CZTERY PONADSTANDARDOWE SPOSOBY POPRAWY BEZPIECZEŃSTWA PUNKTÓW KOŃCOWYCH

SPIS TREŚCI

STRESZCZENIE

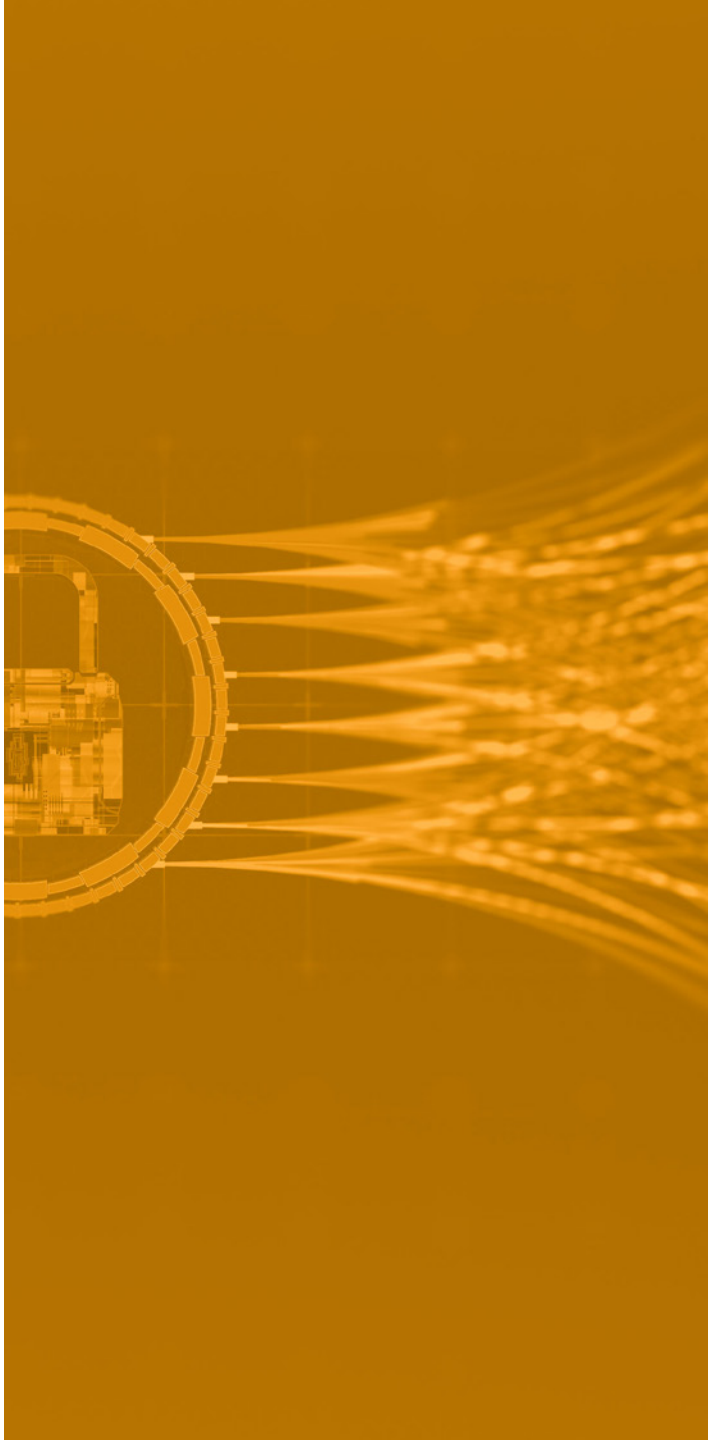
Urządzenia końcowe nadal są jednym z najczęstszych celów cyberataków. Skutecznie zaatakowany laptop może stać się dla złośliwego oprogramowania przyczółkiem do dalszego wielokierunkowego ataku mającego na celu infekowanie kolejnych punktów końcowych w danym przedsiębiorstwie. Aby wyeliminować tę krytyczną lukę w zabezpieczeniach, specjaliści ds. bezpieczeństwa muszą zintegrować zabezpieczenia punktów końcowych w ramach szerzej działającej architektury zabezpieczeń. Dzięki głębokiemu połączeniu obu tych systemów zabezpieczeń istotnie poprawione zostaje bezpieczeństwo całego przedsiębiorstwa. Uzyskuje się wówczas opartą na analizie ryzyka widoczność wszystkich urządzeń końcowych, możliwa jest odbywająca się w czasie rzeczywistym wymiana informacji o zagrożeniach, a także można wdrażać oparte na zasadach mechanizmy kontroli dostępu oraz automatyzować procesy i reakcje dotyczące bezpieczeństwa w celu zapewnienia efektywnej i skutecznej ochrony przedsiębiorstwa w sposób, który przyczynia się również do oszczędzania czasu i pieniędzy.

