Checklista cyberbezpieczeństwa dla użytkowników Axence nVision®

Przygotuj organizację na aktualne zagrożenia

Ze względu na wzmożoną aktywność cyberprzestępców oraz trudną sytuację pandemiczną rząd podjął decyzje, które mogą mieć duży wpływ na bezpieczeństwo danych i systemów informatycznych w większości organizacji:

- wprowadzenie pierwszego stopnia alarmowego ALFA-CRP na terenie całego kraju
- nałożenie obowiązku pracy zdalnej na całą administrację publiczną
- zalecenie do przejścia w tryb pracy zdalnej w sektorze prywatnym

Dzięki Axence nVision® będziesz na to przygotowany!

Jeżeli nie posiadasz oprogramowania nVision lub brakuje Ci któregoś z modułów, skontaktuj się z naszym działem sprzedaży:

Email: sprzedaz@axence.net
Telefon: +48 12 426 40 35

Checklista cyberbezpieczeństwa

Zadbaj o bezpieczeństwo swojej organizacji, wprowadzając poniższe zalecenia:

Odpowiedz na pytania, aby ocenić stan faktyczny poprawności wdrożenia oprogramowania Axence nVision®.

	Funkcja	Tak/Nie	Prawidłowa konfiguracja w nVision
1.	Czy w Axence nVision® monitorowane urządzenia sieciowe są właściwe opisane oraz czy są sklasyfikowane pod kątem ważności dla organizacji i jej ciągłości działania?	○ TAK ○ NIE	Zobacz screen Zobacz screen
2.	Czy Axence nVision® ogłosi alarm i wyśle powiadomienia w przypadku niedostępności krytycznych i ważnych urządzeń?	○ TAK ○ NIE	Zobacz screen
3.	Czy Axence nVision® monitoruje obciążenie krytycznych i ważnych urządzeń w obszarze m.in. CPU, RAM?	○ TAK ○ NIE	Zobacz screen Zobacz screen
4.	Czy Axence nVision® ogłosi alarm i wyśle powiadomienie jeżeli parametry wydajnościowe urządzeń krytycznych i ważnych osiągną stan podwyższony?	○ TAK ○ NIE	Zobacz screen Zobacz screen
5.	Czy w ramach całej organizacji wdrożony jest agent Axence nVision®, pozwalający na pełne monitorowanie urządzeń klasy PC (Windows)?	○ TAK ○ NIE	Zobacz screen Zobacz screen
6.	Czy stacje robocze pracowników, szczególnie te wyznaczone do pracy zdalnej (laptopy) posiadają aktualną wersję systemu operacyjnego?	○ TAK ○ NIE	Zobacz screen
7.	Czy stacje robocze pracowników, szczególnie te wyznaczone do pracy zdalnej (laptopy) są chronione wybranym przez organizację programem antywirusowym?	○ TAK ○ NIE	Zobacz screen
8.	Czy stacje robocze pracowników, szczególnie te wyznaczone do pracy zdalnej (laptopy) są zabezpieczone kryptograficznie przed nieuprawnionym dostępem?	○ TAK ○ NIE	Zobacz screen
9.	Czy polityka monitorowania pracy na służbowym sprzęcie jest włączona w zakresie pełnego monitorowania, co przekłada się na należytą staranność i rozliczalność m.in. w zakresie przepisów RODO?	○ TAK ○ NIE	Zobacz screen
10	Czy w obszarze monitorowania pracy na służbowym sprzęcie jest stosowana polityka blokowania stron WWW oparta o listę niebezpiecznych domen CERT.PL?	○ TAK ○ NIE	Zobacz screen
11.	Czy w obszarze monitorowania pracy na służbowym sprzęcie jest stosowana polityka blokowania stron WWW znanych przestrzeni chmurowych, np. Google Drive czy Dropbox?	○ TAK ○ NIE	Zobacz screen
12.	Czy w obszarze monitorowania pracy na służbowym sprzęcie jest stosowana polityka blokowania praw do uruchomienia znanych aplikacji, pozwalających na automatyczne synchronizowanie plików z dyskami chmurowymi, np. Google Drive czy Dropbox?	○ TAK ○ NIE	Zobacz screen
13.	Czy w obszarze monitorowania pracy na służbowym sprzęcie jest stosowana polityka blokowania praw do uruchomienia znanych aplikacji zdalnego dostępu, takich jak m.in. TeamViewer, AnyDesk, VNC?	○ TAK ○ NIE	Zobacz screen
14.	Czy w obszarze monitorowania pracy na służbowym sprzęcie jest stosowana polityka blokowania praw do uruchomienia aplikacji dedykowanych administratorowi, a dostępnych na stacji Windows, np. powershell.exe czy wscript.exe?	○ TAK ○ NIE	Zobacz screen
15.	Czy w obszarze monitorowania pracy na służbowym sprzęcie jest stosowana polityka blokowania praw do uruchomienia aplikacji, które wprost znajdują się w katalogach zalogowanego użytkownika, np. w katalogu pulpit czy pobrane?	○ TAK ○ NIE	Zobacz screen
16.	Czy w obszarze monitorowania pracy na służbowym sprzęcie jest stosowana polityka blokowania ograniczająca prawo pobierania plików o określonych rozszerzeniach, np. bat, exe, ps1 czy msi?	○ TAK ○ NIE	Zobacz screen
17.	Czy w obszarze zarządzania nośnikami zewnętrznymi, np. pendrive została wdrożona polityka kontroli dostępu przez aktywne ograniczenie użycia obcych dla organizacji nośników?	○ TAK ○ NIE	Zobacz screen
18.	Czy w obszarze rozliczania pracownika z operacji na plikach włączono audytowanie tych operacji w kontekście dopuszczonych nośników zewnętrznych, np. pendrive służbowy?	○ TAK ○ NIE	Zobacz screen
19.	Czy w obszarze rozliczania pracownika z operacji na plikach włączono audytowanie tych operacji w obszarze plików zapisanych na stacji roboczej pracownika, np. w obszarze katalogów użytkownika takich jak pulpit, dokumenty czy pobrane?	○ TAK ○ NIE	Zobacz screen