



PROJEKT RETAIL

MATERIAŁY DODATKOWE

Cyberbezpieczeństwo
w procesie cyfryzacji

PROJEKT RETAIL



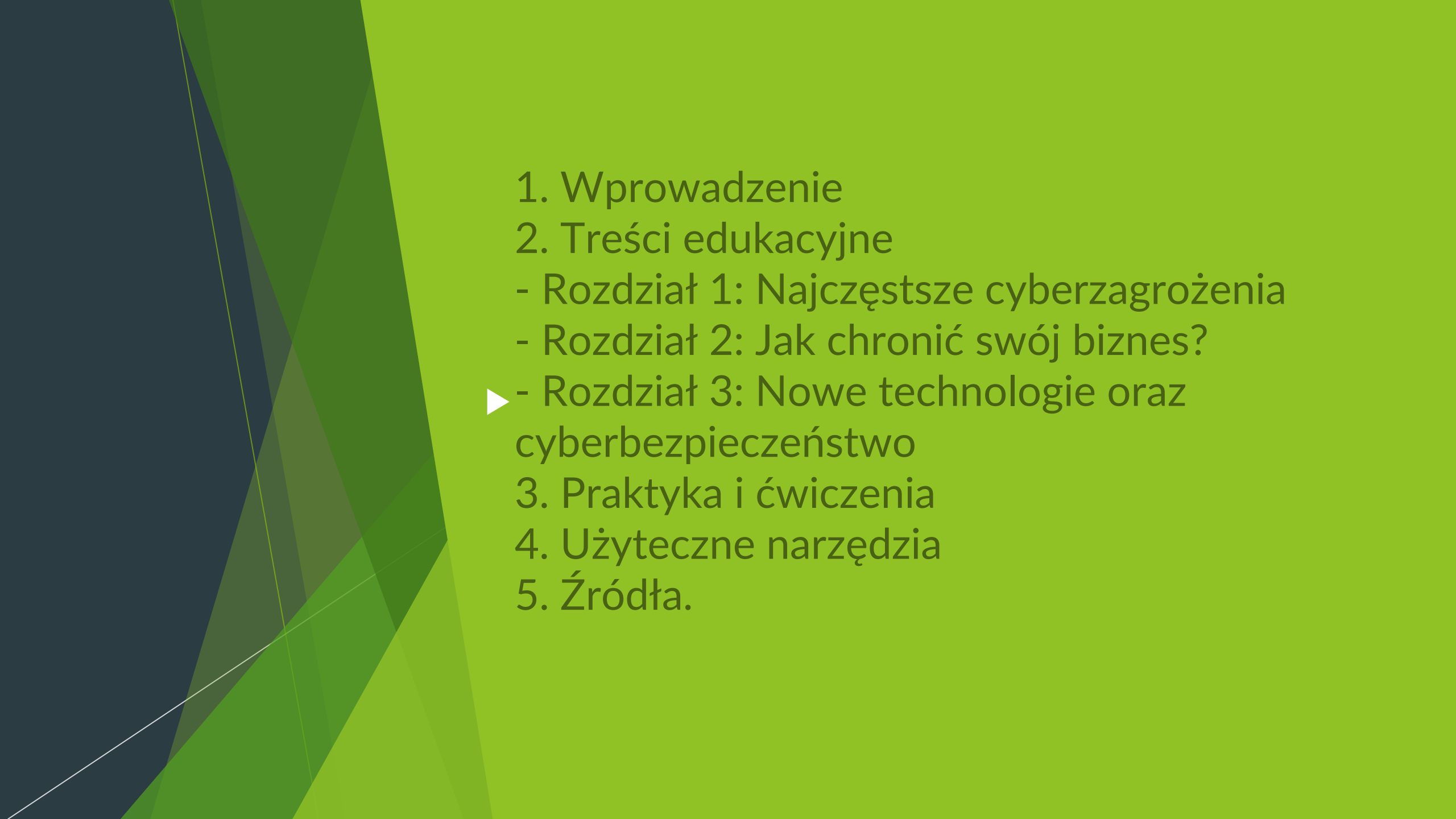
Erasmus+

Projekt finansowany przez:

