TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I SZTUCZNEJ INTELIGENCJI

Część I
Wprowadzenie

Wydawnictwo: poswojsku.pl sp. z o.o. *Dariusz Gołębiowski*

NOTA WYDAWCY

OD AUTORA:

Pamiętaj proszę: uszanuj zaangażowanie oraz godziny pracy, które spędziłem nad napisaniem oraz opracowaniem książki: Twoje bezpieczeństwo w świecie cyber i sztucznej inteligencji – używaj poradnik tylko wtedy, gdy go legalnie nabyłeś/aś.

Wydawnictwo poswojsku.pl:

1. dołożyło wszelkich starań, by zawarte w tej książce informacje były kompletne, poprawne oraz rzetelne,
2. nie ponosi żadnej odpowiedzialności za ewentualne szkody, które mogą wyniknąć z wykorzystania informacji zawartych w tej książce.

Wydawnictwo poswojsku.pl – kontakt:

Strona firmowa: www.poswojsku.pl

e-mail: marketing@poswojsku.pl

ul. Paprocka 86, 98–220 Zduńska Wola

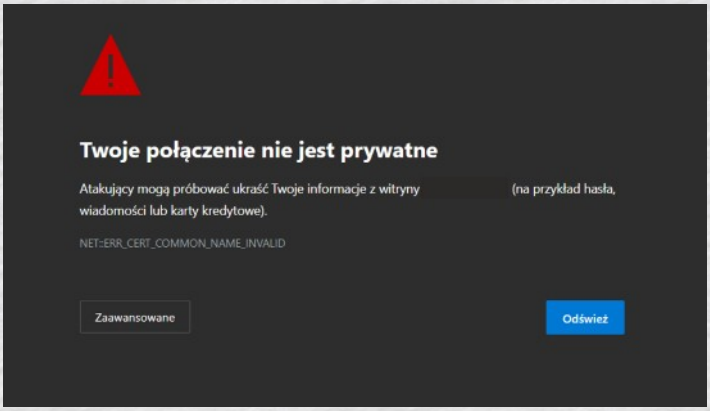
ISBN: 978-83-964647-5-0

Autor: Gołębiowski Dariusz

Zaczytaj się z poswojsku.pl – zobacz nasze propozycje wydawnicze:

TWOJE BEZPIECZEŃSTWO W ŚWIECIE CYBER I SZTUCZNEJ INTELIGENCJI

CZĘŚĆ I WPROWADZENIE



Autor: Dariusz Gołębiowski

GDDM Smart Programming

98-220 Zduńska Wola, ul. Paprocka 86, www.gddm.com.pl,
biuro@gddm.com.pl

OD AUTORA

Cyberbezpieczeństwo oraz ***Sztuczna Inteligencja***, już od wielu miesięcy stają się kluczowymi elementami naszego życia. Zarówno osobistego, jak i zawodowego. W świecie bardzo nasyconym elektroniką oraz wirtualizacją - jesteśmy coraz bardziej narażeni na zagrożenia cybernetyczne. O tego typu zagrożeniach opowiadam na szkoleniach, które prowadzę dla: rodziców, dzieci, nauczycieli, ale także pracowników różnego rodzaju szkół i urzędów. Temat jest tak ważny, że zdecydowałem się na napisanie i wydanie tego poradnika. Został on napisany z myślą o rodzinach z dziećmi, nauczycielach, urzędnikach, pracownikach biurowych. Chcę, żeby mój przekaz dotarł do jak największej liczby osób pracujących przy komputerze i/lub korzystających z tzw. cyberprzestrzeni czyli internetu w każdej jego postaci. Podstawowym celem tego opracowania jest - przedstawienie w sposób przystępny i łatwy do zrozumienia - podstawowych zagadnień cyberbezpieczeństwa oraz związanej z nim sztucznej inteligencji.

Pragnę, aby dla wszystkich osób używających komputera oraz internetu ten poradnik był:

- przestrogą przed cyberzagrożeniami,
- zachętą do stosowania zasad tzw. cyberghigieny.

W pierwszej części tej książki omówię podstawowe pojęcia oraz definicje związane z cyberbezpieczeństwem. Następnie wspólnie przyjrzymy się najczęstszym cyberzagrożeniom, takim jak ataki socjotechniczne, ataki techniczne oraz ataki na tzw. infrastrukturę IT (domową oraz firmową). W dalszej części, przedstawię sposoby ochrony przed niektórymi cyberzagrożeniami, zarówno w życiu osobistym, jak i zawodowym. Będzie także sporo informacji na temat AI oraz narzędzi jakie hakerzy wykorzystują w etycznych i nieetycznych atakach.

