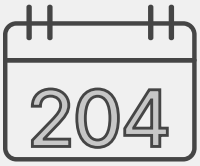
RAPORT

Ukryte koszty związane ze starzejącymi się rozwiązaniami w punktach końcowych

Ransomware, bezplikowe szkodliwe oprogramowanie i problemy z zarządzaniem

Streszczenie

Dyrektorzy ds. bezpieczeństwa systemów informatycznych bardzo martwią się bezpieczeństwem punktów końcowych. Większość z nich zakłada, że prędzej czy później ich punkty końcowe zostaną zaatakowane — i zwykle mają rację. Okazuje się na przykład, że mniej firm jest dziś w stanie skutecznie wykrywać oprogramowanie ransomware niż w 2023 r. (13%, podczas gdy wcześniej było to 22%), co wskazuje, że tego rodzaju oprogramowanie również staje się coraz bardziej zaawansowane i działa w sposób ukierunkowany[1]. Według wyników niedawnego badania spośród 78% kierowników, którzy twierdzili, że ich firmy są przygotowane na ataki, połowa nie była w stanie się przed nimi uchronić [2]. Firmy mają świadomość, że tradycyjne rozwiązania antywirusowe nie chronią skutecznie punktów końcowych, dlatego potrzebna jest bardziej zaawansowana ochrona, zwłaszcza że średni koszt włamania w 2023 r. wynosił aż 4,45 mln dolarów[3].



Średni czas wykrycia udanego ataku wynosi obecnie średnio 204 dni. Do tego należy doliczyć dodatkowe 73 dni na eliminację skutków incydentu[4].

Co prawda rozwiązania do wykrywania i reagowania w punktach końcowych (endpoint detection and response, EDR) pierwszej generacji poprawiły bezpieczeństwo w tym względzie, oferując pewne przydatne funkcje, ale wiąże się to z ukrytymi kosztami. Długi czas reakcji i brak integracji międzyplatformowej narażają firmy na ryzyko ataków z użyciem oprogramowania ransomware i inne zagrożenia oparte na szybkich działaniach.

Ponadto działy zabezpieczeń zmagają się z zalewem alertów pochodzących z wielu systemów kontroli bezpieczeństwa, co zwiększa poziom stresu i ryzyko nieprawidłowej klasyfikacji zagrożeń.

Z kolei ręczne działania naprawcze, takie jak czyszczenie i ponowna instalacja oprogramowania z obrazów, nadmiernie obciążają personel IT i powodują przestoje w środowisku produkcyjnym. Nie ma wątpliwości, że obecne rozwiązania w zakresie zabezpieczeń punktów końcowych nie są w stanie zapewnić szybkości, integracji, korelacji zdarzeń i automatyzacji, których potrzebują dyrektorzy ds. bezpieczeństwa systemów informatycznych.

Konwergencja zabezpieczeń punktów końcowych

Lata temu dyrektorzy ds. bezpieczeństwa systemów informatycznych zdali sobie sprawę, że części zagrożeń nie da się zapobiec, w związku z czym konieczne jest szybsze wykrywanie udanych ataków. Dlatego zaczęli rozbudowywać mechanizmy zabezpieczeń punktów końcowych, wdrażając systemy EDR na urządzeniach o krytycznym znaczeniu dla firmy. Te rozwiązania EDR („pierwszej generacji") monitorowały zdarzenia i działania w punktach końcowych, identyfikując podejrzane zachowania, które mogły wskazywać na obecność zagrożeń, takie jak próby wstrzyknięcia kodu zmieniającego procesy, modyfikacji kluczy rejestru czy dezaktywacji rozwiązań zabezpieczeń. Mimo że rozwiązania EDR pierwszej generacji pozwalały uzyskać informacje, dzięki którym analitycy ds. bezpieczeństwa mogli reagować na incydenty i je badać, w dużej mierze opierały się na procesach ręcznych i nie były zintegrowane z resztą ekosystemu zabezpieczeń i IT w firmie.

Ukryte koszty rozwiązań EDR pierwszej generacji

Zanim rozwiązania EDR przekształciły się w architekturę rozszerzonego wykrywania i reagowania (extended detection and response, XDR), ich zadaniem było rejestrowanie i przechowywanie zdarzeń w punktach końcowych, a także identyfikowanie potencjalnych incydentów, reagowanie na zagrożenia i wspomaganie dochodzeń przy użyciu funkcji wykrywania opartego na zachowaniach, jak również generowanie alertów dotyczących tego rodzaju zagrożeń. Mimo że rozwiązania EDR pierwszej generacji niewątpliwie poprawiły widoczność i usprawniły wykrywanie zagrożeń w punktach końcowych, ulepszenia te wiązały się z kosztami, z których duża część nie była wcale oczywista.