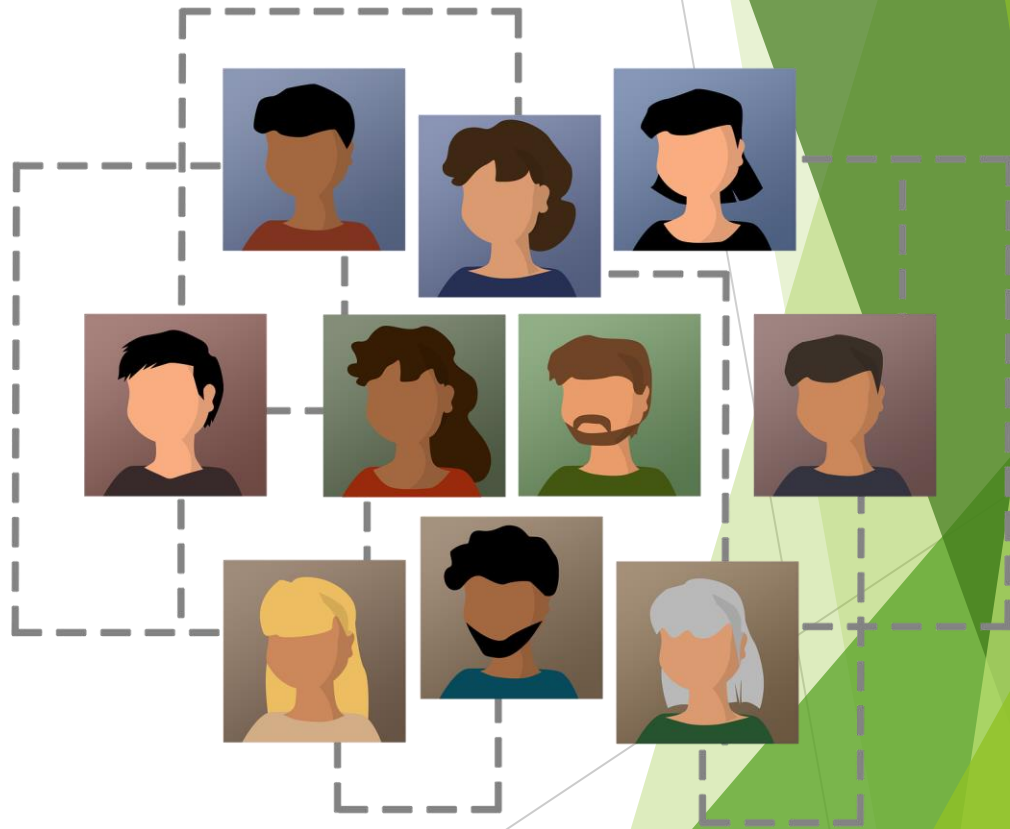
Erasmus+ / Key Action 2 - Współpraca na rzecz innowacji i wymiany dobrych praktyk; Partnerstwa strategiczne na rzecz kształcenia i szkolenia zawodowego.

Strona internetowa projektu Retail: retail.erasmus.site

Poparcie Komisji Europejskiej dla wydania niniejszej publikacji nie stanowi poparcia dla treści, które odzwierciedlają jedynie poglądy autorów i Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

- 
1. Wprowadzenie
 2. Treści edukacyjne
 - Rozdział 1: Najczęstsze cyberzagrożenia
 - Rozdział 2: Jak chronić swój biznes?
 - ▶ - Rozdział 3: Nowe technologie oraz cyberbezpieczeństwo
 3. Praktyka i ćwiczenia
 4. Użyteczne narzędzia
 5. Źródła.

1. Wprowadzenie



Covid-19 zmusił wiele firm do przyspieszenia transformacji cyfrowej. Cyfryzacja może wspierać działalność firmy i umożliwiać jej rozwój w niespotykany dotąd sposób, wspierając jej działalność. Niestety, może też być miejscem cyberataków i kradzieży danych. Dlatego ważne jest, aby przygotować się na taką możliwość i wiedzieć, w jaki sposób możemy prowadzić bezpieczny biznes.

Każda firma musi prowadzić działania dopasowane do jej profilu i poziomu cyfryzacji, ale istnieje kilka wspólnych punktów, na które należy zwrócić uwagę, aby zapewnić cyberbezpieczeństwo firmy.

2. Treść

Ten dodatkowy moduł zostanie podzielony na 3 rozdziały, ćwiczenie praktyczne, odniesienia i dalsze narzędzia.

- Rozdział 1: Najczęstsze cyberzagrożenia.
- Rozdział 2: Jak chronić swój biznes?
- Rozdział 3: Nowe technologie oraz cyberbezpieczeństwo.



2.1. Najczęstsze cyberzagrożenia



TREŚĆ ROZDZIAŁU 1
Najczęstsze cyberzagrożenia

1. Złośliwe oprogramowanie

Malware jest skrótem (anglojęzycznym), od „złośliwego oprogramowania” i może być fragmentem kodu/programem, którego celem jest zakłócanie operacji, kradzież danych lub uszkodzenie sprzętu. Należą do nich popularne trojany, robaki i oprogramowanie szpiegujące.

2. Phishing (Wyłudzanie informacji)

Jest to podszywanie się pod osobę lub instytucję i próba wyłudzenia pieniędzy/danych od użytkownika.