Ten poradnik, jest ważny dla wszystkich rodzin, szczególnie - tych z dziećmi, ponieważ dzieci są najbardziej narażone i najmniej odporne na różnorodne zagrożenia cybernetyczne. Tymczasem wśród ich opiekunów, odnośnie zagrożeń w sieci, przeważają bardzo często nonszalancja połączona z głębokim poziomem niewiedzy. W części poświęconej cyberbezpieczeństwu dzieci wspólnie omówimy bardzo istotne tematy, m.in.:

- Jak uchronić dzieci przed cyberprzemocą?
- Jak chronić dzieci przed zagrożeniami związanymi z mediami społecznościowymi?
- Jak uczyć dzieci bezpiecznego korzystania z Internetu?

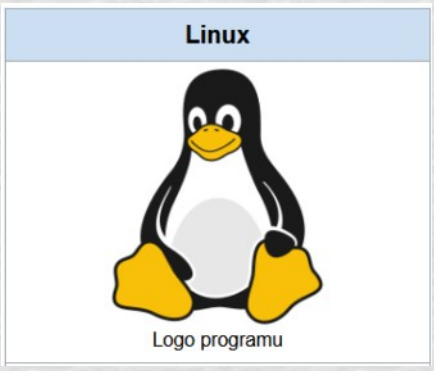
Motto: ZAPOBIEGAJ ZAMIAST LECZYĆ - od rozmowy, poprzez aktywne czynności, do bezpieczeństwa Twojego dziecka

Dla wszystkich pracowników biurowych książka ta jest również istotnym źródłem wiedzy prowadzącym do zachowania cyberbezpieczeństwa. Dlatego zostaną omówione zagadnienia:

- Jak chronić dane osobowe w pracy?
- Jak zapobiegać wyciekom danych?
- Jak wykryć cyberataki i jakiś sposób na nie reagować.

Pokazując system operacyjny Linux, będę chciał, abyś przemyślał/a opcję „przejścia" na jedną z wielu dystrybucji tego wspaniałego i prawdopodobnie najbezpieczniejszego systemu operacyjnego. Wiem, co wielu z Was powie: „Linux jest skomplikowany, trzeba pisać jakieś kody, bo inaczej nie będzie działał". Wybacz, ale obecnie takie stwierdzenie, to zwykła bzdura. Zdecydowana większość dystrybucji, to z punktu widzenia użytkownika nic innego jak kolejny „system okienkowy". Klikasz i używasz, a w promocji otrzymujesz wiele pozytywów, m.in.:

- bezpieczeństwo,
- brak jakichkolwiek opłat za jego zakup czy używanie.



Logo programu

Zdjęcie - źródło - Wikipedia: https://pl.wikipedia.org/wiki/Linux

Podsumowując:

Poradnik jest przeznaczony dla osób, które chcą dowiedzieć się więcej o: świecie cyber, AI, hakerstwie oraz wdrożyć odpowiednie środki bezpieczeństwa w swoim życiu. Mamy nadzieję, że pomoże ona zwiększyć Tobie drogi czytelniku - bezpieczeństwo w cyfrowym świecie - Twoje oraz Twoich bliskich.

Autor poleca

Serdecznie zapraszam do kontaktu. Znajdziesz mnie bez problemu poprzez Wydawnictwo poswojsku.pl, moją stronę www, ale także na popularnych portalach społecznościowych, m.in.: Facebook, LinkedIn, youtube.com/@poswojsku .

Gdybyś szukał/a szkoleń tradycyjnych czy też on-line dla Ciebie i/lub Twojej organizacji z omawianych tutaj tematów - serdecznie zapraszam do skorzystania z moich usług ;): www.gddm.com.pl szkolenia oraz doradztwo - cyberbezpieczeństwo, AI, RODO, programowanie (m.in.: Python, JavaScript, HTML, CSS, SQL).

WPROWADZENIE DO PORADNIKA

do wszystkich rozdziałów - każdej z trzech części

Wkrocz do cyfrowego świata z szeroko otwartymi oczami, a do tego z należytą ostrożnością. W tej książce:

- odkryjesz mroczne zakamarki cyberświata oraz sztucznej inteligencji,
- zdobędziesz wiedzę, która ochroni Cię przed licznymi cyberzagrożeniami.

Cyberbezpieczeństwo (a może raczej - **cyberniebezpieczeństwo?**) **to nieustanny proces.** W dzisiejszych czasach każdy z nas jest narażony na ataki różnego rodzaju hakerów oraz złośliwego oprogramowania. Ten poradnik wyposaży Cię w niezbędne: narzędzia, wiedzę oraz umiejętności, abyś mógł/ogła bezpiecznie poruszać się w cyfrowej rzeczywistości.

Podróż przez ten poradnik ujawni – specjalnie dla Ciebie:

- **Potęgę sztucznej inteligencji w rękach hakerów:** odkryjesz jej niesamowite możliwości oraz, niestety, zagrożenia, jakie niesie dla Twojego cyberbezpieczeństwa.
- **Podstawy prawne cyberbezpieczeństwa:** poznasz podstawowe regulacje chroniące i obowiązujące Ciebie w cyfrowym świecie.
- **Zasady cyberhigieny:** nauczysz się prostych, ale skutecznych sposobów działania, które znacząco zwiększą Twoje bezpieczeństwo w sieci.

