Metody tworzenia firmy odpornej na cyberprzestępcę - **prompty do AI**

Autor Artur Markiewicz

Cześć, pomożesz mi?

Cześć! Oczywiście, w czym mogę Ci pomóc?

Chcesz wiedzieć więcej?

Zobacz informacje na stronie

Metody tworzenia firmy odpornej na cyberprzestępcę - **prompty do AI**

Autor Artur Markiewicz

Spis treści

Metryka dokumentu

Historia

Wersja	Data	Status	Powód zmiany
1.0	2.09.2024	Utworzono	Uzupełnienie dokumentu https://cyberkurs.online/poradnik-metody-tworzenia-firmy-odpornej-na-cyberprzestepce-i-ataki-typu-ransomware/
2.0	20.09.2024	Utworzono	Poprawki merytoryczne, wyrażone opinie, zebranie treści w całość

Licencja

Publikacja materiału

Data	Wersja	Miejsce
2.09.2024	1.0	https://cyberkurs.online/
22.09.2024	2.0	https://cyberkurs.online/

1. Wstęp

Twoi ludzie nie są winni temu, że firma nie jest bezpieczna.
Szukanie winnych u ludzi to ślepa uliczka.
Winne są procesy lub ich brak.
Winny jest poziom wiedzy i ścieżki jej zdobywania.
Winna jest trójka: lenistwo, niekompetencja, pazerność.

Lenistwo to robienie czegoś najkrótszą drogą, żeby było widać efekt. To zaniechanie robienie czegoś innego. W zakresie cyberbezpieczeństwa to nie stosowanie się do procedur, do dobrych praktyk. To ignorowanie czerwonych flag, które powiewają w komunikacie przestępcy. To także prokrastynacja, czekanie na mityczny poniedziałek, żeby zacząć coś robić.

Niekompetencja nie wynika z człowieka, a z deficytu wiedzy. Ludzie unikają wiedzy, bo wymaga uczenia się czegoś nowego (**lenistwo**).
To także brak szerokiego myślenia, ograniczanie się do wycinka, w którym człowiek czuje się dobrze. W zakresie cyberbezpieczeństwa zrobienie jednej rzeczy dobrze nie oznacza, że cały łańcuch będzie wytrzymały. Niekompetencja ma swoje źródło w galopującej rzeczywistości, gdzie czasem trudno jest nadrobić braki wiedzy. Materia do zrozumienia jest spora, a każdy punkt łączy się, zależy od czegoś innego.
Wiedza niezbędna do zapewnienia poziomu cyberbezpieczeństwa nie towarzyszyła nam w naturalnej ścieżce edukacji (do teraz nie towarzyszy).

Pazerność to apetyty na duże zyski małym wysiłkiem energetycznym. To towarzyszy przestępcy. Ma on relatywnie wysoki zwrot z inwestycji przy bardzo mały wkładzie pracy.
Firmy, systemy, ludzie są słabo zabezpieczeni (**niekompetencja**), nie przestrzegają zasad (**lenistwo**), co daje przestępcy bardzo nisko wiszące owoce.

Łatwiej może być kogoś okraść (okup z ataku ransomware) niż podobne pieniądze zarobić w legalny sposób.
Firmy często zdobywają nowe rynki w bardzo agresywny sposób, nie uwzględniając potrzeby cyberbezpieczeństwa takich operacji.
Każdy nowy proces, każda zmiana potrzebuje dostosowania środków bezpieczeństwa. W praktyce to dynamiczna analiza zagrożeń.

Dowolne proporcje tych zjawisk, tworzą przestrzeń, która jest, na którą można nałożyć dobre praktyki i podnieść poziom bezpieczeństwa.

Ludzie branży cyberbezpieczeństwa, specjaliści infoSEC, są od tego, żeby być tuż przed firmą i odgarniać zagrożenia, które są znane i przewidywalne. Są niczym **pług śnieżny**, który jest tuż przed pociągiem pędzącym swoim torem w śnieżną pogodę.
Maszynista, pasażerowie nie odpowiadają za to, że śnieg pada, nie mają na niego wpływu. Jak zignorują i nie zrobią z tym nic, nie dojadą do celu. Ludzie branży są od tego, żeby owe **przeszkody usuwać z drogi** firmy.
Te przeszkody tam są.
Przestępcy są, działają, mają swoje sposoby i techniki.