3. „Man-in-the-Middle” (z jęz. ang.)

Haker „wchodzi” między interakcje 2 podmiotów poprzez np. słabo zabezpieczone Wi-Fi z zamiarem wykradzenia informacji, danych osobowych itp.

2.2.1. Jak chronić swój biznes?

Należy zwrócić uwagę na 2 elementy:

Zasoby ludzkie



Statystyki pokazują, że zdecydowana większość cyberzagrożeń wynika ze słabego wykształcenia pracowników i błędów ludzkich.

Sprzęt



Komputery, laptopy, oprogramowanie, oprogramowanie antywirusowe i możliwe bramy wykorzystywane do ataków hakerów.

TREŚĆ RODZIAŁU 2

Jak chronić swój biznes?

Zasoby ludzkie i bezpieczeństwo cybernetyczne

Sprzęt i cyberbezpieczeństwo

Ochrona danych osobowych.

2.2.2.

Zasoby ludzkie i bezpieczeństwo cybernetyczne

Zasoby ludzkie odgrywają kluczową rolę w zapewnieniu bezpieczeństwa cybernetycznego

Szacuje się, że nawet 90% problemów związanych z cyberbezpieczeństwem to wynik błędów ludzkich. Zagrożenia bezpieczeństwa mogą przejawiać się w różnych (potencjalnie niebezpiecznych) zachowaniach, takich jak: podłączanie urządzeń zewnętrznych (takich jak dyski USB), które mogą zawierać niebezpieczne złośliwe oprogramowanie; otwieranie wiadomości e-mail pochodzących z nieznanych źródeł. Istnieje wiele niebezpiecznych praktyk, ale najczęstszym źródłem problemu są luki w edukacji pracowników na temat cyberbezpieczeństwa.

Aby zapewnić bezpieczeństwo MŚP zaleca się:

- stworzenie planu zasad bezpieczeństwa, procedur i środków zaradczych,
- zapewnienie profesjonalnego wprowadzenia pracowników do tematyki cyberbezpieczeństwa oraz demonstracja niebezpiecznych zachowań, których należy unikać.

TREŚĆ RODZIAŁU 2

Jak chronić swój biznes?

Zasoby ludzkie i bezpieczeństwo cybernetyczne

Zasoby i cyberbezpieczeństwo

Ochrona danych osobowych.

2.2.3. Sprzęt i cyberbezpieczeństwo

Zasoby sprzętowe muszą być odpowiednio zabezpieczone, aby chronić dane gromadzone przez firmę

Zapewnienie odpowiedniej ochrony sprzętu przed ewentualnymi cyberatakami jest bardzo ważne. W tym celu dostępne są różne narzędzia. Najbardziej oczywistą ochroną jest posiadanie oprogramowania antywirusowego. Przykład znajdziesz tutaj: <https://www.usnews.com/360-reviews/antivirus>

Zapory są również koniecznością. Chociaż ich skuteczność nie jest już tak wysoka jak kiedyś i „wykwalifikowany” haker może je ominąć, nadal stanowią pierwszą linię obrony i mogą zapobiec nieautoryzowanemu dostępowi do systemu.

Jeśli zdecydujesz się na handel online, oczywiście otwiera to zupełnie nowy zestaw wyzwań związanych z bezpieczeństwem (zwłaszcza dla klientów). Warto zacząć od zadbania o to, aby Twój sklep był odpowiednio zabezpieczony przy pomocy SSL i TLS (technologia odpowiedzialna za szyfrowanie), oraz HTTPS - popularna „kłódka” w pasku adresu strony.

TREŚĆ RODZIAŁU 2

Jak chronić swój biznes?

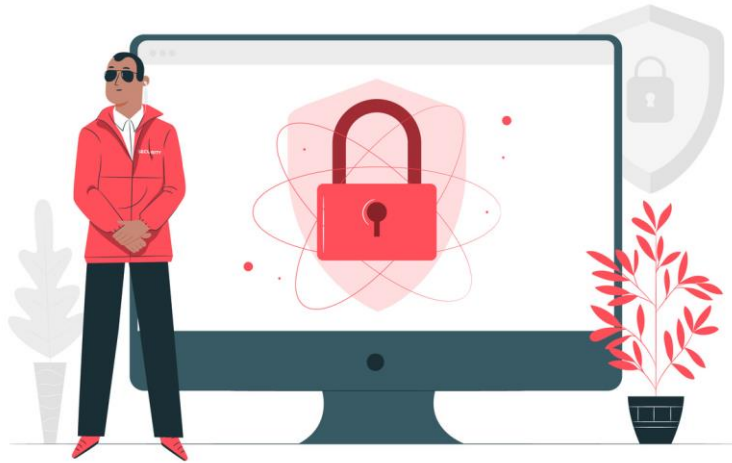
Zasoby ludzkie i bezpieczeństwo cybernetyczne

Zasoby i cyberbezpieczeństwo

Ochrona danych osobowych.