- **Najczęstsze cyberzagrożenia:** poznasz phishing, ataki socjotechniczne, malware i inne pułapki cyberświata.
- **Sposoby ochrony przed cyberzagrożeniami:** odkryjesz techniki ochrony danych, kont, urządzeń i dzieci w cyfrowym świecie.
- **Sekrety bezpiecznego korzystania z internetu:** nauczysz się bezpiecznie pobierać pliki, tworzyć tzw. „silne hasła", szyfrować dane i wiele więcej.
- **Popularne narzędzia hakerskie:** od specjalnych dystrybucji Linuxa po aplikacje do łamania kodów. Poznasz ich nazwy oraz podstawy działania.

A gdy już poznasz całość poradnika - wykorzystaj zdobytą wiedzę, aby chronić siebie, swoich bliskich i swoje dane w cyfrowym świecie. Także z wykorzystaniem sztucznej inteligencji. Pamiętaj, że dbając o cyberbezpieczeństwo budujemy bezpieczniejszą przyszłość dla wszystkich ludzi. To nasz wspólna odpowiedzialność.

Uwaga: Ten poradnik jest przeznaczony dla wszystkich użytkowników internetu, niezależnie od poziomu wiedzy technicznej. Znajdziesz tu zarówno podstawowe informacje o cyberbezpieczeństwie, jak i nieco bardziej zaawansowane techniki.

Zapraszam do lektury – zobacz poniżej, co znajdziesz w każdym z rozdziałów poradnika części 1.

Rozdział 1: Fundamenty Wiedzy

Zaczynajmy! Wkraczasz w fascynujący, ale niebezpieczny świat cyberprzestrzeni!

W tym rozdziale zbudujemy solidne fundamenty wiedzy, niezbędne do poruszania się w cyfrowym świecie z rozwagą i bezpieczeństwem. Odkryjesz:

- **Zagrożenia czyhające na Ciebie w sieci:** od złośliwego oprogramowania po cyberataki i manipulacje.
- **Podstawowe pojęcia cyberbezpieczeństwa, m.in.:** szyfrowanie, uwierzytelnianie, ochrona danych osobowych i wiele innych.
- **Potencjalne obszary zagrożenia:** kto może paść ofiarą cyberataku i z jakiego powodu.
- **Pomocną dłoń ekspertów:** kim są specjaliści od cyberbezpieczeństwa i jak mogą Ci pomóc.
- **Sztuczną inteligencję:** czy stanowi ona zagrożenie, czy może nadzieję dla cyberbezpieczeństwa?
- **Podstawy systemów operacyjnych:** Linux, Android i Windows - mocne i słabe strony, ze szczególnym podkreśleniem bezpieczeństwa systemu Linux na bazie opisu dystrybucji Mint.
- **Narzędzia ochrony przed atakami technicznymi:** firewalle, antywirusy i inne narzędzia bezpieczeństwa.
- **Bezpieczeństwo przeglądarek internetowych:** poznasz różnice, świadomie wybierzesz najlepiej chroniącą Twoją prywatność.
- **Mapy ataków cyfrowych:** kolejna wojna światowa? Zobacz jak wygląda współczesna cyberwojna.

Rozdział 2: Narzędzia do Hakowania oraz Podstawy Prawne

Zanurz się w kreatywnym świecie hakerów i odkryj sekrety ich arsenału!

W tym rozdziale poznasz podstawy wiedzy odnośnie:

- **Hakerów i ich motywacje:** kim są? Przestępcami czy może szlachetnymi rycerza świat cyber?
- **Popularne narzędzia hakerskie:** od specjalnych dystrybucji Linuxa po aplikacje do łamania kodów.
- **Sztuczną inteligencję jako potężne narzędzie w rękach hakerów:** jej możliwości oraz zagrożenia z nią związane.
- **Podstawy prawne cyberbezpieczeństwa:** prawo w cyfrowym świecie łatwo jest złamać, poznaj podstawowe regulacje.
- **Dyrektywę NIS 2:** unijne prawo mające na celu zwiększenie odporności systemów informatycznych.
- **Ciekawe adresy świata cyber:** adresy internetowe, których pomogą Tobie w zgłębieniu cyber tajemnic.

W kolejnych częściach mojej książki znajdziesz między innymi poniższe zagadnienia

Cyberhigiena, to klucz do skutecznej ochrony w cyfrowym świecie!

