

WNIOSEK O UBEZPIECZENIE RYZYK CYBERNETYCZNYCH

(wymagania i potrzeby klienta, opis ryzyka)

dane

Dane klienta

(nazwa, adres, NIP, REGON)

opis

Branża działalności (opis)

kwota w zł

Wysokość rocznych obrotów

Zakres ubezpieczenia, limity odpowiedzialności

500 000 zł

Ubezpieczenie danych elektronicznych

100 000 zł

Ubezpieczenie kosztów uniknięcia lub zmniejszenia skutków ataku komputerowego

500 000 zł

Ubezpieczenie odpowiedzialności cywilnej

kwota w zł

Ubezpieczenie utraty zysku

w tym:

[x]  koszty okupu

[x]  kary i grzywny nałożone na Ubezpieczonego przez organy regulacyjne i administracyjne bezpośrednio w wyniku zajścia zdarzenia ubezpieczeniowego

[x]  uszkodzenie lub zniszczenie sprzętu elektronicznego spowodowane atakiem komputerowym

[x]  odpowiedzialność cywilna za postępowania i kary administracyjne osób trzecich

Informacje ogólne

A.1. Stopień zależności firmy od ciągłości działania środowiska teleinformatycznego:

[ ]  duża zależność – przerwa trwająca poniżej 24 godzin miałaby znaczący wpływ na działalność

[ ]  średnia zależność – przerwa trwająca więcej niż 24 godziny, ale mniej niż 48 godzin miałaby znaczący wpływ na działalność

[ ]  mała zależność – przerwa trwająca ponad 48 godzin miałaby znaczący wpływ

A.2. Szacunkowa liczba użytkowników wszystkich systemów teleinformatycznych

[ ]  1-25

[ ]  26 -100

[ ]  ponad 100

A.3. Szacunkowa, całkowita pojemność pamięci masowej dla serwerów i komputerów

pojemność w TB

A.4.

Czy firma posiada narzędzia teleinformatyczne (własne lub outsourcing), które pozwolą stwierdzić, że doszło

do naruszenia środowiska teleinformatycznego?

[ ]  tak [ ]  nie

Jeśli tak, jakie

opis

Przetwarzanie danych

B.1. Czy firma spełnia wymogi ustawy o ochronie danych osobowych?

[ ]  tak [ ]  nie

B.2. Czy wyznaczono osobę lub podmiot odpowiedzialny za bezpieczeństwo teleinformatyczne firmy (w tym

bezpieczeństwa informacji)?

[ ]  brak wyznaczonej osoby/podmiotu

[ ]  wyznaczono osobę/podmiot, ale nie zdefiniowano jej obowiązków i pełnomocnictw\*

[ ]  obowiązki i pełnomocnictwa osoby/podmiotu odpowiedzialnej zostały zdefiniowane\*

\* kto jest odpowiedzialnych za bezpieczeństwo teleinformatyczne (w tym informacji)

stanowisko lub nazwa podmiotu

– stanowisko lub nazwa podmiotu:

B.3. Liczba rekordów danych osobowych przetwarzanych w ramach prowadzonej działalności (klienci, pracownicy, etc.)

łącznie

Łącznie

B.4. Rodzaj przechowywanych danych osobowych

Informacje handlowe [ ]  tak [ ]  nie

opis

opis typów informacji handlowych

Informacje o stanie zdrowia [ ]  tak [ ]  nie

opis grupy

jakiej grupy dotyczą

Informacje o płatnościach (karty płatnicze, transakcje) [ ]  tak [ ]  nie

inne

Inne, jakie

B.5. Czy stworzona jest polityka ochrony danych osobowych/bezpieczeństwa informacji?

[ ]  tak [ ]  nie

B.6. Czy pracownicy są przeszkoleni w zakresie polityki ochrony danych osobowych/bezpieczeństwa informacji?

[ ]  tak [ ]  nie

B.7. Czy polityka danych osobowych jest weryfikowana pod kątem zgodności z obowiązującymi przepisami prawa?

