w celach politycznych lub społecznych;
często przeciwko rządowi lub korporacjom



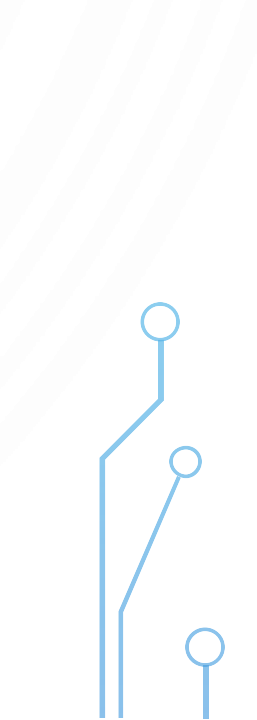
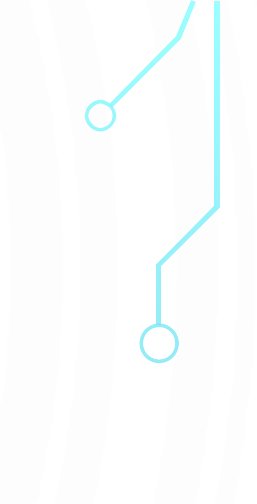
Przestępczość zorganizowana

Osoby tworzące zorganizowane sieci cyberprzestępcze
w celu zwiększania umiejętności technicznych umożliwiających
im przeprowadzanie wyrafinowanych cyberataków



ĆWICZENIE

Wyszukaj w Internecie nazwy grup hakerskich. Rozpoznaj ich logo.



PRACA DOMOWA

Zagraj w grę Najśłabsze ogniwo (do końca), aby zrozumieć ryzyka organizacyjne i działania, które ludzie powinni podjąć, aby im zapobiec.

Kliknij poniższy link, aby rozpocząć grę:

<https://www.isdecisions.com/user-security-awareness-game/>

Graj w grę od pierwszego dnia do końca. Niezależnie od tego, czy dany krok zakończy się sukcesem czy porażką, przeczytaj opis, aby dowiedzieć się więcej na ten temat.

Czy teraz, po zajęciach, lepiej rozumiesz omawiane ryzyka?

IS Decisions

PRODUCTS SUPPORT INSIGHTS COMPANY CONTACT

THE WEAKEST LINK

When the risk is between the chair and the keyboard...

Any organisation is only as secure as you - its users.

Your actions act as an important line of defence
in protecting an organization from security breaches.

But your actions would never risk your employer's security, right?

PROVE IT

PLAY THE GAME

The background is a deep blue gradient with numerous out-of-focus light circles (bokeh) in various shades of blue and teal. On the left side, there are white line art patterns resembling electronic circuit boards or data paths, with small circles at the junctions.

DZIĘKUJĘ ZA UWAGĘ!

MACIEJ.RYBCZYNSKI@UJK.EDU.PL