MIĘDZYGMINNY KOMPLEKS UNIESZKODLIWIANIA ODPADÓW
PRONATURA SP. Z O. O.
adres: ul. Ernsta Petersona 22, 85-862 Bydgoszcz
www.pronatura.bydgoszcz.pl

z myślą o ekologii

Bydgoszcz, dnia 15 lutego 2022r.

L.dz. GZ/MN/492/2022

Sprawa: Ubezpieczenie ryzyk cybernetycznych _nr MKUO ProNatura ZP/TP/8/22

Zgodnie z art. 284 ust. 2 ustawy Prawo zamówień publicznych (t. jedn. Dz.U. 2021r., poz. 1129 ze zm.)
Zamawiający udziela poniższych wyjaśnień:

1. Czy kopia zapasowa danych jest przechowywana offline w środowisku oddzielonym od sieci i testowana pod kątem integralności co najmniej raz na 180 dni?
2. Czy włączyliście Państwo Remote Desktop Protocol (RDP) [protokół zdalnego pulpitu] na wszystkich punktach końcowych sieci, w tym na serwerach, gdzie RDP nie jest wymagany?
3. Czy wszystkie dane osobowe są zaszyfrowane w sieci i podczas transmisji z sieci? Jeżeli nie, proszę podać informacje dotyczące Danych Osobowych, które nie są zaszyfrowane i co Ubezpieczony robi, aby ograniczyć to narażenie.
4. Czy zabezpieczacie Państwo zdalny dostęp do swojej sieci i danych osobowych za pomocą co najmniej dwuskładnikowego uwierzytelniania? Jeżeli nie, proszę podać dane dotyczące środowisk sieci Ubezpieczonego i danych osobowych, które są zdalnie dostępne, które nie mają bezpiecznych połączeń i co Ubezpieczony robi, aby zmniejszyć to narażenie.
5. Czy ponieśli Państwo jakąkolwiek szkodę lub czy zgłoszono wobec Państwa jakiekolwiek roszczenie lub czy wiedzą Państwo o jakiejkolwiek sprawie, która z dużym prawdopodobieństwem może spowodować jakąkolwiek szkodę lub roszczenie, w przypadku których mogliby Państwo ubiegać się o odszkodowanie z naszej polisy ubezpieczenia cybernetycznego?
6. Czy firma zabezpiecza zdalny dostęp do sieci oraz danych za pomocą co najmniej dwupoziomowego uwierzytelnienia?
7. Czy firma posiada zabezpieczenia w postaci antywirusa i zapory w całej sieci, w tym na urządzeniach przenośnych?
8. Jak często aktualizowane są sygnatury wirusów?
9. Czy firma szyfruje wszystkie wrażliwe dane, gdy dane te są:
   - Przenoszone?
   - Przechowywane na serwerach?
   - Przechowywane w urządzeniach przenośnych?
10. Jak często firma przeprowadza zewnętrzny audyt bezpieczeństwa?
11. Kto jest odpowiedzialny za zachowanie bezpieczeństwa sieci?
12. Jak często przeprowadzane są istotne aktualizacje?
13. Czy firma wdrożyła politykę audytowania i zarządzania kontami użytkowników?
14. Czy firma wymaga zmiany haseł co najmniej raz na trzy miesiące?
15. Czy dostęp do wrażliwych danych jest ograniczony zgodnie z wymogami użytkownika?
16. Jak często firma dokonuje przeglądu polityki bezpieczeństwa informacji?

17. Czy firma posiada spisany plan zachowania ciągłości działalności, który jest poddawany corocznemu przeglądowi?
18. Czy plan zachowania ciągłości działalności firmy uwzględnia ocenę zagrożeń w cyberprzestrzeni?
19. Zależność sieciowa – po jakim czasie utrata połączenia z siecią zacznie oddziaływać na działalność?
20. Jak długo zajmie pełne odzyskanie kluczowych systemów?/
21. Czy firma dokonuje corocznych testów DRP (usuwania skutków awarii)/BCP (ciągłości biznesowej)?
22. Czy firma (lub partner zewnętrzny/dostawca usług w chmurze) dokonała konfiguracji sieci w celu: Zapewnienia wysokiej dostępności lub przejmowania funkcji przez system rezerwowy w odniesieniu do strony internetowej i innych istotnych aplikacji?
23. Czy firma tworzy kopię zapasową istotnych danych co najmniej raz na 5 dni?
24. Jak często przeprowadzane są testy integralności danych?
    Odpowiedzi od 1 do 24 mają charakter poufny, w tym zawierają informacje stanowiące tajemnicę przedsiębiorstwa. Zamawiający informuje, iż zostały one przekazane bezpośrednio do Pytającego po uzyskaniu zobowiązania do zachowania poufności.
25. Prosimy o zmianę terminu składania ofert na 17.02.2022 bądź wskazanie innego terminu możliwego do akceptacji przez zamawiającego.
    Odpowiedź: Zamawiający w dniu 10.02.2022r. zmienił termin składania ofert na 17.02.2022r. o czym poinformował wszystkich zainteresowanych przedmiotowym postępowaniem, zamieszczając informację na stronie prowadzonego postępowania.
26. W celu przygotowania oferty ubezpieczenia ryzyk cybernetycznych, proszę o wypełnienie wniosku. Jest on niezbędny do przedstawienia oferty. Wniosek dotyczy ubezpieczenia od ryzyk cybernetycznych i tu chciałbym zwrócić szczególną uwagę na zakres ubezpieczenia.
    Nie będzie odpowiedzialności z tytułu STRATY FINANSOWEJ. Czyli jeśli otrzymacie Państwo maila z np. prośbą o opłacenie faktury i zostanie kliknięty link co spowoduje przejęcie konta przez oszustów w konsekwencji dojdzie do utraty środków - towarzystwo ubezpieczeniowe nie odpowie za taki rodzaj ataku. Aby był pełen zakres odpowiedzialności proponuję ubezpieczyć firmę od ognia (minimalna suma ubezpieczenia) i dołożyć klauzulę cybernetyczną to w takiej konfiguracji odpowiedzialność za ww. atak cybernetyczny będzie.
    Odpowiedź: Wniosek zostanie uzupełniony po wyborze oferty najkorzystniejszej, przed podpisaniem umowy. Zakres ubezpieczenia zgodnie z opublikowanymi zapisami SWZ.

Zatwierdzono:
/-/Konrad Mikołajski- Prezes Zarządu
/-/Jarosław Bańkowski- Wiceprezes Zarządu