

ZADBAMY O BEZPIECZEŃSTWO TWOICH DANYCH

# AUDYT CYBER BEZPIECZEŃSTWA

Krok po kroku pomagamy Klientom i Partnerom zadbać o bezpieczeństwo IT w organizacji

## AUDYT BEZPIECZEŃSTWA IT

Zapraszamy Cię do udziału w bezpłatnym audycie cyberbezpieczeństwa. Wypełnienie formularza zajmie Ci ok. 2-3 minut. Po wypełnieniu formularza audytowego otrzymasz bezpłatnie raport z wynikami do 3 dni roboczych na wskazany adres mailowy.

Poniżej lista pytań. Wybierz jedną najbardziej pasującą odpowiedź.

### BEZPIECZEŃSTWO DANYCH

1. Czy cyklicznie archiwizujesz i weryfikujesz dane przechowywane na stacjach roboczych, laptopach i sieciowych serwerach?

tak  nie  nie wiem

2. Czy przechowujesz swoje dane w kilku bezpiecznych miejscach (nośnik zewnętrzny, rozwiązanie chmurowe)?

tak  nie  nie wiem

3. Czy w Twojej firmie jest osoba odpowiedzialna za zabezpieczanie danych?

tak  nie  nie wiem

4. Czy Twoje pliki zawierające poufne dane są zaszyfrowane?

tak  nie  nie wiem

### BEZPIECZEŃSTWO SIECI LOKALNEJ

5. Czy dostęp do sieci wifi pokrywa całą firmę/miejsca pracy?

tak  nie  nie wiem

6. Czy korzystasz z zapory sieciowej typu Firewall?

tak  nie  nie wiem

# AUDYT CYBER BEZPIECZEŃSTWA

Krok po kroku pomagamy Klientom i Partnerom zadbać o bezpieczeństwo IT w organizacji

7. Czy goście w Twojej firmie mają dostęp do sieci firmowej WiFi lub LAN?

tak  nie  nie wiem

8. Czy sieć dla gości/użytkowników zewnętrznych jest odizolowana od sieci wewnętrznej?

tak  nie  nie wiem

9. Czy monitorujesz cyklicznie sprawność sprzętu komputerowego oraz sieci?

tak  nie  nie wiem

10. Czy zasoby działów są izolowane w sieci lokalnej?

tak  nie  nie wiem

11. Czy wykonujesz próbne ataki na swoją sieć informatyczną?

tak  nie  nie wiem

12. Czy komputery w Twojej firmie pracują w sieci lokalnej?

tak  nie  nie wiem

## BEZPIECZEŃSTWO SPRZĘTU I OPROGRAMOWANIA

13. Czy regularnie zmieniasz hasła do programów?

tak  nie  nie wiem

14. Czy korzystasz z logowania dwuetapowego?

tak  nie  nie wiem

15. Czy Twoi pracownicy stosują hasła unikalne, silne i skomplikowane?

tak  nie  nie wiem

# AUDYT CYBER BEZPIECZEŃSTWA

Krok po kroku pomagamy Klientom i Partnerom zadbać o bezpieczeństwo IT w organizacji

16. Czy masz firmę lub dział, które zabezpieczają Twoje systemy komputerowe?

tak  nie  nie wiem

17. Czy aktualizujesz systemy operacyjne?

tak  nie  nie wiem

18. Czy powadzisz inwentaryzację sprzętu, który powinien być zabezpieczony przed atakami?

tak  nie  nie wiem

19. Czy firmowy sprzęt komputerowy jest wyłączony poza godzinami pracy?

tak  nie  nie wiem

20. Czy komputery firmowe posiadają aktualne oprogramowanie antywirusowe?

tak  nie  nie wiem

21. Czy w Twojej firmie używane są filtry prywatności na monitor?

tak  nie  nie wiem

22. Czy zasilanie awaryjne sprzętu wystarcza na min. 15 minut pracy?

tak  nie  nie wiem

## BEZPIECZEŃSTWO W INTERECIE

23. Czy w Twojej firmie są wdrożone procedury dotyczące bezpiecznego użytkowania Internetu?

tak  nie  nie wiem

24. Czy służbowe urządzenia mobilne w Twojej firmie są zabezpieczone przed atakami?

tak  nie  nie wiem

25. Czy prowadzisz raport incydentów związanych z naruszeniem cyberbezpieczeństwa?

tak  nie  nie wiem

# AUDYT CYBER BEZPIECZEŃSTWA

Krok po kroku pomagamy Klientom i Partnerom zadbać o bezpieczeństwo IT w organizacji

26. Czy pracownicy mają ograniczony dostęp do prywatnych social mediów?

tak  nie  nie wiem

27. Czy firmowa strona i/lub sklep internetowy są na bieżąco aktualizowane?

tak  nie  nie wiem

28. Czy wtyczki do strony i/lub sklepu internetowego są na bieżąco aktualizowane?

tak  nie  nie wiem

## BEZPIECZEŃSTWO UŻYTKOWNIKÓW

29. Czy pracownicy mają dostęp tylko do potrzebnych im aplikacji?

tak  nie  nie wiem

30. Czy w Twojej firmie odbywają się cyklicznie szkolenia dla pracowników dotyczące cyberbezpieczeństwa?

tak  nie  nie wiem

31. Czy pracownicy w Twojej firmie wiedzą, co robić w przypadku wystąpienia cyberataku?

tak  nie  nie wiem

32. Czy kontrolujesz aktywność pracowników w Internecie w czasie pracy?

tak  nie  nie wiem

## BEZPIECZEŃSTWO POMIESZCZEŃ

33. Czy zabezpieczasz dostęp do pomieszczeń, w których znajdują się dane wrażliwe, poufne?

tak  nie  nie wiem

34. Czy posiadasz monitoring budynku?

tak  nie  nie wiem

ZADBAMY O BEZPIECZEŃSTWO TWOICH DANYCH

# AUDYT CYBER BEZPIECZEŃSTWA

Krok po kroku pomagamy Klientom i Partnerom zadbać o bezpieczeństwo IT w organizacji

35. Czy nagrania z monitoringu są archiwizowane przez min. 30 dni?

tak  nie  nie wiem

36. Czy kamery umożliwiają identyfikację osób i obiektów?

tak  nie  nie wiem

37. Czy system alarmowy powiadamia Cię bezzwłocznie o intruzie?

tak  nie  nie wiem

## BEZPIECZEŃSTWO PRACY ZDALNEJ

38. Czy pracujący poza siecią firmy łączą się przez VPN?

tak  nie  nie wiem

39. Czy podpisy kwalifikowane znajdują się w miejscu chronionym?

tak  nie  nie wiem

## BEZPIECZEŃSTWO POCZTY MAILOWEJ

40. Czy skrzynki mailowe posiadają filtry antyspamowe?

tak  nie  nie wiem

41. Czy skrzynki mailowe posiadają zabezpieczenia antyphishingowe?

tak  nie  nie wiem

ZADBAMY O BEZPIECZEŃSTWO TWOICH DANYCH

# AUDYT CYBER BEZPIECZEŃSTWA

Krok po kroku pomagamy Klientom i Partnerom zadbać o bezpieczeństwo IT w organizacji

Zostaw dane, na które wyślemy wynik audytu.

Imię \*

Adres mailowy \*

Nazwa organizacji

Adres strony internetowej lub sklepu internetowego

Akceptuję [Politykę prywatności](#).

Wyrażam zgodę na przesłanie wyników audytu na podany adres mailowy.