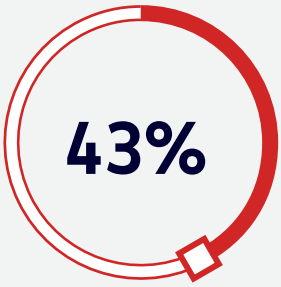
Always Designing for People®

WSPIERANIE CYBERODPORNOŚCI

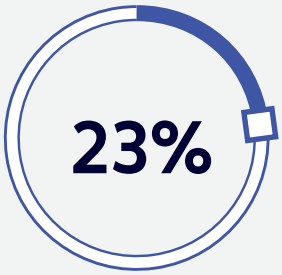
W systemach płacowych są przechowywane jedne z najbardziej wrażliwych danych każdej organizacji, takie jak dane identyfikacyjne, numery rachunków bankowych, informacje o wynagrodzeniach oraz dokumentacja podatkowa. Sprawia to, że są one atrakcyjnym celem cyberataków.

W ankiecie dot. globalnych list płac pt. **„Potencjał list płac w 2026 r."** odnotowano znaczący wzrost tego typu incydentów. 71% kierowników zespołów płacowych zgłosiło co najmniej jeden incydent cyberbezpieczeństwa wpływający na obsługę listy płac w ciągu ostatnich 24 miesięcy. To wzrost w porównaniu z 57% w poprzednim roku. Wzrost o 13 punktów procentowych sugeruje, że zagrożenie nadal będzie rosnąć, w miarę jak strategie ataków stają się coraz bardziej zaawansowane.

Nowe technologie i narzędzia, w tym narzędzia sztucznej inteligencji (AI), mogą ułatwiać bardziej niż kiedykolwiek wcześniej generowanie dużych ilości e-maili typu phishing naraz i inicjowanie wyjątkowo przekonujących niechcianych połączeń telefonicznych. Lista płac odgrywa coraz bardziej strategiczną rolę w organizacjach, dlatego odporne zespoły staną się ważniejsze niż kiedykolwiek wcześniej.



doświadczyło w ciągu ostatnich 24 miesięcy 1 lub 2 zdarzeń zagrażających bezpieczeństwu danych, które miały wpływ na listę płac



doświadczyło w ciągu ostatnich 24 miesięcy 3 lub 4 zdarzeń zagrażających bezpieczeństwu danych, które miały wpływ na listę płac

doświadczyło w ciągu ostatnich 24 miesięcy co najmniej 5 zdarzeń zagrażających bezpieczeństwu danych, które miały wpływ na listę płac

Od świadomości do gotowości

Zespoły płacowe dobrze zdają sobie sprawę z tego ryzyka. Większość kierowników rozumie, na jakie ryzyko są narażeni. Organizacje wciąż są w trakcie przygotowywania się do tej nowej rzeczywistości.

Tylko 41% organizacji ma obejmujący całą firmę plan awaryjny dotyczący listy płac. Oznacza to, że niemal 6 na 10 organizacji — z których wiele doświadczyło już zdarzenia zagrażającego bezpieczeństwu danych — nadal działa bez skoordynowanego planu reagowania.

Nadrabiają jednak zaległości. 49% organizacji opracowało podręczniki i plany dla niektórych rynków, w porównaniu z 33% w ubiegłym roku.

Inwestowanie w specjalne zdolności w zakresie bezpieczeństwa

Odpowiedź na rosnące zagrożenia jest coraz częściej uwzględniana w obsłudze listy płac. 47% procent zespołów płacowych ma obecnie specjalne zasoby zajmujące się bezpieczeństwem danych. Są to specjaliści skupiający się w szczególności na ochronie danych i systemów płacowych. Kolejne 37% deklaruje chęć rozwinięcia takich zdolności, co sugeruje powszechne uznanie, że bezpieczeństwo nie może już pozostawać wyłącznie w gestii zespołów IT.

33% kierowników zespołów płacowych wskazało bezpieczeństwo danych jako jeden z głównych globalnych priorytetów w zakresie doskonalenia w okresie najbliższych dwóch do trzech lat. To sprawia, że bezpieczeństwo danych — wraz ze zgodnością z przepisami i raportowaniem — staje się jednym z kluczowych obszarów zainteresowania.

Budowanie odporności na poziomie lokalnym i globalnym

W miarę jak lista płac zaczyna odgrywać coraz bardziej strategiczną rolę w organizacjach, odporne zespoły staną się ważniejsze niż kiedykolwiek wcześniej. Organizacje najlepiej przygotowane do zarządzania zagrożeniami cyberbezpieczeństwa to te, które nie ograniczają się do reagowania po wystąpieniu incydentu, lecz zapewniają specjalistyczną wiedzę w zakresie bezpieczeństwa na każdym poziomie swojej działalności.

Oznacza to opracowywanie i testowanie planów awaryjnych zarówno na poziomie lokalnym, jak i globalnym, zapewnienie odpowiednich kompetencji i uprawnień do zarządzania kwestiami bezpieczeństwa w obszarze listy płac, ustanowienie jasnych procedur reagowania na incydenty — również z udziałem zewnętrznych dostawców — oraz utrzymywanie ścisłej współpracy z działem IT.

Organizacje, które traktują ochronę danych jako strategiczny czynnik napędowy — a nie tylko obowiązek w zakresie zgodności z przepisami — są lepiej przygotowane do zapobiegania incydentom i szybszego odzyskiwania sprawności po ich wystąpieniu.

41%

opracowało podręcznik oraz plan awaryjny we wszystkich krajach

49%

opracowało podręcznik oraz plany awaryjne w niektórych krajach

9%

rozważa opracowanie planów, ale jeszcze ich nie wdrożyło

1%

nie rozważało opracowania takich planów

DOWIEDZ SIĘ WIĘCEJ

Dowiedz się z pełnego raportu, jak organizacje wzmacniają bezpieczeństwo listy płac i budują cyberodporność: Potencjał list płac w 2026 r.: ankieta dot. globalnych list płac.

WF3615202

Always Designing for People®