W tym rozdziale odkryjesz prawdy bezpiecznego cyber świata:

- **Jak rozpoznać, że padłeś/aś ofiarą cyberataku -** oznaki infekcji złośliwym oprogramowaniem, phishingu i innych zagrożeń.
- **Najskuteczniejsze elementy profilaktyki cyberbezpieczeństwa:** zachowania, które znacząco zwiększą Twoje bezpieczeństwo.
- **Metody nieautoryzowanego pozyskiwania danych:** popularne techniki stosowane przez cyberprzestępców.
- **Zasady bezpiecznego przetwarzania danych:** szyfrowanie, przechowywanie, udostępnianie – ochrona Twojej prywatności.
- **Sztuczna inteligencja a bezpieczeństwo Twoich haseł:** czy za pomocą AI nas zhakują?

Odkryj mroczne zakamarki mentalnego cyberświata, a poznasz jego najczęstsze zagrożenia!

W tym rozdziale dowiesz się o zagadnieniach:

- **Wpływ psychologii na cyberbezpieczeństwo:** jak ludzkie słabości są wykorzystywane przez cyberprzestępców.
- **Ataki socjotechniczne:** manipulacja, motywacja a oszustwo - narzędzia cyberataków.

- **Phishing i jego odmiany:** jak rozpoznać i skutecznie uniknąć cyfrowych zagrożeń.
- **Wpływ sztucznej inteligencji na phishing:** AI pomaga w udoskonalaniu technik phishingu.
- **Logowanie w otwartych sieciach Wi-Fi:** cyberprzestępcy podsłuchują i przejmują Twoje dane.
- **Złośliwe oprogramowanie:** rodzaje, nazewnictwo i opis przykładowych zagrożeń.

Wyposaż się w świetlistą cyber zbroję i podążaj w stronę bezpieczeństwa!

W tym rozdziale odkryjesz:

- **Strategie ochrony przed atakami socjotechnicznymi:** jak rozpoznać manipulację oraz unikać oszustwa.
- **Wyzwania ochrony pracy zdalnej:** bezpieczeństwo danych oraz systemów w domowym biurze.
- **Fundamentalne zasady higieny cyfrowej:** nawyki chroniące przed cyberzagrożeniami.
- **Bezpieczne użytkowanie sprzętu IT w podróży:** ochrona danych przed kradzieżą oraz włamaniem.
- **Zasady bezpiecznego korzystania z mediów społecznościowych:** ochrona prywatności i danych osobowych.

- **Ochrona przed zagrożeniami w mediach:** fake newsy, phishing, malware i inne pułapki.
- **Bezpieczne logowanie:** silne hasła, uwierzytelnianie dwuskładnikowe oraz inne zabezpieczenia.
- **Bezpieczne korzystanie ze smartfonów:** czy jest możliwe? Ochrona aplikacji, danych oraz prywatności.
- **Bezpieczeństwo urządzeń IoT:** jak chronić inteligentne urządzenia przed atakami.

Spójrz na wirtualny świat dzieci i poznaj sposoby ochrony Twoich bliskich przed cyberzagrożeniami!

W tym rozdziale odkryjesz:

- **Rodzaje cyberzagrożeń, z którymi mogą spotkać się Twoje dzieci w codziennym życiu:** cyberprzemoc, złośliwa zawartość, kontakt z nieodpowiednimi treściami, uzależnienie od gier oraz internetu, itp.
- **Jak rozpoznać, że dziecko jest ofiarą cyberprzemocy:** oznaki, których nie możesz przegapić.
- **Skuteczne sposoby dbania o bezpieczeństwo Twojego dziecka w cyfrowym świecie:** rozmowa, edukacja, właściwe wzorce, itp.
- **Funkcje kontroli rodzicielskiej w różnych systemach operacyjnych:** Windows, Android, iOS i inne.
- **Zagrożenia egzystencjonalne związane ze sztuczną inteligencją:** wpływ AI na rozwój i bezpieczeństwo dzieci.

Stań się magiem cyberbezpieczeństwa - zapanuj nad cyfrowym światem!

W tym rozdziale odkryjesz:

- **Zasady bezpiecznego pobierania zdjęć, tekstów oraz innych zasobów z internetu:** jak uniknąć złośliwego oprogramowania.
- **Zasady działania, gdy zostałeś zhakowany/a, ktoś przejął Twoje konto:** odzyskiwanie dostępu, zabezpieczanie danych, zgłaszanie zdarzenia.
- **Magię tworzenia i przechowywania bezpiecznych haseł:** jak uchronić się przed włamaniem i kradzieżą danych bez konieczności pamiętania wielu haseł.
- **Bezpłatne metody szyfrowania:** ochrona dysków, zewnętrznych nośników danych, folderów i plików przed nieuprawnionym dostępem.
- **Sposoby weryfikacji poprawności ściąganych plików:** unikanie złośliwego oprogramowania, weryfikacja za pomocą wartości skrótu a sumy kontrolnej.