[ ]  tak [ ]  nie

B.8. Czy firma posiada plan działania w przypadku wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych?

[ ]  tak [ ]  nie

B.9. Czy dostęp do danych osobowych posiadają wyłącznie pracownicy, którzy takiego dostępu potrzebują?

[ ]  tak [ ]  nie

B.10. Czy dane osobowe są w odpowiedni sposób szyfrowane podczas ich przetwarzania?

[ ]  tak [ ]  nie

B.11. Czy firma przetwarza dane za pośrednictwem chmury obliczeniowej? Kto jest dostawcą usług chmurowych?

dostawca usługi

[ ]  tak [ ]  nie

B.12. Czy w firmie funkcjonuje klasyfikacja informacji?

[ ]  tak [ ]  nie

Zabezpieczenia Organizacyjne

C.1. Czy pracownicy biorą udział w szkoleniach dotyczących zagrożeń teleinformatycznych?

[ ]  tak [ ]  nie

C.2.1. Polityka bezpieczeństwa teleinformatycznego

[ ]  brak polityki bezpieczeństwa teleinformatycznego

[ ]  istnieją wytyczne w zakresie bezpieczeństwa teleinformatycznego, ale nie zostały spisane w formalnym dokumencie

[ ]  istnieje formalny dokument polityki bezpieczeństwa teleinformatycznego\*

[ ]  brak cyklicznych przeglądów/kontroli polityki bezpieczeństwa

[ ]  przeglądy/kontrole przeprowadzane są nieregularnie

[ ]  przeglądy/kontrole przeprowadzane są regularnie

\*Zgodnie z jakim standardem opracowany

opis

C.2.2. Czy przeprowadzono audyt bezpieczeństwa teleinformatycznego?

[ ]  nie przeprowadzono audytu

norma/standard

[ ]  tak, zgodnie z normą/standardem:

Data ostatniego audytu:

data

Czy wdrożono rekomendacje z audytu?

[ ]  tak [ ]  nie

C.3.1. Polityka bezpieczeństwa w relacjach z podmiotami zewnętrznymi (dostawcy, kooperanci), w tym dostęp

do systemów informatycznych

[ ]  brak wytycznych w zakresie bezpieczeństwa teleinformatycznego w relacjach z podmiotami zewnętrznymi

[ ]  wymagania dotyczące bezpieczeństwa teleinformatycznego są nieformalnie przekazywane podmiotom zewnętrznym

[ ]  wymagania dotyczące bezpieczeństwa teleinformatycznego są formalnie/pisemnie przekazywane podmiotom zewnętrznym

C.3.2. Czy zewnętrzni partnerzy handlowi, klienci bądź dostawcy mają dostęp do systemów informatycznych firmy?

[ ]  tak [ ]  nie

Jeżeli tak, jaki

opis

Zabezpieczenia techniczne

D.1. Sieć teleinformatyczna / *ICT network*

D.1.1

Czy firma stosuje mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci wewnętrznej (LAN) i/

lub zewnętrznej (Internet)?

[ ]  tak [ ]  nie

 Jeśli tak, jakie

opis

D.1.2. Czy zastosowano ochronę sieci z podziałem na Vlany?

[ ]  tak [ ]  nie

D.1.3. Zdalny dostęp do środowiska teleinformatycznego firmy (jeśli dotyczy)

[ ]  brak mechanizmów kontroli połączeń zewnętrznych

[ ]  dozwolony jest dostęp bez uwierzytelniania

[ ]  dostęp jest dozwolony wyłącznie po uwierzytelnieniu (login, hasło)

[ ]  wykorzystywana jest dwuskładnikowa metoda

opis

D.1.4 Czy stosowany jest mechanizm blokowania dostępu do wybranych stron internetowych?

[ ]  tak [ ]  nie

D.1.5. Czy systemy operacyjne, serwery i sieci wewnętrzne podłączone są do sieci publicznych?

