Wydawnictwo Cyfrowe poswojsku.pl

Gołębiowski Dariusz

CHROŃ i ROZWIJAJ BIZNES - CYBER AI

Część 1

WYKORZYSTANIE AI W BEZPIECZEŃSTWIE ORGANIZACJI

Pamiętaj proszę:
napracowałem się, uszanuj moje zaangażowanie i godziny pracy spędzone nad napisaniem i opracowaniem powieści książki pt. CHROŃ I ROZWIJAJ BIZNES – CYBER AI Część 1 Wykorzystanie AI w bezpieczeństwie organizacji.

Autorzy oraz Wydawnictwo poswojsku.pl

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

Wydawnictwo poswojsku.pl – kontakt:
www.poswojsku.pl, bok@poswojsku.pl
ul. Paprocka 86, 98-220 Zduńska Wola
ISBN: 978-83-972080-9-4

SPIS TREŚCI

WPROWADZENIE **strona 5**

ROZDZIAŁ 1 **strona 9**

CYBER ZAGROŻENIA

I. Co to jest cyber świat

II. Największe cyber zagrożenia dla firm i instytucji

1. Nazewnictwo i opis najczęściej występujących zagrożeń cyfrowych,
2. Najlepsze sposoby obrony przed zagrożeniami cyfrowymi
3. Malware – podstawowi przedstawiciele,
4. Phishing – podstawowe rodzaje.

III. Dyrektywa NIS 2 - podstawy prawne cyberbezpieczeństwa

1. NIS 2 – podstawowe informacje,
2. Wpływ NIS 2 na małe organizacje (firmy, fundacje, itp.),
3. NIS 2 a tzw. Dobre praktyki w zakresie cyberbezpieczeństwa.

IV. Przykłady zagrożeń:

1. Mail,
2. Portal społecznościowy,
3. SMS.

ROZDZIAŁ 2 **strona 92**

SZTUCZNA INTELIGENCJA AI

I. Co to jest sztuczna inteligencja? Definicja i kluczowe pojęcia
   1. Kluczowe pojęcia AI,
   2. AI kontra bezpieczeństwo teleinformatyczne.

II. Wprowadzenie do sztucznej inteligencji w bezpieczeństwie
   1. Definicja sztucznej inteligencji (AI),
   2. Rola AI w bezpieczeństwie,
      2.1 AI w cyberbezpieczeństwie
      2.2 Wykorzystanie AI w systemach nadzoru i ochrony fizycznej
   3. Potencjalne korzyści, które można uzyskać z zastosowania AI w bezpieczeństwie.
   4. Nowoczesne wyzwania, w tym zagrożenia - silnie związane z zastosowaniem Sztucznej Inteligencji w bezpieczeństwie organizacji
   5. Bezpieczeństwo a przyszłość AI

III. Podstawy prawne AI – AI Akt
   1. Wprowadzenie do AI Act
   2. Cele AI Act
   3. Systemy AI podzielone według ryzyka

4. Kluczowe wymagania dla systemów AI
5. Odpowiedzialność za naruszenia
6. Kto podlega przepisom AI Act?
7. AI Act a inne regulacje
8. AI Act a inne regulacje
9. Wpływ na małe i średnie przedsiębiorstwa (MŚP)
10. Harmonogram wdrożenia

IV. Zagrożenia AI

1. Podstawy bezpieczeństwa IT w małych organizacjach,
2. Dlaczego warto stosować AI w bezpieczeństwie? Główne zalety dla małych firm, fundacji i urzędów,
3. Przegląd najczęściej spotykanych zagrożeń cybernetycznych dla małych organizacji.

ROZDZIAŁ 3 strona 146

WYKORZYSTANIE AI W BEZPIECZEŃSTWIE ORGANIZACJI

I. Wdrożenie AI w małej organizacji

1. Przegląd narzędzi i technologii wspierających bezpieczeństwo organizacji
2. Jak wdrożyć AI w małej organizacji: krok po kroku
3. Praktyczne porady dotyczące utrzymania i monitorowania rozwiązań AI

II. Zarządzanie danymi i prywatnością przy użyciu AI

1. Przykłady zastosowań AI w tzw. RODO
2. Automatyzacja z wykorzystaniem AI - procesów zgodności z regulacjami prawnymi
3. AI - wykrywanie naruszeń prywatności

III. Bezpieczeństwo wewnętrzne organizacji przy wsparciu AI

1. Jak AI wspiera bezpieczeństwo fizyczne (monitoring, kontrola dostępu)?
2. Biometria wspierana przez AI – zastosowania w ochronie dostępu do systemów
3. Monitorowanie pracowników z użyciem AI – etyczne aspekty i zasady odpowiedzialnego użycia