Korzystają z luk, niedoskonałości, błędów, ignorancji, lenistwa, niekompetencji ludzi, firm, technologii.
Nie mamy wpływu na ich motywację, **mamy wpływ na** to co z tym zrobimy.
O tym jest ten poradnik - zbiór promptów do AI w celu pozyskania najlepszego wsparcia.

Wiele poradników powstało po to by były, by je wypchnąć na rynek, zarobić, zrobić i zapomnieć.

Chciałbym, żeby ten poradnik był stosowany i manager mógł do niego wracać.
Treść pisałem tak by była uniwersalna w kontekście tego co jest dziś i co da się przewidzieć w przyszłości :)
Fundamenty powstały na bazie moich doświadczeń, dokumentów, z którymi pracuję.

Zagadnienia merytoryczne są opisane spłyconym językiem.
Nie jest odbiorcą poradnika specjalista inżynier, lecz specjalista, który chce by procesy biznesowe, dane w firmie były bezpieczne.

Manager opiekujący się biznesem nie może dziś ignorować cyberbezpieczeństwa, traktować go jako zła koniecznego.
Zaopiekowanie się tematach ochrony biznesu jest elementem odpowiedzialności za biznes.

Obowiązkiem jest wiedzieć kto wie więcej, kto co zrobił i co planuje robić.
Obowiązkiem jest narzucić kierunek.
Obowiązkiem jest wiedzieć co ma być chronione.
Deficyty wiedzy o tym jak się coś chroni jest zrównoważony właściwymi pytaniami, nadaniem kierunku i przekazaniem obszaru do specjalistów.
To co będzie pokryte środkami bezpieczeństwa zależy od analizy ryzyka i odpowiedzi co i przed czym chronić.

Poradnik był pisany w kontekście ochrony przed atakami ransomware, które mają swoja specyfikę, ale dokładnie te same rady mogą jednocześnie chronić przed wieloma innymi źródłami problemów.

Stawiam zawsze na profilaktykę, która rozpoczyna się od takich materiałów. Przygotowanie się na przewidywalne zagrożenia to analiza ryzyka, stosowanie odpowiednich zabezpieczeń.

Te zagrożenia, które nie były bezpośrednio analizowane najczęściej mogą być pokryte posiadanymi zabezpieczeniami, a nawet jeśli nie, to drogą, którą przebyła organizacja pomoże i będzie wsparciem w reagowaniu na to co nie było przewidziane.

Nawet w najczarniejszym scenariuszu może być moment zapanowania nad konsekwencjami, opanowaniem sytuacji i wyciągnięciem z niej lekcji.

Zarządzanie kryzysowe, procedury przywracania, plan ciągłości działanie, ciągłe doskonalenie będą pomocne w wielu sytuacjach.

Najgorsza sytuacja to bycie w mitycznym, życzeniowym, myśleniu, że nam się nic nie stanie, ataki nas nie spotkają, a nawet jeśli to nie mamy nic do stracenia.

Pytania:
1. Czy będziemy zaatakowani?
2. Kiedy będziemy zaatakowani?
Nie mają znaczenia, bo kiedyś będziemy.

Inne kolejne pytania są ważniejsze:
3. Skąd będziemy wiedzieli, że jesteśmy zaatakowani?
4. Co wówczas zrobimy?
Pomocny w udzieleniu odpowiedzi na te pytania jest ten poradnik.

Od odpowiedzi co to ten atak ransomware, poprzez możliwe konsekwencje, studium przypadków, taktyk przestępców, role zarządu i co powinni wiedzieć, przez mapowanie ryzyk, środki zabezpieczające, rolę szkoleń, kopie zapasowe, kategoryzację danych, na planie ciągłości działania i sposobie reagowania na incydenty kończąc.
Dodatkowo słownik, sugestie innych działań i źródła wiedzy.

Poradnik możesz czytać po kolei, wybranymi rozdziałami lub pytaniami managera co do zakresu (najczęściej ostatni punkt rozdziału).

W poradniku znajdziesz także prompty do AI (model językowy, "sztuczna inteligencja") czyli narzędzia, które może być twoim źródłem aktualnej wiedzy.

