

Pomieszczenia bezpieczne



BEZPIECZNY SYSTEM TYPU
"POMIESZCZENIE W POMIESZCZENIU"

HPC
HIGH PROTECTION CAGE

www.swisste.ch

HPC

HIGH PROTECTION CAGE

Systemy informatyczne stanowią podstawę bezpiecznego i efektywnego funkcjonowania większości przedsiębiorstw. Błąd lub usterka systemu może prowadzić do poważnych utrudnień w pracy przedsiębiorstwa, lub wręcz uniemożliwić jego dalsze funkcjonowanie. Dzięki High Protection Cage (HPC) możecie Państwo chronić swoją bazę danych przed uszkodzeniami spowodowanymi przez ogień, wodę, niedozwolony dostęp oraz inne potencjalne zagrożenia.

HPC oferuje maksymalną ochronę, co oznacza bezpieczeństwo przedsiębiorstwa.

High Protection Cage (HPC) firmy Swisste.ch gwarantuje najlepsze zabezpieczenie urządzeń IT według najwyższych standardów bezpieczeństwa zgodnych z normą EN 1047-2 wg ECB-S*, spełnia najwyższe normy bezpieczeństwa w zakresie ochrony przeciwpożarowej oraz ochrony przed innymi zagrożeniami, takimi jak nieautoryzowany dostęp, ochrona przed gruzem, kurzem i wodą. W precyzyjnie określonej w normie procedurze testów i certyfikacji są opisane dokładnie warunki badania i wymagane wyniki badań. Ponadto systematyczne kontrole jakości przy produkcji elementów i montażu gwarantują stabilny wysoki poziom jakości.

HPC oferuje najwyższy stopień ochrony, niemożliwy do osiągnięcia przy użyciu klasycznych materiałów.

HPC może być używany wszędzie tam, gdzie są wymagane najlepsze środki ochrony dla serwerowni i centrów obliczeniowych.

CHARAKTERYSTYKA OGÓLNA

Podczas prób wykonanych przez ECB-S wzrost temperatury wewnątrz HPC wyniósł 33 K. Jest to wynik o wiele lepszy od wymaganych 50 K, co pozwala spełnić wymagane warunki z dużym zapasem!

Dla zapewnienia jeszcze większego poziomu bezpieczeństwa HPC zostało poddane dalszym testom i sprawdzianom ponad wymagania normy EN 1047-2.

Zastosowanie

Pomieszczenia HPC powinny znaleźć zastosowanie wszędzie tam, gdzie wymagania dotyczące serwerowni lub centrum obliczeniowego są szczególnie wysokie, oraz gdy nie da się technicznie usunąć zagrożenia pożarowego w ich otoczeniu.

Zalety

Zastosowanie sprawdzonego i certyfikowanego pomieszczenia systemowego zapewnia najwyższy poziom bezpieczeństwa. HPC spełnia również najwyższe wymagania BSI oraz BITKOM.

Cechy

- HPC zapewnia ochronę przed zagrożeniami takimi jak:
 - Ogień
 - Wzrost temperatury
 - Woda
 - Wilgotność
 - Pole elektromagnetyczne
 - Kurz
 - Nieautoryzowany dostęp
 - Obciążenie gruzem
 - Integracja ze strukturą budynku
- Masywna konstrukcja
- Możliwość wybudowania zarówno na parterze jak i na wyższych piętrach
- Integracja ze wszystkimi mediami (klimatyzacja, instalacja elektryczna).



BEZPIECZNY SYSTEM TYPU "POMIESZCZENIE W POMIESZCZENIU"

Zastosowanie HPC jest wskazane w każdym przypadku, gdy w otoczeniu serwerowni lub centrum obliczeniowego potencjalne zagrożenia nie są możliwe do wyeliminowania, np. zwiększone zagrożenie pożarowe ze względu na przylegający do chronionego pomieszczenia magazyn. Ponadto pomieszczenie HPC może zostać zastosowane, gdy dostępna infrastruktura nie zapewnia należytej stabilności i ochrony ogniowej (np. podczas adaptowania przemysłowej hali na potrzeby serwerowni).