SPIS TREŚCI Części 1

w kolejnych częściach poradnika znajdziesz:

CZĘŚĆ II CYBERHIGIENA
Nota Wydawcy
Od autora
Wprowadzenie do poradnika
SPIS TREŚCI
Rozdział CYBERBEZPIECZEŃSTWO W PRAKTYCE - PODSTAWOWE ZASADY CYBERHIGIENY
Jak rozpoznać, że jesteś ofiarą Cyberataku
Profilaktyka cyberbezpieczeństwa
Metody nieautoryzowanego pozyskania danych - przykłady
Bezpiecznie przetwarzanie danych: szyfrowanie, przechowywanie, udostępnianie, komunikacja
Czy AI złamie wszystkie nasze hasła?
Rozdział NAJCZĘSTSZE CYBERZAGROŻENIA
Kwestie personalno-mentalnościowe ludzi
Ataki socjotechniczne – charakterystyka
Phishing i jego odmiany
AI – wirtuoz phishingu „czytający nasze zachowania”
Fałszywe strony internetowe
Logowanie w otwartych sieciach
Złośliwe oprogramowanie - rodzaje, nazewnictwo, opis przykładowych zagrożeń
Rozdział SPOSOBY OCHRONY PRZED CYBERZAGROŻENIAMI
Ataki socjotechniczne - zasady ochrony
Ataki techniczne – penetracja sieci – zasady ochrony

Rozdział 1

FUNDAMENTY WIEDZY

Zagrożenia:

cyberbezpieczeństwo a cyberniebezpieczeństwo

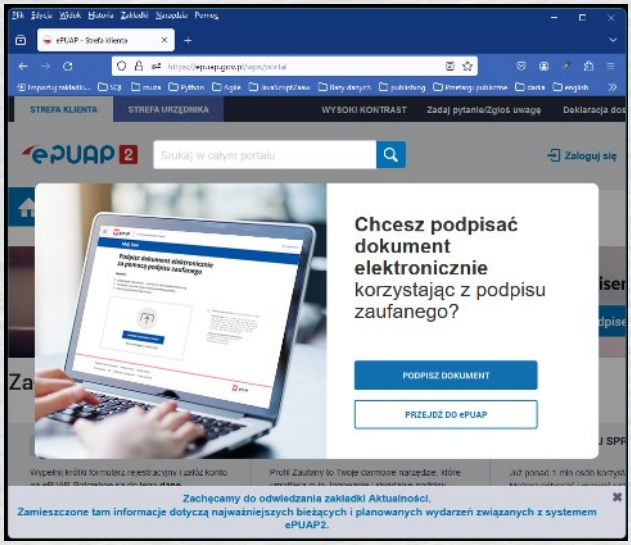
Od co najmniej kilkunastu lat większość społeczeństw żyje w dwóch światach:

- rzeczywistym,

  oraz

- cyfrowym.

Tendencją z roku na rok coraz bardziej zauważalną jest, że świat cyfrowy wypiera ten rzeczywisty. Coraz więcej codziennych czynności wykonujemy z wykorzystaniem lub nawet wewnątrz świata cyfrowego. Cyfrowe dokumenty potwierdzające nasze istnienie już teraz w dużej części znajdują się w zasobach cyfrowych w postaci choćby tzw. mObywatela. Mamy do niego dostęp w każdej dowolnej chwili, wystarczy użyć naszego smartfona i kliknąć odpowiednią aplikację. To oczywiście ma swoje zalety, jak chociażby nigdy wcześniej nie spotykaną w historii ludzkości, wygodę korzystania z dobrodziejstw cyfrowych zasobów bez wychodzenia z własnego domu czy nawet łóżka. Jest to proste, łatwe i przyjemne, może nawet zbyt bardzo.



Zdjęcie – źródło: strona https://epuap.gov.pl/wps/portal

Ale poza niewątpliwymi korzyściami, pojawiają się także zagrożenia dla naszego bytu, które również nigdy wcześniej nie miały miejsca w znanej nam historii ludzkości. Szczególnie, że w świecie cyfrowym i tym rzeczywistym, zaczyna odgrywać znaczącą rolę jeszcze jeden nowy czynnik: sztuczna inteligencja (AI - ang. artificial intelligence). Zagrożenia świata cyfrowego określane są często nazwą: ***Cyberbezpieczeństwo***. Jest to zagadnienie, które otacza nas już całkiem i to dookoła. Choć tak właściwie, to może lepszym byłoby stwierdzenie: ***Cyberniebezpieczeństwo***? Może to tylko niewielka różnica językowa, ale cyberbezpieczeństwo brzmi niegroźnie, zapewne właśnie dlatego nie wszyscy traktują to zagadnienie na poważnie. Więc może powinniśmy określać je mianem cyberniebezpieczeństwa? Czy wówczas wydźwięk tego słowa byłby mocniejszym ostrzeżeniem i to dla większej liczby ludzi?