Powodzenia,
Artur Markiewicz

DOKUMENT, KTÓRY CZYTASZ TO TYLKO WYBRANY ZAKRES.
W TYM MATERIALE SĄ PROMPTY DO WŁASNEJ PRACY.
PEŁEN PORADNIK METODY TWORZENIA FIRMY ODPORNEJ NA CYBERPRZESTĘPCĘ I ATAKI TYPU RANSOMWARE ZNAJDZIESZ TU

2. Podziękowania

Bardzo dziękuję mojemu przyjacielowi projektowemu, który zainspirował mnie do rozszerzenia poradnika o prompty AI.
Artur Maciąg od wielu lat jest moim doskonałym rozmówcą, wiele naszych rozmów tzw. ploteczki o branży było źródłem mojej wiedzy i apetytu na więcej.
Tym razem udało się przelać na papier inspirację z jednej z takich rozmów.

Artur, dziękuję!

Kieruję także podziękowania dla Społeczności Linkedin za wsparcie i zachętę do zbudowania tego poradnika.

To dzięki Wam i dzięki waszym treściom stworzyłem ten dokument.

3. Korzystanie z AI

Wprowadzenie promptów AI do tego poradnika ma na celu zwiększenie samodzielności managerów w obszarze cyberbezpieczeństwa oraz ułatwienie pracy z przedstawionymi tu materiałami.

Prompty te zostały zaprojektowane tak, aby wspierać managerów w budowaniu kontekstu, znajdowaniu najlepszych rad, wytycznych oraz sposobów stosowania środków bezpieczeństwa w ich firmach.

Kluczowe założenia

Cześć, pomożesz mi?

PODAWANIE ŹRÓDEŁ: KAŻDA ODPOWIEDŹ GENEROWANA PRZEZ AI POWINNA ZAWIERAĆ ODNIESIENIE DO ŹRÓDEŁ, Z KTÓRYCH POCHODZI INFORMACJA. DZIĘKI TEMU MANAGEROWIE MOGĄ BYĆ PEWNI, ŻE OTRZYMUJĄ DANE OPARTE NA SPRAWDZONYCH I WIARYGODNYCH INFORMACJACH, CO JEST KLUCZOWE W PODEJMOWANIU DECYZJI ZWIĄZANYCH Z BEZPIECZEŃSTWEM FIRMY.

BUDOWANIE KONTEKSTU: PROMPTY SĄ ZAPROJEKTOWANE TAK, ABY POMAGAŁY MANAGEROM W TWORZENIU KONTEKSTU SPECYFICZNEGO DLA ICH FIRMY. DZIĘKI TEMU MOŻLIWE JEST LEPSZE DOSTOSOWANIE STRATEGII I DZIAŁAŃ DO UNIKALNYCH POTRZEB ORGANIZACJI, CO ZWIĘKSZA SKUTECZNOŚĆ WDROŻONYCH ŚRODKÓW OCHRONNYCH.

Aby ułatwić tworzenie spersonalizowanych promptów, które będą odpowiadały na konkretne potrzeby Twojej firmy, proponuję skorzystanie z poniższego Master Promptu.
To narzędzie pozwoli Ci na budowanie kolejnych promptów, które AI będzie mogła wykorzystać do generowania szczegółowych rekomendacji i odpowiedzi.

Master Prompt

> *Używając najnowszych i sprawdzonych informacji dostępnych w Twojej bazie danych, pomóż mi zbudować listę szczegółowych promptów do AI, które dostosują pytania, strategie ochrony oraz studium przypadków do specyfiki mojej firmy w branży [branża]. Jestem managerem, który nie jest ekspertem technicznym, więc proszę o podanie odpowiedzi w sposób zrozumiały, unikając nadmiernie technicznego języka. Proszę również o podanie źródeł, na których opierają się te odpowiedzi, oraz uwzględnienie najlepszych praktyk w obszarze cyberbezpieczeństwa.*

Wyślij wiadomość do

Każdy z tych promptów, podobnie jak Master Prompt, zakłada, że AI korzysta z najnowszych i sprawdzonych informacji, zawsze podając źródła, na których się opiera.
Dzięki temu możesz być pewien, że otrzymane rekomendacje są aktualne i wiarygodne, co pozwala na ich efektywne wdrożenie w Twojej firmie.

Dostosuj prompty do unikalnych zagrożeń, z którymi spotyka się twoja firma, poprzez dodanie specyficznych fraz dotyczących branży lub technologii, takich jak ‘IoT’, ‘przemysł 4.0’.
Mimo wszystko podchodź do odpowiedzi krytycznie i dopytuj.

