Instrukcja do formularza oceny ryzyka cyber

Pyt. 1 (Zdalny dostęp do Systemu informatycznego Ubezpieczonego wymaga wieloetapowego uwierzytelnienia) i pyt. 3 (Dostęp do oprogramowania Microsoft o365 wykorzystywany przez Ubezpieczonego wymaga wieloetapowego uwierzytelnienia) W odniesieniu do wymogu wieloetapowego uwierzytelniania , Leadenhall wskazuje na przykłady darmowo dostępnych materiałów szkoleniowych w zakresie wdrażania wieloskładnikowego uwierzytelniania użytkownika:

https://support.microsoft.com/pl-pl/office/konfigurowanie-logowania-do-platformy-microsoft-365-w-zakresie-uwierzytelniania-wieloskładnikowego-ace1d096-61e5-449b-a875-58eb3d74de14

https://seqred.pl/jak-wlaczyc-uwierzytelnianie-wieloskladnikowe-w-office-365/

Pyt. 6 Wdrożone są procedury: procedura aktualizacji oprogramowania wykorzystywanego przez Ubezpieczonego oraz procedury kontroli dostępu i wykorzystania systemu informatycznego. Powyższe procedury powinny uwzględniać regularne aktualizowanie wykorzystywanego przez Ubezpieczonego oprogramowania zgodnie z zaleceniami producenta, kontrolę dostępu do systemu komputerowego Ubezpieczonego i kontrolę wykorzystywania go przez uprawnione osoby, a także procedurę zabezpieczenia przed nieuprawnionym do niego dostępem

Wzór przykładowej procedury w załączeniu.

Pyt. 10 Ubezpieczony potwierdza i zapewnia, że jeżeli on sam lub jego dostawca usług informatycznych korzysta z niewspieranego przez producenta oprogramowania, jest ono odseparowane od reszty sieci informatycznej

W przypadku odpowiedzi twierdzącej, zastosowanie ma dodatkowe wyłączenie: Ubezpieczyciel nie będzie obowiązany do jakiegokolwiek Odszkodowania będącego następstwem Roszczenia opartego na, bezpośrednio lub pośrednio wynikającego z, albo, które może być przypisane lub w jakikolwiek sposób powiązane z funkcjonowaniem jakiegokolwiek oprogramowania, które nie jest wspierane przez jego producenta lub dostawcę. Przez oprogramowanie, które nie jest wspierane należy rozumieć brak zobowiązania producenta lub dostawcy oprogramowania do wykrywania jego podatności oraz zapewniania aktualizacji oprogramowania w celu usuwania podatności, jego naprawy lub ulepszania.

Pyt. 11 Pracownicy Ubezpieczonego (oraz sam ubezpieczony) są regularnie, przynajmniej raz do roku, szkoleni z zakresu zagrożeń teleinformatycznych (w tym tzw. phishingu).

Leadenhall wskazał, iż wystarczające jest przeprowadzanie przynajmniej raz do roku takiego szkolenia przez osobę z adekwatnym doświadczeniem – może to być tak podmiot zewnętrzny, jak i osoba zatrudniona przez ubezpieczonego. Dowodem na przeprowadzenie takiego szkolenia może być np. faktura za wykonanie takiej usługi na rzecz ubezpieczonego, certyfikat wystawiony wewnętrznie itp.

Jednocześnie Leadenhall wskazał na możliwość skontaktowania z zewnętrznym ekspertem prowadzącym tego typu szkolenia na zasadach komercyjnych.

Pyt. 13 Istnieje pisemna procedura szyfrowania danych osobowych i poufnych przechowywanych na mobilnych urządzeniach i nośnikach i wynoszonych poza siedzibę Ubezpieczonego.

Wzór przykładowej procedury przekazujemy w załączeniu.

W przypadku odpowiedzi negatywnej, zastosowanie ma dodatkowe wyłączenie: W uzupełnieniu wyłączeń określonych w par. 20 warunków ubezpieczenia ochrona ubezpieczeniowa nie obejmuje jakichkolwiek Szkód, kosztów lub strat spowodowanych jakimkolwiek Roszczeniem, ani jakichkolwiek Kosztów zarządzania kryzysowego, Kosztów reakcji lub innych kwot wynikających z lub spowodowanych, bezpośrednio lub pośrednio, przez utratę, zniszczenie, uszkodzenie lub kradzież jakichkolwiek Urządzeń przenośnych, chyba że dane na nich zapisane były zaszyfrowane. Przez Urządzenia przenośne należy rozumieć laptopy, palmtopy, tablety, telefony komórkowe i smartfony, nośniki pamięci masowej oraz jakiekolwiek inne urządzenia przenośne, na których można zapisać dane.

Pyt. 14 Istnieje pisemny plan przywrócenia (Disaster Recovery Plan) lub zapewnienia ciągłości działalności w wypadku nieprzewidzianych zdarzeń (Business Continuity Plan), w tym zakłóceń pracy sieci, cyber ataku.

Wytyczne jakiego rodzaju obszary powinien obejmować wskazany plan przywrócenia (Disaster Recovery Plan) przedstawione w załączniku.

W przypadku odpowiedzi negatywnej Leadenhall nie oferuje ochrony w zakresie klauzuli G dotyczącej Kosztów Odtworzenia Danych oraz Cyber BI.”