W zamierzchłych czasach nasi przodkowie oraz praprzodkowie, potencjalne cyberniebezpieczeństwa znali, co najwyżej z tzw. literatury science-fiction lub baśni, bajek czy opowiadań ludowych. A tymczasem obecnie - świat cyfrowy, wykorzystywany przez nas samych w sposób nieodpowiedzialny czy nieświadomy, może spowodować mnóstwo kłopotów dla naszego istnienia i funkcjonowania w społeczeństwie oraz na Ziemi. Niestety – poziom niewiedzy w zakresie zagrożeń jest ogromny i ciągle zbyt mało rozumiany. Właśnie dlatego codziennie słyszymy o udanych atakach hakerskich na różnego rodzaju instytucje, urzędy oraz firmy. Zauważ, że niestety bardzo rzadko zdarzają się informacje o zhakowaniu osób fizycznych. Dlaczego? Bo z punktu widzenia społeczeństwa, pojedyncza jednostka ludzka ma niewielkie znaczenie. A wierz mi, codziennie miliony tysiące ludzi są narażone na działalność przestępczą w cyfrowym świecie. Wielu z nich jest poszkodowanych psychicznie i fizycznie, w wyniku utraty m.in.:

- zasobów finansowych,
- danych osobowych - przejęcie tożsamości cyfrowej,
- uszkodzenia fizycznego posiadanego majątku,
- prywatnych zasobów typu: zdjęcia, maile, filmy, dane teleadresowe,
- dostępów do mediów społecznościowych,
- itp.

Zagrożenia w świecie cyfrowym

Świat cyber - wirtualny - podobnie jak świat rzeczywisty, przynosi swoim użytkownikom (internautom) bardzo poważne zagrożenia. Wspominałem o obszarach, w których możemy stracić pieniądze, wizerunek, zdrowie czy nawet w skrajnym przypadku - życie.

Poniższe zdjęcie to wspólna praca Autora książki oraz generatora AI – źródło: https://chatgpt.openai.org.

Źródła zagrożeń mogą być bardzo różne, dla przykładu:

- powszechny dostęp do sieci internet,
- brak wiedzy i świadomości użytkowników świata cyfrowego,
- używanie sprzętu IT (smartfony, laptopy, tablety, itp.) oraz dostępnych aplikacji,
- posiadanie urządzeń elektronicznych (np. IoT- Internet of Things, czyli Internet rzeczy - więcej na ten temat znajdziesz w dalszej części tej książki).

Grafika: multimedia LibreOffice

Aby było łatwiej zrozumieć zagrożenia świata cyfrowego, poznajmy kilka podstawowych pojęć. Są one nieodzownie z nim związane i wpływają na naszą codzienność, tworząc dla nas z jednej strony możliwości rozwoju, a z drugiej stanowią bardzo duże niebezpieczeństwo.

Cyberbezpieczeństwo - podstawowe pojęcia

Cyberprzestrzeń (źródło: pl.wikipedia.org/wiki/Cyberprzestrze%C5%84) jest to iluzja świata rzeczywistego - stworzona za pomocą metod teleinformatycznych. Podzielona jest ona na tzw. „obszary wpływów", które dość znacząco różnią się od siebie. Nasza – europejska, charakteryzuje się względnym bezpieczeństwem, osiągniętym m.in. poprzez wprowadzenie tzw. RODO. Niestety, w pozostałych częściach cyberprzestrzeni nie obowiązują unijne przepisy. A że internet działa jako całość, więc zagrożenia z pozostałych obszarów sieci www, silnie przenikają do części europejskiej.

Najważniejsze obszary wpływów to (po myślnikach – agencje normujące stan danej części internetu).

- Europejski - ENISA

  zdjęcie - źródło www.enisa.europa.eu/ - European Union Agency for Cybersecurity, jak już wspominałem, to byłaby całkiem bezpieczna część internetu, gdyby nie cała jego reszta.

- Amerykański - www.cisa.gov/ - Cybersecurity & Infrastructure Security Agency, zdjęcie- źródło: https://www.cisa.gov/.

Dla firm z USA dane osobowe, to nic innego jak towar handlowy, na którym można nieźle zarobić. Oznacza to, że z naszego punktu widzenia wcale nie jest tutaj bezpiecznie. Niestety nie da się być w internecie i nie korzystać z jego amerykańskiej części. Choćby dlatego, że to Ameryka w dużej mierze zarządza internetem od strony technicznej.