Chcesz wiedzieć więcej? Zobacz informacje na stronie

Dodatek o prywatności danych

Korzystanie z narzędzi AI może znacząco ułatwić pracę i zwiększyć efektywność działań w obszarze cyberbezpieczeństwa.
Ważne jest jednak, aby być świadomym potencjalnych ryzyk związanych z udostępnianiem informacji tym systemom.
Wprowadzając dane do aplikacji AI, istnieje możliwość niezamierzonego ujawnienia poufnych informacji, które mogą zostać przetworzone lub przechowywane poza kontrolą Twojej firmy.

Cześć, pomożesz mi?

UWAGA: AUTOR PORADNIKA NIE PONOSI ODPOWIEDZIALNOŚCI ZA EWENTUALNE SKUTKI WYNIKAJĄCE Z NIEWŁAŚCIWEGO KORZYSTANIA Z NARZĘDZI AI ORAZ UDOSTĘPNIANIA POUFNYCH INFORMACJI. ZALECA SIĘ ZACHOWANIE OSTROŻNOŚCI I PRZESTRZEGANIE WEWNĘTRZNYCH POLITYK BEZPIECZEŃSTWA.

Aby zminimalizować ryzyko, warto rozważyć korzystanie z licencjonowanych rozwiązań AI, które gwarantują, że dane nie opuszczają infrastruktury Twojej firmy i są przetwarzane zgodnie z obowiązującymi standardami bezpieczeństwa.
Takie podejście pozwala na pełne wykorzystanie możliwości sztucznej inteligencji przy jednoczesnym zachowaniu najwyższego poziomu ochrony danych.

Wyślij wiadomość do

4. Co to jest atak typu Ransomware

Ataki typu ransomware są dynamicznym i ewoluującym zagrożeniem.
Managerowie muszą zrozumieć mechanizmy tych ataków oraz sposoby ich rozpoznawania.
Poprzez zadawanie AI pytań o aktualne formy ataków i zagrożeń, będą w stanie lepiej przygotować swoje firmy na potencjalne incydenty.

Kluczowe prompty do AI

Te prompty dla rozdziału "Co to jest Atak typu Ransomware" mają na celu pomóc managerowi w zrozumieniu natury ataków typu ransomware.

Zrozumienie mechanizmów ataku ransomware

> *Jako manager, chcę zrozumieć, jak działają mechanizmy ataków typu ransomware i jakie są ich najnowsze formy. Uwzględnij kontekst firmy, która działa w [branża]. Proszę o szczegółowe wyjaśnienie oraz źródła potwierdzające te informacje.*

Analiza zagrożeń związanych z ransomware

> *Pomóż mi jako managerowi, przeanalizować zagrożenia związane z ransomware dla mojej firmy, która działa w [branża]. Proszę o informacje na temat najnowszych form tego zagrożenia oraz źródła dotyczące ich wpływu na organizacje.*

Rozpoznawanie sygnałów ataku ransomware

> *Jakie są najczęstsze sygnały świadczące o tym, że firma jest celem ataku ransomware? Jako manager, chciałbym zrozumieć te sygnały, aby lepiej chronić moją firmę, która działa w [branża]. Proszę o aktualne informacje i źródła.*

Ochrona firmy przed ransomware

> *Jakie są najskuteczniejsze metody ochrony firmy przed atakami ransomware? Proszę o aktualne rekomendacje oraz źródła dotyczące najlepszych praktyk w tym zakresie.*

Edukacja pracowników na temat ransomware

> *Jak mogę jako manager uczyć pracowników na temat zagrożeń związanych z ransomware i sposobów*

zapobiegania takim atakom? Proszę o materiały edukacyjne i źródła, które można wykorzystać.

Przykłady przypadków ataków ransomware w podobnych firmach

Jako manager, chcę poznać przykłady ataków ransomware, które dotknęły firmy działające w podobnej branży do mojej. Proszę o informacje na temat tych przypadków oraz wyciągnięte wnioski, wraz ze źródłami potwierdzającymi te dane.

Cześć, pomożesz mi?

Przeciwdziałanie ransomware przy minimalnym budżecie

Cześć! Oczywiście, w czym mogę Ci pomóc?

Jakie są najskuteczniejsze metody ochrony przed ransomware, które mogę wdrożyć w mojej firmie przy ograniczonym budżecie? Proszę o rekomendacje, poparte źródłami.