Długi czas reakcji

Mimo zmian i inwestycji w nowe technologie wykrywanie i blokowanie włamań nie jest znacząco krótsze, jak mogłoby się wydawać.

W przypadku cyberataków, których głównym celem jest kradzież danych, rozwiązania EDR pierwszej generacji są w stanie reagować w miarę szybko. Takie ataki przeprowadza się ukradkiem, a polegają one na zebraniu informacji, utworzeniu mapy sieci i określeniu lokalizacji cennych zasobów, co może trwać tygodniami. Wielu dyrektorów ds. bezpieczeństwa systemów informatycznych uważa, że w walce z tego rodzaju zagrożeniami i w ramach zapobiegania kradzieży danych czas wykrywania i reakcji może wynosić 24 godziny, a nawet kilka dni.

Z kolei celem innych ataków, takich jak te z użyciem oprogramowania ransomware, nie jest kradzież danych, tylko sabotaż. Cyberprzestępcom wystarczają minuty, a nawet sekundy, aby dokonać udanego ataku, co znacznie skraca ramy czasowe reakcji. Współczesne odmiany oprogramowania ransomware są projektowane w taki sposób, aby znaleźć cele w sieci firmowej, a następnie rozprzestrzeniać się w kierunku bocznych odnóg systemu — np. na serwery i inne sieci — w czasie poniżej minuty.

Przykładem takiego narzędzia jest NotPetya — cyberbroń występująca pod postacią oprogramowania ransomware, której głównym celem jest powodowanie zniszczeń. W takim przypadku atak następuje znacznie szybciej, niż zespół ds. zabezpieczeń jest w stanie zareagować. To samo dotyczy prób ręcznego powstrzymania ataku przy użyciu rozwiązań EDR pierwszej generacji. Każde rozwiązanie, które nie jest oparte na blokowaniu w czasie rzeczywistym, zwiększa ryzyko udanego ataku na infrastrukturę firmy.

Przestoje środowiska produkcyjnego

Gdy zespół ds. zabezpieczeń zidentyfikuje zaatakowany punkt końcowy, pierwszym krokiem jest powstrzymanie zagrożenia. Narzędzia EDR pierwszej generacji często poddają punkt końcowy kwarantannie, aby zapobiec rozprzestrzenianiu się ataku i nie dopuścić do utraty danych. Ta technika sprawdza się jako środek ochronny, ale powoduje też, że punkt końcowy staje się bezużyteczny dla użytkowników, a nawet może doprowadzić do zatrzymania procesów produkcyjnych. Zespoły ds. zabezpieczeń często spędzają dużo czasu na ręcznej weryfikacji alertów, sprawdzając, czy dane zagrożenie jest prawdziwe, zanim poddadzą punkty końcowe kwarantannie. Ponadto wiele urządzeń znajduje się w znacznym oddaleniu od personelu IT — np. ze względu na rozproszony model infrastruktury firmowej lub pracę zdalną — przez co dodatkową zaletą jest możliwość zdalnego wykonywania procedur rozwiązywania problemów. Mimo że niektóre starsze rozwiązania EDR udostępniają funkcje powłoki zdalnej, możliwość bezpiecznego i szybkiego nawiązywania połączeń z punktami końcowymi zwiększa podatność na zagrożenia w przypadku przejęcia tożsamości administratora, czego przykłady mogliśmy obserwować podczas wielu głośnych ataków.

Analitycy ds. bezpieczeństwa także podchodzą sceptycznie do narzędzi zabezpieczających punkty końcowe, które mają zapewniać zautomatyzowane reakcje (polegające np. na zatrzymaniu procesu i poddaniu punktu końcowego kwarantannie). Tego rodzaju zautomatyzowane rozwiązania mogą aktywować kwarantannę nawet w przypadku fałszywego alertu. Następuje wówczas wyłączenie linii produkcyjnej, co jest kosztowną i kłopotliwą pomyłką.

W fazie działań naprawczych większość działów IT wciąż wybiera całkowite wyczyszczenie pamięci zainfekowanego urządzenia i ponowną instalację oprogramowania z obrazu z powodu braku zaufania do tradycyjnych narzędzi antywirusowych, które nie zapewniają trwałego czyszczenia, stwarzając ryzyko ponownej infekcji. Jest to jednak czasochłonny proces wykonywany ręcznie, który wymaga odłączenia urządzenia od sieci na czas naprawy.