PODSUMOWANIE **strona 180**

WPROWADZENIE

Witaj w świecie, gdzie technologia i bezpieczeństwo przenikają się na niespotykaną dotąd skalę, a sztuczna inteligencja staje się potężnym, aczkolwiek ciągle jeszcze bardzo mało poznanym, sojusznikiem w wędrówkach po cyberprzestrzeni oraz w walce z zagrożeniami cyber świata. Ta książka nie jest tylko teoretycznym podręcznikiem — to przewodnik, który krok po kroku przeprowadzi Cię przez podstawy cyberbezpieczeństwa z wykorzystaniem AI.

Od dynamicznie zmieniających się zagrożeń cyfrowych po mechanizmy ich przewidywania i neutralizowania — CHROŃ I ROZWIJAJ BIZNES – CYBER AI to pierwszy krok w budowaniu solidnych fundamentów ochrony dla Twojej organizacji. Sztuczna inteligencja nie jest tu postrzegana jako odległy koncept, lecz jako dostępne narzędzie, które — jeśli dobrze zrozumiane i wdrożone — może odmienić sposób, w jaki chronimy dane, zasoby i przyszłość naszych firm.

Niezależnie od tego, czy jesteś menedżerem, specjalistą ds. IT, czy liderem małej organizacji, która stawia pierwsze kroki w cyfrowym świecie, znajdziesz tu praktyczne wskazówki i techniki. Nauczysz się, jak wykorzystywać AI do identyfikacji zagrożeń, zarządzania ryzykiem, oraz w jaki sposób technologie mogą wspierać rozwój Twojej organizacji w bezpieczny i zrównoważony sposób.

Odkryj świat nowoczesnego zarządzania bezpieczeństwem z pomocą AI i przygotuj swoją organizację na wyzwania przyszłości.

ROZDZIAŁ 1 CYBER ZAGROŻENIA

I. CO TO JEST CYBER ŚWIAT

Cyber świat otacza nas dookoła, w postaci m.in.:

- portali i forów społecznościowych,
- komunikatorów internetowych,
- wiadomości oraz przypomnień, które otrzymujemy na telefon komórkowy z różnego rodzaju aplikacji,
- poczty email, itp.

Żyjemy w nim równolegle z naszym rzeczywistym bytem.

Dzieje się tak z kilku powodów:

- naszej ludzkiej mentalności nastawionej na wygodny styl życia,
- powszechny dostęp do sieci internet,
- używanie coraz bardziej zaawansowanego technologicznie sprzętu IT (smartfony, laptopy, tablety, urządzenia IoT, itp.) oraz aplikacji,
- coraz bardziej intensywne wspieranie naszego bytu przez różnego rodzaju rozwiązania AI (sztuczna inteligencja).

CYBERPRZESTRZEŃ

jest to iluzja świata rzeczywistego - stworzona za pomocą metod teleinformatycznych.

Powyższa definicja jest zaczerpnięta w całości z Wikipedii. (źródło: pl.wikipedia.org/wiki/Cyberprzestrze%C5%84). Oddaje ona idealnie omawiane zagadnienie, dlatego postanowiłem ją przytoczyć, zamiast tworzyć własny opis.

Cyberprzestrzeń podzielona jest ona na tzw. „obszary wpływów", które dość znacząco różnią się od siebie. Nasza, czyli europejska cyberprzestrzeń, charakteryzuje się względnym bezpieczeństwem. Osiągnięte to zostało poprzez wprowadzenie różnego rodzaju przepisów ochronnych, m.in. tzw. RODO. Niestety, w pozostałych obszarach cyberprzestrzeni - nie obowiązują unijne przepisy. A że internet działa jako całość, więc niestety niemal wszystkie zagrożenia z pozostałych obszarów sieci www, silnie przenikają do części europejskiej. W związku z czym narażeni jesteśmy na całe mnóstwo różnego rodzaju cyber zagrożeń lub jak mawiają inni – cyber niebezpieczeństw.

Najważniejsze obszary wpływów w omawianej cyber przestrzeni

- **Europejski**

  Byłaby to całkiem bezpieczna część internetu, gdyby nie cała jego reszta :(, której krótkie omówienie znajdziesz poniżej. Jednakże i tak Europejczycy powinni się cieszyć, bo istniejące przepisy unijne, chociaż próbują wspierać bezpieczeństwo oraz prywatność mieszkańców UE.