WSTĘP — INTEGRACJA ZABEZPIECZEŃ PUNKTÓW KOŃCOWYCH I SIECI

Urządzenia końcowe są jednym z najczęstszych celów cyberataków. Jeśli pojedynczy laptop z luką w zabezpieczeniach zostanie skutecznie zaatakowany, po ponownym podłączeniu go do sieci infekcja taka może bardzo szybko rozprzestrzenić się na całe przedsiębiorstwo. W 2017 r. średni koszt skutecznego ataku na punkty końcowe wynosił ponad 5 mln USD na przedsiębiorstwo[1]. Z tego względu przedsiębiorstwa poświęcają obecnie gigantyczne 1156 godzin tygodniowo na wykrywanie i powstrzymywanie zagrożeń wynikających z takich ataków, co średnio daje 3,4 mln USD tygodniowo[2].

Poza samymi zagrożeniami problem stojący za wspomnianymi zasobochłonnymi mechanizmami obrony (i ogólnie za lukami w zabezpieczeniach punktów końcowych) polega na tym, że zabezpieczenia sieci i zabezpieczenia punktów końcowych zazwyczaj działają w kompletnej izolacji od siebie i charakteryzują się niewielką interoperacyjnością. Aby zatem zwiększyć ochronę punktów końcowych i ogólnie całego przedsiębiorstwa, należy zmienić dotychczasowe podejście.

Można wymienić cztery główne obszary, w których tego rodzaju głęboka integracja może przyczynić się do znacznej poprawy bezpieczeństwa przedsiębiorstwa: widoczność oparta na analizie ryzyka, kontrola, wymiana informacji o zagrożeniach i automatyzacja.



[1] Charlie Osborne, „Fileless attacks surge in 2017, security solutions are not stopping them", ZDNet, 15 listopada 2017 r.
[2] „The Cost of Insecure Endpoints", Ponemon Institute, czerwiec 2017 r.

53%

przedsiębiorstw stwierdza, że liczba zainfekowanych złośliwym oprogramowaniem punktów końcowych wzrosła w ciągu ostatnich 12 miesięcy.

„The Cost of Insecure Endpoints", Ponemon Institute, czerwiec 2017 r.

01 — WIDOCZNOŚĆ OPARTA NA ANALIZIE RYZYKA

Przedsiębiorstwa muszą znać status swoich punktów końcowych w sieci bez wymuszania sesji VPN. Mechanizmy zabezpieczeń muszą być zdolne do wykrycia **wszystkich użytkowników i urządzeń** oraz do oceny i monitorowania stosownych zagrożeń. Na zagrożenia takie składają się między innymi istniejące luki w zabezpieczeniach, przestarzałe oprogramowanie i potencjalnie niechciane aplikacje w połączeniu z ryzykownymi zachowaniami użytkowników końcowych. Zapewnienie widoczności opartej na analizie ryzyka wymaga dostępu do **danych telemetrycznych** dotyczących wszystkich punktów końcowych i zdolności do udostępniania ich w czasie rzeczywistym wszystkim wdrożonym w przedsiębiorstwie mechanizmom zabezpieczeń (zaporom, bezpiecznym środowiskom testowym i funkcjom filtrowania stron WWW).

Osoby odpowiedzialne za sieć przedsiębiorstwa powinny na pierwszy rzut oka stwierdzić, czy przedsiębiorstwo z dnia na dzień poprawia swoje bezpieczeństwo. Dzięki uproszczonemu **zarządzaniu z poziomu jednej konsoli** można uzyskać pełny obraz zagrożeń dotyczących punktów końcowych, w tym tożsamości użytkowników, statusu ochrony, istniejących luk w zabezpieczeniach i zdarzeń dotyczących bezpieczeństwa.

Oczekuje się, że wartość rynku rozwiązań zapewniających widoczność i kontrolę punktów końcowych wzrośnie o

23,2%

do 2021 r., co przyczyni się do lepszego wykrywania potencjalnych zagrożeń i zapobiegania im.

„Endpoint Security Software Market Will Reach $5.9 Billion by 2021”, Forrester, 21 sierpnia 2017 r.

