Bitdefender

Nowe niebezpieczeństwo dla zespołów ds. cyberbezpieczeństwa – coraz większa luka w sile roboczej

17.04.2023

Organizacje różnej wielkości i z różnych branż poruszają się aktualnie po bardzo trudnym krajobrazie cyberzagrożeń, w którym zwykły antywirus zazwyczaj jest niewystarczający do zapewnienia odpowiedniej ochrony. Środowiska IT w ostatnich latach rozszerzyły się i stały się bardziej podatne na cyberataki, ponieważ firmy coraz częściej migrują do chmury i polegają na zdalnej sile roboczej rozproszonej na całym świecie. Jednocześnie rośnie liczba zagrożeń. Przewiduje się, że globalne koszty cyberprzestępczości wzrosną o 15%, osiągając 10,5 biliona dolarów rocznie do 2025 roku. W jaki więc sposób firmy i organizacje powinny przygotować swoją infrastrukturę sieciową i jaką strategię ochrony powinny obrać?

Coraz większa luka w sile roboczej

Wśród wielu zagrożeń związanych z ochroną cybernetyczną być może najbardziej palącym wyzwaniem stojącym przed organizacjami jest dotkliwy niedobór siły roboczej w branży cyberbezpieczeństwa. Zgodnie z najnowszym badaniem Cybersecurity Workforce Study przeprowadzonym przez (ISC)2 luka w sile roboczej zespołów do spraw cyberbezpieczeństwa wzrosła w 2022 roku o 26%, a na całym świecie potrzeba 3,4 miliona więcej specjalistów w tej dziedzinie.
Wspomniany niedobór wpływa na zdolność organizacji do obrony przed zagrożeniami. Prawie trzy czwarte (74%) respondentów ankiety stwierdziło, że niedobór siły roboczej naraża ich organizację na umiarkowane lub ekstremalne ryzyko ataku, a prawie połowa (48%) – że nie ma wystarczająco dużo czasu na odpowiednią ocenę ryzyka i zarządzanie nim.

Gartner szacuje, że prawie połowa liderów do spraw cyberbezpieczeństwa odejdzie ze swoich stanowisk do 2025 roku ze względu na rosnącą presję związaną z pracą. Ta firma badawcza przewiduje, że to nie bezpośrednie złamanie systemów antywirusowych, lecz wypalenie pracowników, rotacja w branży i brak talentów będą odpowiadały za większość znaczących incydentów związanych z cyberbezpieczeństwem.

Przyciąganie i szkolenie nowych talentów wymaga czasu, a niektórzy eksperci wyrażają zaniepokojenie, że następnemu pokoleniu osób wchodzących na rynek pracy brakuje niezbędnych umiejętności lub zainteresowania rolami związanymi z cyberbezpieczeństwem. Istnieją

jednak sposoby, dzięki którym organizacje mogą dziś wypełnić lukę i zwiększyć odporność cybernetyczną dzięki rozwojowi systemów antywirusowych oraz zaawansowanym nowym technologiom i usługom zarządzanym.

Wykorzystanie XDR do wypełnienia luki w umiejętnościach

Oprócz podejmowania wyzwań opisanych powyżej zespoły do spraw cyberbezpieczeństwa zarządzają obecnie coraz bardziej złożonym środowiskiem za pomocą wielu różnych programów, antywirusów i innych narzędzi. Proces ten wymaga pracy ręcznej w celu skorelowania spostrzeżeń z różnych strumieni danych, co często skutkuje przeciążeniem systemów i fałszywymi alarmami.

Jednym z rozwiązań tego problemu są technologie rozszerzonego wykrywania i reagowania (XDR). XDR to najnowsza innowacja w dziedzinie cyberbezpieczeństwa. Wywodząc się z technologii wykrywania i reagowania (EDR), XDR znacznie wykracza poza tradycyjne punkty końcowe i obejmuje całe środowisko organizacji: urządzenia fizyczne i podłączone do sieci, platformy wirtualne i chmurowe, hostowane obciążenia, aplikacje zwiększające produktywność o systemy tożsamości i uwierzytelniania.

XDR nie jest jedynie kolejnym modułem systemów antywirusowych, lecz zupełnie nowym narzędziem, które nie tylko zwiększa widoczność i zasięg, ale także tworzy współdzieloną warstwę wykrywania, zapewniając zarządzanie całym środowiskiem bezpieczeństwa w jednym okienku. To rozwiązanie pomaga organizacjom przezwyciężyć

lukę w umiejętnościach związanych z cyberbezpieczeństwem poprzez:

Zapewnienie scentralizowanego i zautomatyzowanego podejścia do operacji związanych z bezpieczeństwem.
Zmniejszenie konieczności ręcznej interwencji i uwolnienie zespołów do spraw cyberbezpieczeństwa, aby mogły skupić się na bardziej strategicznych zadaniach.
Poprawienie widoczności i wykrywania zagrożeń. XDR zapewnia pełniejszy obraz stanu bezpieczeństwa organizacji, ułatwiając zespołom do spraw cyberbezpieczeństwa identyfikację zagrożeń i reagowanie na nie.
Automatyzację reagowania i łagodzenia. XDR może zmniejszyć ryzyko błędu ludzkiego i zapewnić spójne egzekwowanie zasad bezpieczeństwa w całej organizacji.

„XDR, mający kluczowe znaczenie dla wypełnienia niedoboru siły roboczej zespołów do spraw cyberbezpieczeństwa, tworzy również czytelne dla człowieka raporty i graficzne ilustracje incydentów, umożliwiając w ten sposób analitykom bezpieczeństwa identyfikację zagrożenia i zrozumienie całego zakresu incydentu. Eksperci mogą szybko zobaczyć, które zasoby zostały dotknięte, jakie metody ataku zostały użyte, główną przyczynę, najważniejsze informacje o incydencie i zalecane działania. Zapewnienie tego wszystkiego w jednym scentralizowanym miejscu, w jednym widoku, w łatwym do zrozumienia raporcie oszczędza czas, zmniejszając liczbę fałszywych alarmów i sprawiając, że członkowie zespołu bezpieczeństwa nie muszą marnować czasu podczas badania incydentu” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego

dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/coraz-wieksza-luka-w-sile-roboczej/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 17.04.2023
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.