  Dbaniem o tzw. dobrostan obszaru EU i jej obywateli zajmuje się m.in. organizacja ENISA.

zdjęcie - źródło www.enisa.europa.eu/ - European Union Agency for Cybersecurity.

- **Amerykański**

  Dla firm z USA dane osobowe (także obywateli Unii Europejskiej), 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.

  Organizacja normująca o zasady obowiązujące w tej części świata to CISA www.cisa.gov/ - Cybersecurity & Infrastructure Security Agency.

Zdjęcie - źródło: https://www.cisa.gov/.

- **Chiński**

  Ta część międzynarodowej sieci www słynna jest przede wszystkim z totalnej inwigilacji, czyli kontrolowania, podsłuchiwania oraz nagrywania wszystkiego i wszystkich. Chyba tak najkrócej można by określić strategie chińskiego internetu. Ich serwery „pękają w szwach" od potężnych ilości przechowywanych danych.

  Choć tak po prawdzie, to amerykańskie są chyba nie mniejsze :).

  Nad omawianym obszarem pieczę trzyma m.in. Chińska Administracja Cyberprzestrzeni - CAC - centralna agencja regulująca. Zajmuje się cenzorem, nadzorem oraz kontrolą Internetu dla ChRL.

  Zdjęcie – źródło: www.cac.gov.cn

- **Indyjski**

  Indie mają podejście podobne do amerykańskiego – dane są po to, aby na nich zarobić i sprzedać jak najwięcej towarów handlowych. Organizacja rządowa Indii dbająca głównie o ochronę krytycznych systemów informacyjnych oraz infrastrukturę, to NCIIPC.

Zdjęcie – źródło: National Critical Information Infrastructure Protection Centre - nciipc.gov.in

- **Rosyjski**

  Ta część internetu zawsze była niebezpieczna. 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 Federacją Rosyjską. Zatem dając dobry przykład nie byłem na ich stronach i nie umieszczę ilustracji związanej z fsb.ru. 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 w początkach swojego istnienia to była ostoja: wolności słowa, idei, ciekawych dyskusji, itd. Tak było na początku jego istnienia i ciągle niektórzy używają go w tym celu. Niestety w większej swojej części, zawiera „całe tony" zła: przemoc, przestępczość, handel wszystkim co nielegalne oraz naszymi danymi – ukradzionymi w cyber świecie.

Dla tak zwanego „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.

Wymieniłem powyżej najważniejsze obszary przestrzeni cyfrowej, ale jak zapewne się domyślasz nie jest to pełna lista. Z ważniejszych, które pominąłem, to obszary związane z Ameryką Południową oraz pozostałą częścią Azji, m.in. Koreą Południową..

Planując rozwój Twojej firmy, czy też ogólniej – organizacji, musisz zwrócić uwagę na potencjalne zyski i koszty. Używając określonych narzędzi teleinformatycznych (np. aplikacji handlowych) zwróć uwagę, na ich pochodzenie i potencjalne niebezpieczeństwa z tym związane.

II. NAJWIĘKSZE CYBER ZAGROŻENIA DLA FIRM I INSTYTUCJI

W obecnym świecie, nafaszerowanym technologią, wszystkie organizacje mają do czynienia z olbrzymią liczbą zagrożeń. Dotyczy to:

- **świata cyfrowego – cyberprzestrzeni**
- **świata rzeczywistego,**
- **połączenia obydwu wyżej wymienionych.**

Przestępcy w swoich działaniach są niezwykle:

- **kreatywni,**
- **brutalni,**
- **bezlitośni.**

W dzisiejszych czasach - niestety - bardzo wysoka jest skuteczność działań przestępczych świata cyber, co związane jest z wieloma czynnikami. W mojej opinii najważniejsze z nich, to:

- sztuczna inteligencja,
- brak wystarczającej wiedzy osób (szczególnie tzw. pracowników biurowych) korzystających ze świata nowoczesnych technologii,
- powszechność zaawansowanych urządzeń IT,
- łatwość dostępu do internetu.

1. NAZEWNICTWO I OPIS NAJCZĘŚCIEJ WYSTĘPUJĄCYCH ZAGROŻEŃ CYFROWYCH

Phishing

Jest to próba pozyskania danych użytkownika (np. loginu oraz hasła), zwykle poprzez dostarczeniem nieprawdziwych informacji, typu:

„Twoje konto wymaga potwierdzenia! Kliknij”. Nazwa zaczerpnięta jest z dwóch słów angielskich:

- password („hasło”)
- fishing („wędkowanie”).

Phishing posiada wiele odmian i jest prawdopodobnie przyczyną największej ilości różnego rodzaju incydentów bezpieczeństwa. Od niego zaczyna się wiele innego rodzaju ataków. Posiada on mnóstwo odmian. Omówię go szerzej w dalszej części tego rozdziału.

