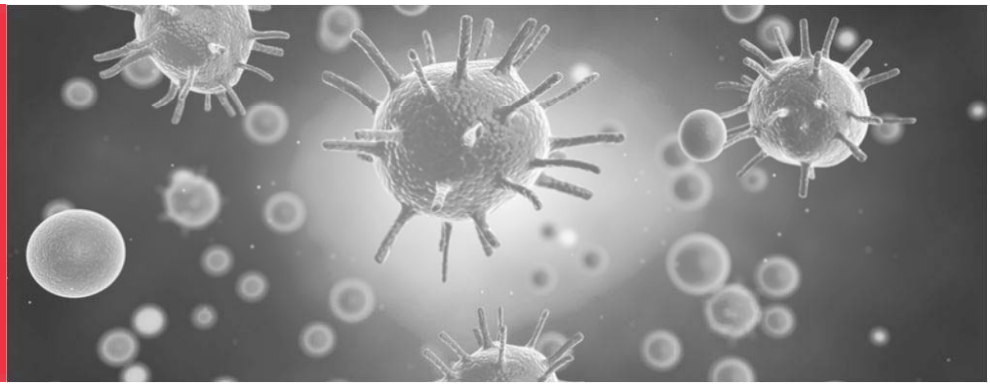
DZP
więcej niż prawo

KORONAWIRUS ALERT

24/7



Wsparcie biznesu 24/7 w dobie pandemii koronawirusa

Cyberprzestępczość – ochrona przed przestępcami komputerowymi w sytuacji zagrożenia epidemicznego

Czas, w którym wszystkie oczy zwrócone są w stronę walki z wirusem, jest również czasem, w którym **przedsiębiorcy są najbardziej zagrożeni cyberprzestępczością, tj. przestępczością popełnianą za pomocą Internetu**. Spadek liczby pracowników czynnie wykonujących swoje zadania, konieczność wprowadzenia pracy zdalnej oraz skupienie się na utrzymaniu ciągłości świadczenia usług powoduje, iż ochrona systemów komputerowych i baz danych spada na dalszy plan. Warto jednak pamiętać, że **czujność i dbałość o bezpieczeństwo cyfrowe nigdy nie były tak ważne jak obecnie**.

Jakie działania mogą podjąć cyberprzestępcy?

- **oszustwo internetowe**: stworzenie fałszywej bramki agentów rozliczeniowych (np. PayU); przejęcie dostępu do elektronicznej skrzynki pocztowej, podszywanie się pod kontrahenta oraz przesłanie w jego imieniu faktury zawierającej numer konta przestępcy;
- **kradzież bazy danych**: przełamanie zabezpieczeń w celu uzyskania dostępu do bazy danych (np. zawierającej informacje o klientach, historię transakcji), skopiowanie rekordów, sprzedaż nielegalnie pozyskanych informacji;
- **szpiegostwo komputerowe**: wykorzystanie złośliwego oprogramowania w celu pozyskania wiedzy o działalności przedsiębiorstwa;
- ***ransomware***: zablokowanie dostępu do systemu komputerowego oraz żądanie okupu za jego zdjęcie;
- ***carding***: wykradanie danych kart płatniczych w celu zakupu produktów lub usług na koszt faktycznego właściciela karty.

Co może/powinien zrobić przedsiębiorca?

- poinstruowanie pracowników o **konieczności zastosowania szczególnej czujności** podczas pobierania plików nieznanego pochodzenia, zlecania wykonania przelewów *online* czy dokonywania transakcji internetowych z użyciem karty płatniczej;
- poinformowanie o **zakazie przekazywania przez wiadomości e-mail czy rozmowy telefoniczne wszelkich danych mogących posłużyć do przełamania zabezpieczeń** systemów komputerowych (np. loginów, haseł, numerów kont);
- **zainstalowanie/uaktualnienie oprogramowania antywirusowego**, *antymalware*'owego, antyspamowego, *antyspyware*'owego oraz pozostawienie aktywnej zapory sieciowej (tzw. *firewall*'a);
- regularne *tworzenie kopii zapasowych*, tzw. backupów;
- dbałość o **przechowywanie logów** serwera i stron internetowych;

- notowanie wszelkich informacji o niepokojących lub nietypowych zdarzeniach.

Jak zachować się w sytuacji zidentyfikowania cyberprzestępstwa?

Ze względu na mnogość zachowań cyberprzestępców nie można stworzyć uniwersalnego schematu postępowania. Jeżeli doszło do przełamania zabezpieczeń, ważne jest, aby zmienić hasła i zbadać integralność danych. Gdyby zaś sprawca wyłudził pieniądze, istotne jest poinformowanie banku, który może ustanowić blokadę środków na rachunku wykorzystanym do popełnienia przestępstwa. W przypadku żądania okupu należy pamiętać, że spełnienie oczekiwań przestępcy nie daje gwarancji uzyskania ponownego dostępu do systemu komputerowego czy utraconych danych.

Ważne jest, aby zareagować jak najszybciej. Im mniej czasu upłynie od zdarzenia, tym większe prawdopodobieństwo zminimalizowania strat oraz zabezpieczenia dowodów, które następnie mogą posłużyć w postępowaniu karnym czy cywilnym.

Jeżeli już doszło do popełnienia przestępstwa, **kluczowe jest współdziałanie z organami ścigania, podjęcie działań na gruncie ochrony danych osobowych oraz ewentualne rozważenie sporu cywilnego z usługodawcami dostarczającymi właściwe rozwiązania techniczne**.

Jesteśmy do Państwa dyspozycji

Rafał Karbowniczek
Senior Associate | Praktyka Postępowań Spornych
E: rafał.karbowniczek@dzp.pl

Małgorzata Karasińska
Associate | Praktyka Postępowań Spornych
E: malgorzata.karasinska@dzp.pl