[ ]  tak [ ]  nie

D.1.6 Czy firma używa zapór sieciowych (firewall)?

[ ]  tak [ ]  nie

D.2.1. Proszę wymienić rodzaje aktualnie wykorzystywanych systemów operacyjnych (system wraz z jego wersją)

a) serwery

nazwy systemów

b) komputery

nazwy systemów

c) telefony

 nazwy systemów

D.2.2. Czy systemy operacyjne / oprogramowanie występujące w firmie są powszechnie dostępne?

[ ]  tak [ ]  nie

opis

D.2.3. Polityka instalowania aktualizacji oraz poprawek do systemów operacyjnych i oprogramowania

[ ]  brak procesu aktualizacji oprogramowania

[ ]  istnieje nieformalny proces aktualizacji oprogramowania

[ ]  poprawki i aktualizacje są instalowanie automatycznie

[ ]  stosowany jest nadzór techniczny pozwalający ocenić ryzyko implementacji poprawek i aktualizacji

[ ]  instalowane są poprawki i aktualizacje do systemów operacyjnych i oprogramowania

D.2.4. Ochrona przed złośliwym oprogramowaniem (keyloggery, wirusy, trojany itp.)

[ ]  nie stosuje się zabezpieczeń antywirusowych na stacjach roboczych oraz serwerach

[ ]  na wszystkich komputerach i serwerach są zainstalowane zabezpieczenia antywirusowe

[ ]  na wszystkich komputerach i serwerach są zainstalowane zabezpieczenia antywirusowe, które są regularnie

 aktualizowane

Inne, jakie

opis

D.2.5. Kopia zapasowa danych

[ ]  kopie zapasowe nie są wykonywane

[ ]  kopie zapasowe wykonywane są dla wybranych zasobów informacyjnych firmy

[ ]  kopie zapasowe wykonywane są dla wszystkich zasobów informacyjnych firmy

D.2.6. Jak często wykonywana jest kopia zapasowa

opis

D.2.7. Czy są procedury wykonywania kopii zapasowych danych?

[ ]  tak [ ]  nie

D.2.8. Czy kopie zapasowe danych są testowane pod względem poprawności odtworzenia?

[ ]  tak [ ]  nie

D.2.9. W jaki sposób chroni się nośniki zawierające kopie zapasowe danych?

opis

D.2.10. Czy przedsiębiorstwo wykorzystuje outsourcing usług teleinformatycznych?

[ ]  tak [ ]  nie

Jeśli tak, jakich usług

opis

D.2.11. Czy użytkownicy posiadają prawa administratora lokalnego na swoich komputerach?

[ ]  tak [ ]  nie

D.2.12. Proszę wskazać stan procesów zarządzania zabezpieczeniami stosowanymi obecnie korzystając z poniższych ocen. W kolumnie obok nazwy procesu należy wpisać odpowiednią liczbę (1-5)\* poniżej opis:

ocena

opis

Rejestrowanie użytkowników

Uwagi:

ocena

Usuwanie użytkowników

opis

Uwagi:

ocena

Automatyczne wylogowanie

opis

Uwagi:

ocena

Zarządzanie hasłami

opis

Uwagi:

ocena

Uprawnienia kontroli dostępu

opis

Uwagi:

ocena

Tworzenie kopii zapasowych

opis

Uwagi:

Przechowywanie kopii zapasowych

ocena

poza przedsiębiorstwem

opis

Uwagi:

ocena

Wykrywanie włamań

opis

Uwagi:

ocena

Testowanie odtwarzania danych

opis

Uwagi:

\*Ocena (1-5)

1 – Brak procesów

2 – Istnieje proces nieformalny

3 – Istnieje formalny, udokumentowany proces

4 – Istnieje formalny, udokumentowany proces oraz mierzone są najważniejsze wskaźniki efektywności procesu

5 – Istnieje formalny, udokumentowany proces, mierzone są najważniejsze parametry, a ponadto proces jest stale doskonalony na podstawie wyników pomiarów

Bezpieczeństwo fizyczne i środowiskowe

E.1. Czy stosowane są jakiekolwiek zabezpieczenia fizyczne pomieszczeń, w których znajduje się sprzęt teleinformatyczny?