- Chiński www.cac.gov.cn/ - Chińska Administracja Cyberprzestrzeni (CAC - centralna agencja regulująca cenzorem, nadzorem i kontrolą Internetu dla ChRL), totalna inwigilacja, czyli kontrolowanie, podsłuchiwanie oraz nagrywanie wszystkiego i wszystkich – tak najkrócej można by określić strategie chińskiego internetu,

- Rosyjski www.government.ru/en/department/113 - federal security service www.fsb.ru. Ta część internetu zawsze była niebezpieczna, jak tylko sięgam pamięcią. A po wybuchu wojny w Ukrainie, pojawiło się w niej jeszcze więcej zagrożeń. Dlatego zdecydowanie trzeba omijać internet oraz wszelkie oprogramowanie, które są lub nawet tylko – mogą być powiązane w jakikolwiek sposób z Rosją. Zatem dając dobry przykład nie byłem na ich stronach i wybacz, ale nie umieszczę ilustracji związanej z fsb.ru. Podkreślam, nie jest to opinia rusofoba, tylko realna ocena potencjalnych zagrożeń.
- Darknet - zbiorcza nazwa anonimowej i w dużej mierze nielegalnej części internetu, którą stanowią różnorodne anonimowe strony internetowe, sklepy, fora dyskusyjne, itp.

  Strony i/lub osoby działające w darknecie, bardzo często związane są z różnego rodzaju działalnością przestępczą.

  Ale darknet to także ostoja wolności słowa, ciekawych dyskusji, a przynajmniej tak było na początku jego istnienia.

  Natomiast dla zwykłego użytkownika internetu mam radę – nie odwiedzaj darknetu, nie ma sensu. Zagrożeń, które tam są i które możesz przez przypadek „załapać” na swój komputer – jest bardzo dużo. Nie warto ryzykować bezpieczeństwa Twojego, rodziny czy organizacji – z powodu zwykłej ciekawości.

Zdjęcie: Darknet – wizualizacja AI

W tym miejscu pragnę poruszyć po raz pierwszy w tym poradniku temat dzieci w darknecie. Współpracując z różnymi szkołami, prowadząc szkolenia dla dzieci, rodziców czy nauczycieli - bardzo często poruszane było m.in. wyżej wymienione zagadnienie. I niestety okazuje się, że zbyt dużo dzieci było już w darknecie i widziało tam okropne rzeczy.

Myślę, że wiele osób dorosłych nie chciałoby ujrzeć tego, co zobaczyli małoletni użytkownicy darknetu. Jestem głęboko przekonany, że w dużej mierze jest to wina osób dorosłych (rodziców, opiekunów, nauczycieli), które nie rozmawiają lub unikają rozmów z dziećmi na trudne tematy:

- czasami ze względu na brak wiedzy,
- a czasami licząc, że jeżeli o czymś nie powiemy, to dziecko się o tym nie dowie.

Ale przecież w naszych czasach, wiedza jest dostępna na jedno kliknięcie, o czym dorośli często zapominają. Powinniśmy chronić dzieci poprzez:

- rozmowę,
- wytłumaczenie – edukację,
- założenie odpowiednich barier informatycznych – więcej znajdziesz w dalszej części poradnika.

Ten ostatni podpunkt zgodnie z zasadą:

„ufaj, ale kontroluj”

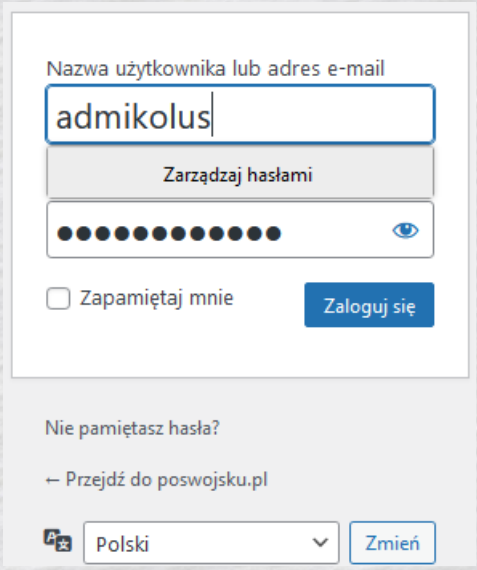
- pozostałe części internetu – są dla nas na dzisiaj mniej istotne, choć faktem jest, że jest ich całkiem sporo (m.in.: indyjski, brazylijski, arabski, itp.).

Znamy już kontekst znaczenie cyberprzestrzeni, ale ze światem wirtualnym wiąże się mnóstwo różnego rodzaju pojęć. Aby dobrze zrozumieć istotę cyberbezpieczeństwa, poznajmy podstawowe nazewnictwo i to, co się pod nim kryje.

