MONITORING
WYKRYWANIE
REAKCJA
ZAPOBIEGANIE

NEANTIC
CYBER SECURITY

Analiza stanu cyberbezpieczeństwa

Co sprawdzamy:

Cyberbezpieczeństwo to coraz szerszy obszar działania, zarówno dla budujących zabezpieczenia, jak i tych którzy je łamią.
Ataki hakerskie dotyczą firm, instytucji oraz osób prywatnych.
W przypadku przedsiębiorstw zagrożona jest zarówno własność intelektualna, jak i ciągłość procesów produkcyjnych.

Konsekwencją ataku może być: utrata wizerunku, pieniędzy, a w skrajnych przypadkach zdrowia i życia.

Budowanie odporności organizacji, uzyskiwanie świadomości w zakresie cyberbezpieczeństwa to jedne z głównych wyzwań i priorytetów w naszej pracy.

W ramach analizy:
przeprowadzimy analizę stosowanych w firmie rozwiązań teleinformatycznych wpływających na odporność organizacji w zakresie cyberbezpieczeństwa.
Przegląd obejmie: stosowane zabezpieczenia, systemy bezpieczeństwa oraz ich praktyczne wykorzystanie.
Pozwoli to na ocenę zdolności organizacji do przeciwdziałania, wykrywania i reagowania na cyber zagrożenia.

Efekty analizy:
- Kompleksowa analiza stanu cyberbezpieczeństwa firmy
- Raport obszaru technologicznego obejmujący rozwiązania teleinformatyczne, stosowane zabezpieczenia, systemy bezpieczeństwa oraz ich praktyczne wykorzystanie wraz z rekomendacjami,
- Mapa powiązań między usługami kluczowymi/cyfrowymi a infrastrukturą IT,
- Raport z przeprowadzonego badania pozwalający na lepsze dopasowanie do potrzeb organizacji programu świadomości z zakresu cyberbezpieczeństwa.

Korzyści:
- Ograniczenie strat materialnych i intelektualnych.
- Wiedza dająca przewagę i możliwość przeciwdziałania atakom.
- Sukcesywne zwiększanie poziomu świadomości członków organizacji w zakresie cyberbezpieczeństwa.
- Zdolność przeciwdziałania, wykrywania i reagowania na cyber zagrożenia.

Więcej informacji? Napisz: soc@neantic.pl