Bitdefender

Ryzyko i konsekwencje prawne nieujawnienia naruszenia bezpieczeństwa

13.06.2023

W dzisiejszej erze cyfrowej odpowiedzialność firm wykracza poza zwykłe zapobieganie zagrożeniom cybernetycznym. Wiąże się to również z wiedzą, jak skutecznie reagować w przypadku naruszenia bezpieczeństwa, które jest bardziej nieuniknione niż możliwe. Przy stale zmieniającym się krajobrazie zagrożeń cybernetycznych firmy każdej wielkości i we wszystkich branżach muszą być przygotowane na potencjalne zakłócenia bezpieczeństwa. Przygotowanie to często przybiera formę solidnej strategii reagowania na incydenty (IR), która jest krytycznym elementem ram bezpieczeństwa cybernetycznego każdej firmy.

Dlaczego zgłaszanie naruszeń jest ważne

Znaczenie skutecznej komunikacji i terminowego powiadamiania o naruszeniach jest nie do przecenienia. Są one niezbędne do wdrożenia

środków zaradczych i odzyskiwania zasobów w razie skutecznego ataku, a jednocześnie są niezbędne ze względów zgodności z przepisami.

Jak ujawnienie naruszenia pomaga w działaniach naprawczych

Natychmiastowe zgłaszanie naruszeń umożliwia poinformowanie o zdarzeniu wszystkich zainteresowanych stron: wewnętrznych i zewnętrznych. Na przykład jeśli Twoje dane zostaną naruszone wskutek ataku hakerskiego u Twojego kontrahenta, to musisz zostać natychmiast o tym powiadomiony, aby przygotować i chronić swoją firmę. Podobnie jeśli naruszenie w Twoim systemie może mieć wpływ na Twojego klienta, on również powinien zostać powiadomiony tak szybko, jak to możliwe.

Dzięki skuteczniejszym i szybszym środkom zaradczym możesz ograniczyć skutki naruszenia ochrony danych oraz potencjalne szkody dla reputacji i relacji biznesowych Twojej firmy. Sprawna komunikacja pomaga również utrzymać zaufanie klientów — natychmiast informując klientów, w jaki sposób sytuacja ich dotyczy i jakie środki podejmujesz, aby zapobiec dalszym szkodom, możesz zbudować jeszcze większe zaufanie klientów i złagodzić potencjalne szkody dla reputacji swojej firmy.

Standardy regulacyjne i zgodności wymagające odpowiedzialnego ujawniania naruszeń

Na froncie regulacyjnym wiele ostatnich przepisów dotyczących ochrony danych zawiera określone wymagania dotyczące powiadamiania o

naruszeniu. Na całym świecie możemy spotkać się z wieloma różnymi standardami ochrony danych, jednak w tym artykule skupimy się tylko na tych, które występują w Europie.

RODO

RODO wymaga od firm zgłaszania naruszeń w ciągu 72 godzin, „jeśli jest to wykonalne", z wyjątkiem sytuacji, gdy naruszenie „nie powoduje zagrożenia dla praw i wolności osób fizycznych". Jeżeli organizacja opóźnia się ze zgłoszeniem naruszenia, należy podać przyczyny opóźnienia. RODO przewiduje wysokie kary za nieprzestrzeganie przepisów. W zależności od naruszeń grzywny mogą sięgać:

- 10 milionów euro lub 2% rocznego obrotu, w zależności od tego, która wartość jest wyższa
- 20 milionów euro (22 miliony dolarów) lub 4% rocznego obrotu, w zależności od tego, która wartość jest wyższa.

Wysokość kary zależy od dochodzenia organu regulacyjnego, stopnia zaniedbania i wagi naruszenia.

Europejska dyrektywa NIS-2 („Bezpieczeństwo sieci i informacji, wersja 2")

Rozporządzenie UE, NIS-2, weszło w życie 6 stycznia 2023 r. i wprowadziło rygorystyczne środki nadzorcze oraz usprawniło obowiązki sprawozdawcze. Firmy, których to dotyczy, muszą teraz przekazać wstępne powiadomienie w ciągu 24 godzin od uzyskania informacji o

incydencie organowi zgłaszającemu, a w ciągu 72 godzin firma musi przedstawić wstępną ocenę naruszenia. Oczekuje się, że w ciągu miesiąca od ataku firmy przedstawią raport końcowy szczegółowo opisujący zakres ataku, a także wszelkie podjęte działania łagodzące.

Grzywny NIS-2 mogą sięgać nawet 10 milionów euro lub 2% rocznych przychodów firmy, w zależności od tego, która z tych kwot jest wyższa.

Co organizacje mogą zrobić, aby poprawić zgłaszanie naruszeń

W dobie zwiększonego ryzyka cybernetycznego organizacje muszą aktywnie zwiększać możliwości zgłaszania naruszeń. Oto kilka najlepszych praktyk:

Opracuj jasną politykę i proces

Firmy muszą opracować kompleksową politykę zgłaszania naruszeń i zapewnić jej egzekwowanie we wszystkich działach. Obejmuje to zdefiniowanie procesów, których należy przestrzegać, w zależności od rodzaju i wagi naruszenia, a także proces ujawniania.

Wyznacz kluczowych interesariuszy i ich obowiązki

Kluczowi interesariusze to ci, na których można polegać w przypadku incydentu związanego z bezpieczeństwem, powinni pochodzić z różnych działów i muszą być brani pod uwagę w zależności od tego, jak wyglądają środki zaradcze i reakcja. Mogą to być np. pracownicy działów: IT, PR i prawnicy.

Współpracuj z osobami trzecimi

„Współpraca z zewnętrznymi dostawcami może znacznie zwiększyć możliwości organizacji w zakresie reagowania na naruszenia. Warto wziąć pod uwagę specjalistów ds. reagowania na incydenty i środków zaradczych, a także dostawców usług antywirusowych, którzy przyczynią się do poprawy ogólnych możliwości monitorowania i wykrywania. Te osoby trzecie mogą również pomóc w utrzymaniu ścieżki audytu, co może być nieocenione w przypadku dochodzeń. Wykazując, że podjęto proaktywne działania w celu zapobiegania naruszeniom, zarządzania nimi i ich naprawiania, możesz potencjalnie złagodzić skutki prawne" – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Przygotuj się na nową normalność

Naruszenia danych w firmach i placówkach publicznych stają się zjawiskiem powszechnym. Zgodnie z raportem Bitdefender ponad 50% respondentów z całego świata stwierdziło, że w ciągu 12 miesięcy doszło do naruszenia lub wycieku ich danych (w przypadku respondentów z USA było to 70%).

Aktualnie przedsiębiorstwa znajdują się pod ogromną presją, by zwiększać odporność swoich zabezpieczeń przy coraz mniejszych zasobach. Włączenie skutecznego zgłaszania naruszeń do ram cyberbezpieczeństwa to nie tylko najlepsza praktyka, ale konieczność. Akceptując tę rzeczywistość, firmy będą zmuszone do ustalania

priorytetów i inwestowania w zwiększanie możliwości zgłaszania naruszeń, co ostatecznie pomoże im skuteczniej poruszać się po złożonym krajobrazie zagrożeń cybernetycznych.

Źródło:https://bitdefender.pl/ryzyko-i-konsekwencje-prawne-nieujawnienia-naruszenia-bezpieczenstwa/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 13.06.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender
Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.