PROGRAM BEZPIECZNEGO BIZNESU

strategia cyberbezpieczeństwa

OKREŚLENIE REALNYCH ZAGROŻEŃ

Każda organizacja jest wyjątkowa. Ma swoje zasoby, kadry i okoliczności biznesowe. Wiążą się z tym konkretne zagrożenia i ryzyka.

CEL 1: poznanie firmy i przypisanie zagrożeń

OMÓWIENIE STOSOWANYCH ZABEZPECZEŃ

Organizacja już posiada zabezpieczenia techniczne, procesowe, kolekcję dobrych praktyk.

CEL 2: poznanie stosowanych zabezpieczeń

OBSZARY DO POPRAWY

Znając biznes, zagrożenia, stosowane zabezpieczenia, można wskazać obszary do poprawy. Uwzględniając dobre praktyki i techniczne możliwości można holistycznie wyciągać wnioski.

CEL 3:holistyczne kierunki zmian

PLAN ZMIAN I REALIZACJA

Opracowany plan zmian uwzględnia krytyczność, budżet, możliwości, celowość następnych kroków.

CEL 4: opracowanie planu
CEL 5: realizacja zmian

OD ZROZUMIENIA DO DZIAŁANIA

MAŁYMI KROKAMI

więcej na:
www.cyberkurs.online

602 55 12 85