Wpływ ransomware na reputację firmy

Jakie mogą być długoterminowe skutki ataku ransomware na reputację mojej firmy? Proszę o informacje na temat wpływu takich incydentów oraz źródła potwierdzające te dane.

Wyślij wiadomość do

11. Szkolenia i edukacja pracowników

Ludzie są często najsłabszym ogniwem w łańcuchu bezpieczeństwa organizacji. Dlatego regularne szkolenia z zakresu cyberbezpieczeństwa są kluczowe. Szkolenia te pomagają pracownikom zrozumieć zagrożenia, takie jak phishing czy ransomware oraz uczą, jak unikać pułapek, które mogą zagrozić firmie.
Edukacja musi być stała i dostosowana do zmieniającego się środowiska zagrożeń, aby personel był świadomy najnowszych technik stosowanych przez cyberprzestępców.

Po uzyskaniu wyników promptu dotyczącego zagrożeń phishingowych, przekaż te dane działowi IT i marketingu, aby opracowali dedykowane szkolenia dla pracowników oraz wzmocnili filtry pocztowe.

Kluczowe prompty do AI

Te prompty dla rozdziału "Szkolenia i Edukacja Pracowników" mają na celu pomóc managerowi w opracowaniu i wdrożeniu skutecznych programów szkoleniowych z zakresu cyberbezpieczeństwa.

Tworzenie programów szkoleniowych z zakresu cyberbezpieczeństwa

> *Jako manager, chcę dowiedzieć się, jak opracować skuteczny program szkoleniowy z zakresu cyberbezpieczeństwa dla moich pracowników. Proszę o najnowsze wytyczne i najlepsze praktyki, poparte odpowiednimi źródłami.*

Regularność i zakres szkoleń

> *Jak często powinienem organizować szkolenia z zakresu cyberbezpieczeństwa, aby były one skuteczne? Jako manager, proszę o aktualne rekomendacje dotyczące częstotliwości i zakresu szkoleń, poparte źródłami.*

Metody angażowania pracowników w szkolenia

> *Jakie są najlepsze metody angażowania pracowników w szkolenia z zakresu cyberbezpieczeństwa, aby były one skuteczne i przynosiły realne korzyści? Proszę o informacje i źródła dotyczące najnowszych technik angażowania.*

Ocena skuteczności szkoleń

> *Jak mogę jako manager ocenić skuteczność przeprowadzonych szkoleń z zakresu cyberbezpieczeństwa? Proszę o najnowsze metody oceny i źródła dotyczące ich skuteczności.*

Dostosowanie szkoleń do zmieniających się zagrożeń

Jak mogę jako manager dostosować programy szkoleniowe do zmieniających się zagrożeń cybernetycznych? Proszę o aktualne informacje i źródła dotyczące najnowszych zagrożeń oraz metod ich uwzględniania w szkoleniach.

Cześć, pomożesz mi?

Cześć! Oczywiście, w czym mogę Ci pomóc?

Wyślij wiadomość do

17. Reagowanie na Incydent: Kluczowe kroki dla firmy

Skuteczna reakcja na incydent cyberbezpieczeństwa wymaga szybkiego i dobrze zorganizowanego działania.
Kluczowe kroki obejmują identyfikację incydentu, ograniczenie szkód, analizę jego przyczyn oraz wdrożenie środków naprawczych.
Managerowie powinni opracować plan reagowania na incydenty, który jasno definiuje role i obowiązki zespołów odpowiedzialnych za bezpieczeństwo, a także zapewnia odpowiednią komunikację wewnętrzną i zewnętrzną.
Regularne ćwiczenia symulacyjne mogą pomóc zespołom w lepszym przygotowaniu się na rzeczywiste incydenty, minimalizując czas reakcji i skutki potencjalnych ataków.

Kluczowe prompty do AI

Te prompty dla rozdziału mają na celu pomóc managerowi w efektywnym reagowaniu na incydenty związane z cyberbezpieczeństwem.