W pionie firmy wykorzystującym infrastrukturę IT pracownicy wiedzy realizują swoje obowiązki, posługując się komputerami. Pozbawiając tych pracowników laptopów i komputerów stacjonarnych podczas fazy działań naprawczych, ogranicza się ich produktywność — szczególnie w przypadku rozbudowanego modelu pracy zdalnej. Ponadto w wielu firmach po prostu wymienia się zainfekowany komputer na nowy, aby uniknąć większych przestojów, co jest dodatkowo uciążliwe, gdy trzeba wysyłać nowe urządzenia do domów pracowników. W pionie technologiczno-operacyjnym firmy sytuacja wygląda zupełnie inaczej. Dezaktywacja krytycznego systemu sterowania lub urządzenia produkcyjnego może spowodować zamknięcie całej linii produkcyjnej, co wiąże się ze znacznymi kosztami w postaci opóźnień w realizacji zamówień, utraconych przychodów i dodatkowej pracy techników potrzebnej do ponownego uruchomienia linii.

Fałszywe alerty

Systemy EDR generują wiele alertów i wskazań, które wymagają ręcznej weryfikacji pod kątem szkodliwości. Te czynności powodują znaczny spadek produktywności zespołów ds. zabezpieczeń i odciągają je od działań, które zwiększają dojrzałość zabezpieczeń firmy. Ponadto wraz ze wzrostem liczby ataków trudno jest skalować zakres ręcznej weryfikacji, zwłaszcza biorąc pod uwagę ciągły niedobór specjalistów ds. cyberbezpieczeństwa. Duża liczba fałszywych alertów może powodować przemęczenie analityków, a w konsekwencji doprowadzić do przeoczenia prawdziwych symptomów ataku wśród szumu informacyjnego.

Niedobór specjalistów

Zaprojektowanie i wdrożenie skutecznej strategii wykrywania incydentów i reagowania na nie wymaga zespołu wykwalifikowanych specjalistów ds. zabezpieczeń. Znalezienie takich specjalistów jest jednak trudne ze względu na utrzymujące się luki na rynku pracy. Według niedawnego badania niedobór specjalistów ds. cyberbezpieczeństwa wzrósł o 13%, co oznacza, że w 2023 r. na całym świecie brakowało około 4 mln osób wykonujących ten rodzaj pracy[5].

Z punktu widzenia dyrektorów ds. bezpieczeństwa systemów informatycznych jest to bardzo trudna sytuacja. Jeśli nie będą oni w stanie szybko obsadzić kluczowych stanowisk, braki kadrowe spowodują obniżenie bezpieczeństwa punktów końcowych, co przełoży się na obciążenie obecnych pracowników. Z drugiej strony zatrudnianie niedoświadczonych kandydatów może prowadzić do kosztownych błędów, takich jak nieregularne wdrażanie krytycznych aktualizacji zabezpieczeń i błędy w konfiguracji będące przyczyną fałszywych alertów.

Podsumowanie

Starsze rozwiązania w zakresie zabezpieczeń punktów końcowych w dużej mierze opierają się na zapobieganiu zagrożeniom lub wykrywaniu ich bez reagowania w czasie rzeczywistym. Takie podejście nie zapewnia ochrony przed zaawansowanymi atakami. Radzenie sobie ze współczesnymi zagrożeniami jest coraz trudniejsze. Wyrafinowane i szybkie cyberataki bez trudu pokonują tradycyjne zabezpieczenia punktów końcowych, które są po prostu przestarzałe.

Eliminowanie wykrytych luk w zabezpieczeniach także jest trudne ze względu na problemy ze znalezieniem, rekrutacją, zatrudnieniem i zatrzymaniem wykwalifikowanych specjalistów ds. bezpieczeństwa. Zespoły zajmujące się zabezpieczeniami są przeciążone coraz liczniejszymi alertami, z których duża część jest fałszywa. Może to doprowadzić do ich paraliżu, przez co nie będą w stanie przebić się przez ogrom informacji o zagrożeniach generowanych przez systemy zabezpieczeń. Rozwiązania takie jak EDR — a zwłaszcza XDR — umożliwiają wykrywanie incydentów bezpieczeństwa i umożliwiają automatyczne reagowanie na nie w infrastrukturze firmy.

[1] Global Threat Landscape Report (Globalny raport o zagrożeniach), Fortinet, 7 sierpnia 2023 r.

[2] Fortinet 2023 Ransomware Global Research Report (Globalny raport z badań Fortinet dotyczący oprogramowania ransomware w 2023 r.), Fortinet, 24 kwietnia 2023 r.

[3] Cost of a Data Breach Report 2023 (Raport o kosztach naruszenia ochrony danych w 2023 r.), IBM, 24 lipca 2023 r.

[4] Tamże.

[5] How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce (Wpływ sytuacji gospodarczej, luki kompetencyjnej i sztucznej inteligencji na globalny rynek pracowników zajmujących się cyberbezpieczeństwem), ISC², 31 października 2023 r.

28 czerwca 2024 5:03

2618523-0-0-PL