2.2.4. Ochrona danych osobowych

Dbanie o bezpieczeństwo cybernetyczne to również dbanie o dane i informacje, które przechowujesz, w tym o dane osobowe Twoich klientów i pracowników.



TREŚĆ RODZIAŁU 2

Jak chronić swój biznes?

Zasoby ludzkie i bezpieczeństwo cybernetyczne

Zasoby i cyberbezpieczeństwo

Ochrona danych osobowych.

RODO obowiązuje w Unii Europejskiej od 2018 roku (całe rozporządzenie dostępne [tutaj](#)).

Oznacza to, że przechowywanie danych musi być zgodne z określonymi środkami ochrony.

RODO wprowadziło nowe prawa dla obywateli (na przykład „prawo do bycia zapomnianym”) oraz nowe obowiązki dla przedsiębiorstw zarówno w ich stacjonarnej, jak i internetowej działalności. Do takich obowiązków należy np. obowiązek wprowadzenia zasad prywatności na etapie projektowania (np. sklepu). Są to: prywatność w fazie projektowania lub prywatność domyślna (z jęz. ang. *privacy by design*; *privacy by default*).

2.3. Nowe technologie oraz cyberbezpieczeństwo

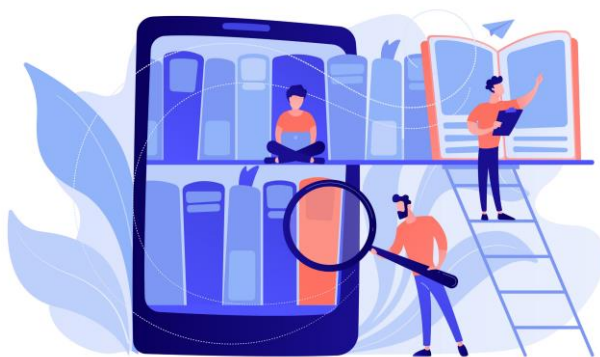


TREŚĆ RODZIAŁU 3
Nowe technologie oraz cyberbezpieczeństwo

Czwarta rewolucja przemysłowa (Przemysł 4.0), wprowadza firmy w nową erę połączonych urządzeń. Chociaż jego pozytywy są liczne, niesie ze sobą również pewne ryzyko, które związane jest z Internetem Rzeczy. Technologia ta w uproszczeniu polega na podłączeniu wielu urządzeń, które mogą wchodzić w interakcje bez udziału człowieka. Wiąże się to z ryzykiem - tak duża liczba połączonych urządzeń (szacuje się, że w 2030 roku będzie ich aż 25,4 mld) będzie bramą dla hakerów, którzy włamując się do mniej bezpiecznych urządzeń, będą mogli uzyskać dostęp do najważniejszych elementów infrastruktury w firmach.

3. Praktyka i ćwiczenia

Zastanów się nad poziomem cyberbezpieczeństwa w Twojej firmie.



1. Jakie szkolenie jest dostępne dla pracowników?
2. Jak możesz poprawić własne kompetencje w zakresie cyberbezpieczeństwa?
3. Czy dane Twoich klientów są dobrze chronione?
4. Czy korzystasz z aktualnego oprogramowania antywirusowego?
5. Czy masz plan na wypadek cyberincydentu?

4. Narzędzia



RODO

Link: <https://gdpr-info.eu/>

Film o cyberbezpieczeństwie

Link: <https://www.youtube.com/watch?v=inWWhr5tnEA>

Cyberbezpieczeństwo dla małych firm

Link: <https://www.fcc.gov/general/cybersecurity-small-business>



5. Źródła

Cyberbezpieczeństwo: najczęstsze typy cyberataków

Link: <https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/>

Dlaczego edukowanie pracowników w zakresie cyberinteligencji i bezpieczeństwa zmniejszy ryzyko:

Link: <https://www.cybintsolutions.com/employee-education-reduces-risk/>

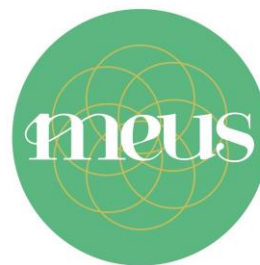
Czym jest RODO? (Wersja polskojęzyczna)

Link: <https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-rodo-i-jakie-zmiany-wprowadza-nowa-ustawa-parlamentu-europejskiego>



PROJEKT RETAIL

Partnerzy



POLISH CHAMBER OF COMMERCE

Strona internetowa projektu Retail: retail.erasmus.site