Malvertising

dotarcie do użytkowników świata cyfrowego przeglądających jedynie zaufane strony internetowe. Ich nośnikiem są zwykle reklamy internetowe wyświetlane poprzez sieci reklamowe.

Ransomware

Program komputerowy (skrypt), który powoduje zaszyfrowanie danych użytkownika, co poprzedzone jest zwykle ich wypłynięciem na zewnętrzny serwer. Następnie poszkodowany/a otrzymuje żądanie opłaty za:

- odblokowanie zasobów,
- uniknięcie wystawienia ich do publicznej sprzedaży (zwykle w darknecie).

Zazwyczaj kod ransomware znajduje się na komputerze ofiary dużo wcześniej niż moment zablokowania dostępu do zasobów. Zaszyfrowanie danych jest przedostatnim etapem ataku. A ostatnim jest zazwyczaj informacja o zablokowaniu komputera i wysunięcie żądań okupu.

Wiper

Często wraz z Ransomware na komputery poszkodowanych trafia tzw. wiper, czyli program komputerowy, który usuwa (niszczy) całą zawartość twardych dysków. Przestępcy wówczas „uprzejmie informują", że:

„Wiemy, iż masz kopie zapasowe danych i je sobie odzyskasz. Ale pełne Twoje dane, posiadamy na naszych serwerach. Musisz zapłacić, abyśmy ich nie udostępnili."

DDoS

Atak hakerski (Distributed Denial of Service- Rozproszona/ Rozpowszechniona Odmowa Usługi), którego celem jest sparaliżowanie systemu komputerowego l/lub sieci www, czyli np. strony www. Dzieje się tak w wyniku wysłanie potężnej ilości zapytań do konkretnego systemu. Efektem jest zwykle:

- brak dostępu do sieci i usług,
- wydłużony czas ładowania stron,
- zmniejszenie wydajności sieci, itp.

Cross-site scripting

Jest to specjalny kod na stronie internetowej, który powoduje wykonanie akcji niezamierzonej i nieoczekiwanej przez internautę. Zwykle odbywa się to bez jakiejkolwiek świadomości osoby atakowanej.

Odmianą są ataki XSS, czyli wstrzyknięcie złośliwych skryptów do wcześniej nieszkodliwych i zaufanych stron internetowych. Atakujący może użyć XSS do wysłania złośliwego skryptu do użytkownika, którego przeglądarka nie ma możliwości dowiedzenia się, że skrypt nie powinien być zaufany, dlatego nie ma oporów przed jego wykonaniem. A ponieważ uważa, że skrypt pochodzi z zaufanego źródła, złośliwy skrypt może uzyskać dostęp do tokenów sesji, plików cookie lub innych poufnych informacji przechowywanych przez przeglądarkę oraz używanych z tą witryną.

Jedną z metod zabezpieczenia przed tym atakiem, może być nowoczesny program antywirusowy wraz z systematycznie aktualizowanymi:

- systemem operacyjnym
- innymi aplikacjami.

SQL Injection

uzyskanie nieuprawnionego dostępu do bazy danych poprzez lukę w zabezpieczeniach aplikacji, często popartą czynnikiem ludzkim.

Przechwytywanie danych

Ta forma hackingu nazywana jest często: Man in the Middle - „człowiek pośrodku”.

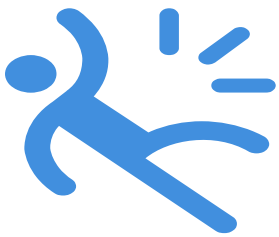
Przestępca - haker - znajduje się pomiędzy dwoma stronami transakcji, np. między Tobą a Twoim bankiem. Efektem może być przechwycenie środków pieniężnych lub innych istotnych informacji (oraz ich niepożądana modyfikacja).

Brute Force

Atak siłowy jest jednym z najtrudniejszych do zrealizowania sposobów dotarcia „do wnętrza organizacji". Łatwiej oraz z decydowanie mniejszym kosztem – można tego dokonać poprzez tzw. phishing.

W omawianym rodzaju ataku możemy mieć do czynienia między innymi z:

- łamaniem „słabych haseł" używanych przez pracowników firmy czy instytucji, a to jest trudne do zrealizowania „bez pomocy" :) użytkowników systemów IT;
- wykorzystaniem tzw. podatności systemów i/lub różnego rodzaju aplikacji, czyli w wielkim uproszczeniu „dziur w zabezpieczeniach".