02 — KONTROLA

Po zapewnieniu widoczności można wdrożyć odpowiednie mechanizmy kontroli. Zabezpieczenia punktów końcowych muszą zostać odpowiednio **wzmocnione** oraz zastosowane muszą zostać właściwe procedury służące utrzymaniu odpowiedniej **higieny tych zabezpieczeń**, aby poprawić ogólne bezpieczeństwo przedsiębiorstwa.

Właściwe rozwiązanie zabezpieczające punkty końcowe powinno egzekwować przyjęte zasady i kontrole w ramach wszystkich urządzeń i tylko punkty końcowe spełniające wszystkie wymogi i standardy w zakresie bezpieczeństwa powinny mieć możliwość dostępu do zasobów sieci. Oparte na zasadach mechanizmy kontroli dostępu można wdrożyć na bazie danych telemetrycznych. W przypadku wykrycia skutecznie zaatakowanego lub wysoce podejrzanego punktu końcowego może być on wówczas bezpiecznie odizolowany i oznaczony na potrzeby działań naprawczych.

WZMACNIANIE ZABEZPIECZEŃ PUNKTÓW KOŃCOWYCH

Przedsiębiorstwa muszą identyfikować, instalować i konfigurować skuteczne mechanizmy bezpieczeństwa, a także ustalać odczyty bazowe. Kluczowe czynniki sukcesu to w tym przypadku łatwość zbierania danych (49%), przekształcanie danych w użyteczne informacje (47%), wykwalifikowani operatorzy (46%) oraz automatyzacja / interoperacyjność narzędzi (43%).

Lee Neely, „Endpoint Protection and Response: A SANS Survey", SANS Institute, 12 czerwca 2018 r.

56%

specjalistów ds. IT zgłasza brak możliwości określenia zgodności urządzeń końcowych z obowiązującymi normami (na przykład brak możliwości weryfikacji pod kątem istniejących luki w zabezpieczeniach).

„The Cost of Insecure Endpoints", Ponemon Institute, czerwiec 2017 r.

03 — WYMIANA INFORMACJI O ZAGROŻENIACH I ROZWIĄZYWANIE PROBLEMÓW ZWIĄZANYCH Z ALERTAMI

Głęboka integracja narzędzi zabezpieczających punkty końcowe i sieć umożliwia natychmiastową, dwukierunkową wymianę informacji o zagrożeniach. W miarę coraz lepiej ukierunkowanych ataków (z zastosowaniem technik zindywidualizowanego phishingu i niestandardowego złośliwego oprogramowania) ta kluczowa zdolność obronna będzie coraz bardziej przydatna dla przedsiębiorstw.

Wymiana informacji w czasie rzeczywistym w całym przedsiębiorstwie pozwala na natychmiastową reakcję na skoordynowane ataki na konkretne przedsiębiorstwo lub określoną branżę. Ilekroć mechanizm zabezpieczający sieć, bramę sieciową lub punkty końcowe wykryje nowe zagrożenie, informacje o tym zagrożeniu mogą zostać automatycznie wysłane do wszystkich pozostałych mechanizmów zabezpieczających wdrożonych w całym przedsiębiorstwie.

Zabezpieczenia punktów końcowych, które są zdolne do wysyłania i odbierania informacji o zagrożeniach we współpracy z zabezpieczeniami sieci, mogą również oferować funkcje weryfikacji alertów i rozwiązywania problemów związanych z takimi alertami. Oznacza to, że wspomniane zabezpieczenia mogą zestawiać dane dotyczące określonych zdarzeń z danymi dotyczącymi ruchu w sieci lub zagrożeń w celu weryfikacji alertów, zagrożeń na powierzchni ataku i potencjalnych naruszeniach bezpieczeństwa.

„Informacje o zagrożeniach dla bezpieczeństwa punktów końcowych powinny być przesyłane do systemów wykrywania zagrożeń i reagowania na nie. W ten sposób powinien zostać skrócony czas wykrywania przypadków, reagowania na przypadki i eliminowania przypadków zagrożeń i luk w zabezpieczeniach, które atakujący chcą do swoich celów wykorzystać”.

Lee Neely, „Endpoint Protection and Response: A SANS Survey”, SANS Institute, 12 czerwca 2018 r.