Kluczowe kroki reagowania na incydent

> *Jako manager, chcę poznać aktualne kluczowe kroki, które firma powinna podjąć w odpowiedzi na incydent bezpieczeństwa, taki jak atak ransomware. Proszę o szczegółowy opis tych kroków wraz z odniesieniami do najnowszych źródeł.*

Ocena gotowości firmy na incydenty

> *Pomóż mi jako managerowi, ocenić gotowość mojej firmy na reagowanie na incydenty związane z cyberbezpieczeństwem. Proszę o najnowsze wytyczne i źródła dotyczące oceny i poprawy gotowości firmy na takie sytuacje.*

Wdrożenie planu reagowania na incydent

> *Jakie są najlepsze praktyki wdrażania planu reagowania na incydenty w firmie? Jako manager, chciałbym otrzymać aktualne informacje na ten temat, poparte źródłami, które wskazują na skuteczność tych działań.*

Szkolenie zespołów reagowania na incydenty

> *Jakie szkolenia powinienem przeprowadzić, aby mój zespół był przygotowany do skutecznego reagowania na incydenty? Proszę o najnowsze rekomendacje oraz źródła.*

Minimalizacja skutków incydentów

Jakie działania mogę podjąć jako manager, aby zminimalizować skutki incydentów cyberbezpieczeństwa? Proszę o aktualne informacje oraz najlepsze praktyki, poparte źródłami.

Cześć, pomożesz mi?

Cześć! Oczywiście, w czym mogę Ci pomóc?

Wyślij wiadomość do

25. Propozycja ćwiczeń symulacyjnych

Ćwiczenia symulacyjne to jeden z najbardziej efektywnych sposobów przygotowania firmy na potencjalne ataki cybernetyczne, w tym ransomware.
Regularne przeprowadzanie symulacji incydentów pozwala zespołom doskonalić swoje umiejętności reagowania, sprawdzać procedury w praktyce i minimalizować potencjalne błędy podczas rzeczywistego ataku.
Managerowie powinni opracować różnorodne scenariusze ćwiczeń, które odzwierciedlają możliwe zagrożenia, i regularnie testować gotowość zespołów.

Kluczowe prompty do AI

Te prompty mają na celu pomóc managerowi w opracowaniu, wdrażaniu i analizie skutecznych ćwiczeń symulacyjnych.

Opracowanie scenariuszy ćwiczeń symulacyjnych

```
Jako manager, chcę opracować różnorodne scenariusze
ćwiczeń symulacyjnych dla mojej firmy, które pomogą
przygotować zespół na ataki typu ransomware. Proszę o
przykłady skutecznych scenariuszy oraz źródła
potwierdzające ich wartość.
```

Najlepsze praktyki w przeprowadzaniu symulacji

```
Jakie są najlepsze praktyki w zakresie przeprowadzania
ćwiczeń symulacyjnych w firmie? Jako manager, chcę
poznać najnowsze rekomendacje dotyczące częstotliwości
symulacji, przygotowania zespołu oraz ewaluacji
wyników. Proszę o informacje oraz źródła
potwierdzające te zalecenia.
```

Ewaluacja gotowości zespołu po ćwiczeniach symulacyjnych

```
Jak mogę jako manager ocenić skuteczność mojego
zespołu po przeprowadzeniu ćwiczeń symulacyjnych?
Proszę o rekomendacje dotyczące metod ewaluacji oraz
źródła, które potwierdzają ich skuteczność.
```

Dostosowanie symulacji do nowych zagrożeń

```
Jak mogę jako manager dostosować ćwiczenia symulacyjne
do nowych i rozwijających się zagrożeń, w tym
ransomware? Proszę o informacje na temat metod
aktualizacji scenariuszy oraz źródła, które
potwierdzają ich skuteczność w dynamicznie
zmieniającym się środowisku.
```

Integracja ćwiczeń symulacyjnych z procedurami firmy

```
Jak mogę skutecznie zintegrować ćwiczenia symulacyjne
z istniejącymi procedurami bezpieczeństwa mojej firmy?
Proszę o informacje na temat najlepszych metod
integracji oraz źródła, które potwierdzają skuteczność
tego podejścia.
```

Cześć, pomożesz mi?

Cześć! Oczywiście, w czym mogę Ci pomóc?

Wyślij wiadomość do

Autor dokumentu

Artur Markiewicz

Konsultant cyberbezpieczeństwa

WWW: https://cyberkurs.online/

LI: https://www.linkedin.com/in/artur-markiewicz/

- Lider, trener, konsultant.
- Cyber Security Consultant w Trecom,
- Członek Zarządu ISSA Polska,
- Członek Zespołu Cyfrowy Skaut,
- Lider projektu #ISSAPolskalocal.
  Realizuje i koordynuje projekty IT dla biznesu, edukacji czy administracji publicznej.

Źródło poradnika