

Górnośląska Agencja
Przedsiębiorczości
i Rozwoju sp. z o.o.
Wincentego Pola 16
44-100 Gliwice

(+48) 32 339 31 10
gapr@gapr.pl
www.gapr.pl

PROGRAM SZKOLENIA ONLINE Bezpieczny biznes w sieci

15 czerwca 2021, godz. 09:00
Prowadzący szkolenie: Kamil Małolepszy

AGENDA WYDARZENIA

09:00	Start spotkania
09:00 – 09:10	Działalność ośrodka Enterprise Europe Network – najbliższe wydarzenia, możliwość współpracy zagranicznej oraz doradztwo Prowadzenie: Aleksandra Krawucka, menadżer EEN GAPR
09:10 – 10:45	Bezpieczeństwo systemów informatycznych – wprowadzenie. <ul style="list-style-type: none">• Cyberzagrożenia i ataki – wyzwanie XXI wieku;• Możliwe konsekwencje finansowe i prawne ataku dla funkcjonowania organizacji/firmy;• Cyberprzestępstwa – skala zjawiska. Zagrożenia w sieci. <ul style="list-style-type: none">• Typologia ataków oraz ich rodzaje:<ul style="list-style-type: none">○ Ataki wymierzone w infrastrukturę sieciową;○ Ransomware○ Phishing;○ Ataki wykorzystujące luki stron internetowych oraz portali społecznościowych;○ DDoS;○ Ataki ukierunkowane na konkretną osobę/organizację.• Rodzaje szkodliwego oprogramowania;• Czy organizacja/firma jest w stanie w pełni zabezpieczyć się przed atakiem?

Górnośląska Agencja
Przedsiębiorczości
i Rozwoju sp. z o.o.
Wincentego Pola 16
44-100 Gliwice

(+48) 32 339 31 10
gapr@gapr.pl
www.gapr.pl

	<p>Człowiek – najsłabsze ogniwo systemu bezpieczeństwa.</p> <ul style="list-style-type: none"> • Skąd przestępcy czerpią informacje na temat obiektu ataku? • Socjotechnika; • Polityka bezpieczeństwa systemów informatycznych; • Które elementy systemów należy chronić najbardziej?
10:45 – 11:00	Przerwa
11:00 – 12:45	<p>Zasady bezpiecznego korzystania z sieci firmowej.</p> <ul style="list-style-type: none"> • Właściwe zabezpieczenie sieci firmowej; • WiFi – udostępniać czy nie? • Praca zdalna – szanse i zagrożenia; • Jak bezpiecznie korzystać z przeglądarek, bankowości elektronicznej oraz mediów społecznościowych; • Przesyłanie danych ze szczególnym uwzględnieniem dokumentów zawierających dane osobowe i dane poufne; • Chmura – czy jest bezpieczna? • Zasady zabezpieczenia stanowiska komputerowego przez niepowołanym dostępem; • Szyfrowanie danych, backup, odzyskiwanie danych; • Uwierzytelnianie dwuskładnikowe; • Czy korzystanie z pamięci przenośnych jest bezpieczne? <p>Regulamin użytkownika systemu</p> <ul style="list-style-type: none"> • Zasady uwierzytelniania; • Zasady korzystania z zabezpieczeń; • Reagowanie na incydenty; • Monitorowanie pracy użytkownika zgodnie z RODO; <p>Bezpieczeństwo systemów a ochrona danych osobowych RODO</p>
12:45 – 13:00	<p>Sesja pytań i odpowiedzi Podsumowanie szkolenia</p>