Badanie według normy EN 1047-2 różni się znacząco od zwykłych badań materiałów budowlanych. Stąd wynikają późniejsze zalety w zakresie bezpieczeństwa i ochrony wrażliwych systemów informatycznych. Różnice pomiędzy badaniami

- **Badanie pomieszczenia systemowego**
Zamknięty korpus (ściany, sufit, podłoga) włącznie ze wszystkimi komponentami (drzwi, przepusty, zasuwki) umieszczany jest w piecu i poddawany godzinnemu oddziaływaniu ognia.
- **Podczas całego testu (faza płomieniowania i faza chłodzenia) wzrost temperatury w zamkniętym korpusie nie może być większy niż 50 °C / 50 Kelwinów.**
- **Wilgotność powietrza nie może przekroczyć 85%.**
- **Rozgrzane elementy konstrukcyjne po 45 minutach nagrzewania muszą wytrzymać test obciążeniowy (3 uderzenia ciężaru o wadze 200 kg z wysokości 1,5m)**

*European Certification Body GmbH jest neutralną i międzynarodową jednostką certyfikującą wg. Normy EN 4501
www.ecb-s.com

§ Ustawodawstwo zagraniczne i polskie

"Ustawodawcy zobowiązują zarządzających przedsiębiorstwami do ochrony danych oraz ustalają ich odpowiedzialność w przypadku możliwych do uniknięcia szkód w zakresie IT."

- **KonTraG** (Ustawa o kontroli i przejrzystości w firmie) Kierownictwo przedsiębiorstwa musi osobiście ustalić podstawowe zasady polityki korporacji i musi podejmować sprawdzone i udokumentowane decyzje zapewniające bezpieczeństwo przedsiębiorstwu.
- **BSI** (Niemiecki Federalny Urząd ds. Bezpieczeństwa w dziedzinie technologii informatycznych) Zbiór zaleceń w zakresie bezpieczeństwa informatycznego w aspekcie prawnym. Przyjęcie go oznacza zgodność i wprowadzenie określonych zasad bezpieczeństwa informatycznego zgodnie z najnowszą wiedzą techniczną, najnowszymi przepisami np. z normą ISO / IEC 27001 i ISO / IEC 15048.
- **Basel III** – przewodnik dla banków – wprowadzenie standardów bezpieczeństwa poprawiających stan bezpieczeństwa.
- **SOX** (SarbanesOxleyAct) – zasady, obowiązki i zadania osób zarządzających (CTO i CFO) dla przedsiębiorstw w USA notowanych na giełdzie. Na europejskim rynku znane jako EuroSox.
- **GRC** (Governance, Risk and Compliance) wewnętrzne analizy przedsiębiorstwa, zgodnie z którymi niezawodność, sprawdzalność i dokumentacja powinny gwarantować bezpieczeństwo informatyczne.
- **Solvency II** – tak jak Basel II reguluje ryzyko osób zarządzających przedsiębiorstwem w zakresie finansów. Przedsiębiorstwa otoczone są wieloma różnymi zagrożeniami, które muszą zostać opanowane aby bezpiecznie działać na rynku. W obliczu dynamicznych zmian na rynkach finansowych zasady te pozwalają na lepsze zarządzanie ryzykiem przedsiębiorstwa.
- **Bundesdatenschutz** – (Niemieckie prawo ds. ochrony danych osobowych) reguluje sposób ochrony danych osobowych.
- **GIODO** – Generalny Inspektor Ochrony Danych Osobowych reguluje sposób ochrony danych osobowych w Polsce zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).



SZYTE NA MIARĘ, ROZWIĄZANIE DLA TWOJEGO CENTRUM DANYCH