[ ]  nie stosuje się zabezpieczeń fizycznych pomieszczeń

[ ]  tak (wymienić jakie)

opis

Zarządzanie Ryzykiem

F.1.1. Czy dotychczas dochodziło do incydentów związanych z bezpieczeństwem sieci i danych?

[ ]  tak [ ]  nie

Jeśli tak, jakie

opis

Jeśli tak, to jakie działania podjęto:

opis

F.2.1. Czy w firmie wdrożone i stosowane są plany ciągłości działania (BCP) na wypadek ataku komputerowego?

[ ]  tak [ ]  nie

F.2.2. Czy w firmie wdrożone i stosowane są procedury odtworzenia kluczowych zasobów informatycznych

firmy (DRP)?

[ ]  tak [ ]  nie

opis

Informacje dotyczące przetwarzania danych osobowych

Dane podane we wniosku, w tym dane osobowe są przetwarzane przez naszą spółkę dla wykonania usługi oraz przekazywane zakładom ubezpieczeń w celu przygotowania oferty i umowy ubezpieczenia.

Administratorem danych osobowych które otrzymujemy w związku ze świadczeniem usług w ramach współpracy z klientem jest Noble&David sp. z o.o. (ul. Tartaczna 3/47, 80-839 Gdańsk, biuro@nobledavid.pl), z którym możesz kontaktować się we wszystkich sprawach dotyczących ochrony Twoich danych.

Przekazanie nam danych osobowych jest dobrowolne, jednak ich niepodanie uniemożliwi nam wykonanie usługi.

Dane przetwarzamy przez okres nie dłuższy, niż jest to niezbędne do realizacji celu dla którego dane te są przetwarzane, w szczególnych przypadkach dane będą przechowywane na podstawie prawnie uzasadnionego naszego interesu do końca okresu przedawnienia przysługujących Tobie roszczeń.

Osoby, których dane osobowe występują we wniosku mają szereg uprawnień, z jakich mogą skorzystać w związku z przetwarzaniem przez nas danych osobowych:
prawo do uzyskania większej liczby szczegółów na temat sposobu, w jaki przetwarzamy dane osobowe,
prawo dostępu do swoich danych oraz otrzymania ich kopii,
prawo do sprostowania (poprawiania) swoich danych,
prawo do usunięcia danych,
prawo do ograniczenia przetwarzania danych,
prawo do wniesienia sprzeciwu wobec przetwarzania danych,
prawo do przenoszenia danych,

prawo do wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych.
Prawa te podlegają pewnym wyłączeniom w celu ochrony interesu publicznego i naszych interesów.

Polityka ochrony danych osobowych opisana jest i publicznie dostępna na stronie internetowej Noble&David sp. z o.o. [www.nobledavid.pl](http://www.nobledavid.pl) (zakładka Polityka prywatności).

[ ]  oświadczam, że zapoznałem się z zasadami przetwarzanie moich danych osobowych opisany wyżej w części „Informacje dotyczące przetwarzania danych osobowych”

[ ]  wyrażam zgodę na przetwarzanie moich danych osobowych w sposób opisany wyżej w części „Informacje dotyczące przetwarzania danych osobowych”

[ ]  wyrażam zgodę na składanie przez Noble&David sp. z o.o. oświadczeń i przekazywanie informacji związanych ze świadczoną usługą przy użyciu telefonu lub innego telekomunikacyjnego urządzenia końcowego jak również na podany adres poczty elektronicznej, zgoda może być cofnięta w każdym czasie, bez podawania przyczyny

Osoba wypełniająca kwestionariusz

imię i nazwisko

Imię i nazwisko:

stanowisko

Stanowisko:

miejsce

Miejsce:

Data: data