- Komputer, czyli między innymi: komputer PC, tablet, laptop, smartfon, telewizor, odkurzacz, ekspres do kawy, opaska na nadgarstek, lodówka, alarm domowy, samochód – a przecież można by wymienić o wiele, wiele więcej.
- Najważniejsze systemy operacyjne: Linux, Windows, Android, iOS, macOS, HarmonyOS, pozostałe.
- Szyfrowanie - zamienianie naszych czytelnych danych do formy, która będzie nieczytelna dla osób z zewnątrz. Zwykle do odczytania potrzeba specjalnego klucza. Może być nim hasło albo tzw. zabezpieczenie sprzętowe.
- Kodowanie (wykorzystywane np. przez programistów czy matematyków) - przedstawienie zasobów (np. danych) w formie wygodnej do pracy dla ludzi i/lub komputerów. Nie jest związane z bezpieczeństwem danych, ale bardzo ułatwia interpretację informacji przez odbiorców.
- Uwierzytelnianie – prowadzi do zapewnienia, że tylko odpowiednie osoby, usługi i aplikacje z odpowiednimi uprawnieniami mogą uzyskiwać dostęp do określonych zasobów.

Składa się z trzech etapów:

- Identyfikacja: określenie tożsamości zazwyczaj za pomocą nazwy użytkownika - loginu.
- Uwierzytelnianie: wprowadzenie hasła, celem udowodnienia prawa dostępu do zasobów.
- Autoryzacja: dany system sprawdza, czy użytkownik (tutaj ‘admikolus’) o określonym loginie i haśle ma uprawnienia do zasobów.



- Backup - kopia danych: dysk, urządzenie zewnętrzne – przenośne, chmura IT.

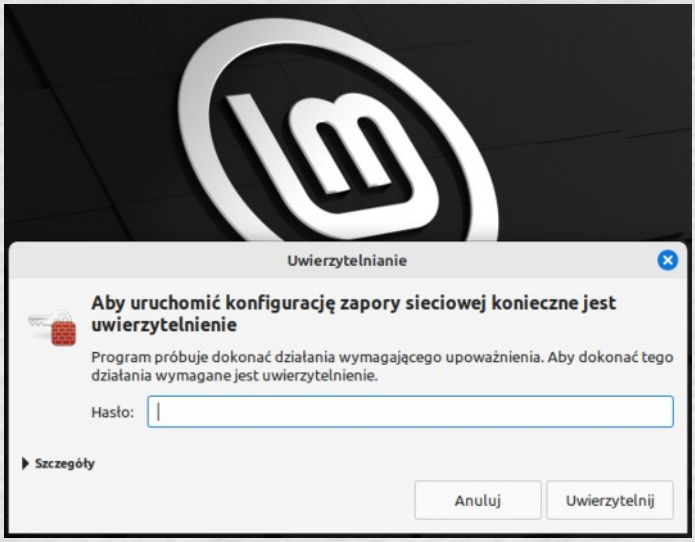
- Chmura IT - usługa udostępniania zasobów IT, miejsce przechowywania danych oraz aplikacji.
- KSC - Krajowy System Cyberbezpieczeństwa – o tym warto choć w zarysie wiedzieć – więcej znajdziesz na (zdjęcie – źródło gov.pl):
  - www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa- .

- Dane- istotne, wrażliwe informacje o osobie fizycznej. Więcej możesz znaleźć na stronach związanych z tzw. RODO: uodo.gov.pl/p/prezes-i-urzad , uodo.gov.pl/pl/p/poradniki , edps.europa.eu/_en - Europejski Inspektor Danych Osobowych (EIOD).
  - Cyberbezpieczeństwo i RODO są wzajemnie powiązane (np. adres IP, "ciasteczka" - traktowane są jako dana osobowa).

- Exploit - sposób wykorzystania podatności systemu, program wykorzystujący istniejące błędy w oprogramowaniu- źródło: pl.wikipedia.org/wiki/Exploit .
- Rootkit (ang. root "korzeń, rdzeń") – narzędzie pomocne we włamaniach do systemów IT - ukrywa niebezpieczne pliki oraz procesy, które umożliwiają utrzymanie kontroli nad systemem – źródło: pl.wikipedia.org/wiki/Rootkit .

Zdjęcie: Linux Mint

zmiany w zaporze sieciowej wymagają uwierzytelnienia



- Firewall – „ściana ogniowa”, zapora sieciowa - bariera pomiędzy siecią wewnętrzną a zewnętrzną (internetem) – nigdy jej nie wyłączaj w Twoim systemie operacyjnym.

Zdjęcie – wizualizacja AI: Firewall – „ściana ogniowa”. Przed tego typu zaporą zainstalowaną w Twoim komputerze jest cały internet. Za nią jest chroniony Twój komputer oraz Twoje zasoby.

Dziękuję za lekturę próbki mojej książki i zapraszam do pełnej wersji poradnika
a w przyszłości także do kolejnych jego części:
Części II CYBERHIGIENA
Części III DZIECKO I TY

Dariusz Gołębiowski - Autor

DZIĘKUJĘ ZA UWAGĘ :)

zapraszam do kolejnych części

AUTOR:

DARIUSZ GOŁĘBIOWSKI

GDDM Smart Programming

www.gddm.com.pl

Wydawnictwo: poswojsku.pl sp. z o.o.