2. NAJLEPSZE SPOSOBY OBRONY PRZED ZAGROŻENIAMI CYFROWYMI

1. Phishing

- Opis:

  Oszustwo polegające na podszywaniu się pod zaufane osoby lub organizacje w celu wyłudzenia danych (np. loginów, haseł).

- Sposoby obrony:

SERDECZNIE ZAPRASZAM DO SKORZYSTANIA Z PEŁNEJ WERSJI PORADNIKA - POZDRAWIAM

AUTOR: DARIUSZ GOŁĘBIOWSKI

PODSUMOWANIE

W tym poradniku przeszliśmy wspólnie przez dynamiczny świat cyberbezpieczeństwa wspieranego przez sztuczną inteligencję. Poznaliśmy podstawowe narzędzia, które mogą zmienić sposób, w jaki organizacje (także Twoja) zabezpieczają swoje dane i zasoby oraz wypracowaliśmy zrozumienie technologii, które — właściwie użyte — mogą stanowić o przewadze konkurencyjnej i stabilności w coraz bardziej cyfrowej rzeczywistości.

Stawiając kroki w stronę przyszłości z AI, zyskaliśmy świadomość, że cyberbezpieczeństwo to nie tylko technologia, ale przede wszystkim podejście. To zestaw działań, które każda organizacja powinna:

- planować,
- dostosowywać,
- rozwijać,

dbając w ten sposób o potrzeby organizacji i odpowiadając na rosnące wyzwania środowiska cyfrowego.

Dzięki przedstawionym w tym poradniku informacjom i poradom, prawdopodobnie masz już fundamenty, które pozwolą na świadomą ochronę Twojej organizacji.

Kolejnym krokiem, który będziesz mógł/ła wykonać będzie rozpoczęcie strategii świadomego rozwijania biznesu w zgodzie z najnowszymi osiągnięciami technologii. Tym zagadnieniem zajmuję się w drugiej części tego poradnika. Już teraz serdecznie zapraszam do skorzystania z moich kolejnych porad, czyli następnego ebooka tej serii.

Niech ta książka będzie punktem wyjścia do wdrażania strategii cyberbezpieczeństwa w organizacjach różnej wielkości, inspirując do dalszego zgłębiania tematu. Kolejne części serii „CHROŃ I ROZWIJAJ BIZNES – CYBER AI" przybliżą kolejne aspekty i pokażą, jak technologia może wspierać rozwój, innowacje oraz stabilność organizacji w każdym aspekcie jej działalności.

Podążając tą ścieżką, stajesz się nie tylko strażnikiem bezpieczeństwa i spokoju, ale także architektem nowoczesnej organizacji przyszłości.

Pozdrawiam

Ciebie - moja Droga Czytelniczko *oraz*

Ciebie - mój Wspaniały Czytelniku

Autor poradnika - Dariusz Gołębiowski

W poradniku wykorzystano:

- **własne materiały graficzne,**
- **prace graficzne: Chat GPT4,**
- **cliparty z programu LibreOffice na licencji CCO.**

DZIĘKUJĘ ZA UWAGĘ

Autor poradnika: DARIUSZ GOŁĘBIOWSKI

Zapraszam do zapoznania się z innymi książkami, które napisałem lub współtworzyłem.

Więcej informacji znajdziesz na stronach firmy:

Wydawnictwo Cyfrowe poswojsku.pl , www.poswojsku.pl

Prawa autorskie i znaki towarowe:

Wszystkie wymienione nazwy firm, produkty, usługi i logo są znakami towarowymi lub zastrzeżonymi znakami towarowymi ich odpowiednich właścicieli. Nazwy te służą wyłącznie celom informacyjnym i nie oznaczają poparcia ani powiązania z tymi markami.

OpenAI i ChatGPT są znakami towarowymi OpenAI.

Microsoft, Copilot, Bing, oraz Windows są zarejestrowanymi znakami towarowymi firmy Microsoft.

Gemini jest zarejestrowanym znakiem towarowym Google LLC.

Claude AI jest znakiem towarowym Anthropic PBC.

Mistral AI jest znakiem towarowym Mistral AI.

Bielik AI jest zarejestrowanym znakiem towarowym jego właściciela.

Apple, iOS i macOS są zastrzeżonymi znakami towarowymi firmy Apple Inc. w Stanach Zjednoczonych i/lub innych krajach.

Android jest zastrzeżonym znakiem towarowym firmy Google LLC.

Facebook jest zastrzeżonym znakiem towarowym firmy Meta Platforms, Inc.

Inne wymienione nazwy firm, produktów i usług mogą być znakami towarowymi odpowiednich właścicieli.