04 — AUTOMATYZACJA

Automatyzacja to Święty Graal integracji. Zautomatyzowane reakcje i procesy pozwalają na szybsze w wykrywanie zagrożeń i lepszą przed nimi ochronę przy jednoczesnym zmniejszeniu obciążeń dla przepracowanych i borykających się z niedoborem pracowników działów IT. Dzięki uniknięciu wydłużającego czas reakcji zaangażowania ludzi ataki i incydenty mogą być obsługiwane szybko, efektywnie i skutecznie. Automatyzacja zabezpieczeń punktów końcowych. może być zatem wykorzystania w następujący sposób:

Funkcje **zarządzania lukami w zabezpieczeniach** powinny pozwalać stosowanemu rozwiązaniu zabezpieczającemu punkty końcowe na automatyczne wprowadzanie odpowiednich poprawek w oprogramowaniu / systemie operacyjnym oraz pozwalać na elastyczne eliminowanie pomniejszych problemów. Funkcje te pozwalają nie tylko eliminować podstawowe luki w zabezpieczeniach, ale również ograniczyć liczbę ręcznie wykonywanych czynności przez wspomniane działy IT.

Funkcje **automatycznego reagowania na incydenty i powstrzymywania zagrożeń** pozwalają na natychmiastowe przeciwdziałanie wykrytym zagrożeniom w celu zapobiegania szerzej zakrojonym infekcjom. Jeśli punkt końcowy działa w podejrzany sposób spełniający kryteria definicji ataku (indicator of compromise, IOC), może zostać bezzwłocznie odizolowany od reszty sieci, aby zapobiec rozprzestrzenianiu się zagrożenia na innych urządzeniach lub wewnątrz sieci przedsiębiorstwa. Taka automatyczna kwarantanna chroni dane wrażliwe i ogranicza ekspozycję na ryzyko bez obciążania pracą działu IT oraz skraca czas powstrzymania i wyeliminowania danego zagrożenia. Ponadto pozwala zapewnić, że dana infrastruktura jest zdolna do działania w sposób zgodny z coraz bardziej rygorystycznymi standardami ochrony prywatności i przepisami branżowymi.

Aby zapewnić maksymalną możliwą interoperacyjność posiadanych funkcji automatyzacji w ramach całej architektury zabezpieczeń sieci, należy szukać zabezpieczeń punktów końcowych opartych na **otwartych interfejsach API**, które są zgodne z zabezpieczeniami oferowanymi przez innych producentów. Nie tylko pozwala to na rozszerzenie integracji zabezpieczeń, ale również ułatwia maksymalizację inwestycji w dotychczasowe mechanizmy zabezpieczeń i oprogramowanie antywirusowe.

„Automatyzacja rozwiązań w zakresie wykrywania zagrożeń i reagowania na nie w punktach końcowych to priorytet dla specjalistów IT, którzy chcą uzyskać skuteczną kontrolę nad tymi punktami”.

Lee Neely, „Endpoint Protection and Response: A SANS Survey”, SANS Institute, 12 czerwca 2018 r.

POSUMOWANIE — JAKIEGO ROZWIĄZANIA SZUKAĆ

Wielu dostawców zabezpieczeń używa słowa „integracja” jako słowa-wytrychu. Należy jednak pamiętać, że nie wszystkie poziomy integracji są sobie tożsame. Efektywna integracja między zabezpieczeniami punktów końcowych i zabezpieczeniami sieci powinna stanowić odpowiedzi na następujące pytania:

Widoczność

- Czy widoczne są wszystkie urządzenia i można zidentyfikować użytkowników?
- Czy można monitorować związane z tym ryzyko? Istniejące luki w zabezpieczeniach? Przestarzałe aplikacje? Czynniki spełniające definicję ataku?
- Czy dane telemetryczne punktu końcowego mogą być przesyłane w czasie rzeczywistym do innych zabezpieczeń w przedsiębiorstwie?

Kontrola

- Czy można egzekwować zasady na podstawie kryteriów definicji ataku lub konkretne wymogi dotyczące zgodności z przepisami na poziomie sieci?
- Czy dane rozwiązanie wzmacnia zabezpieczenia punktów końcowych?
- Czy dane rozwiązanie może ograniczyć dostęp na bazie podstawowych zasad higieny zabezpieczeń?

Wymiana informacji o zagrożeniach

- Czy dane rozwiązanie może wymieniać informacje o zagrożeniach z innymi elementami architektury zabezpieczeń w przedsiębiorstwie?

Rozwiązywanie problemów związanych z alertami

- Czy dane rozwiązanie zawiera funkcje weryfikacji alertów / rozwiązywania problemów związanych z alertami, aby ograniczyć zjawisko „szumu informacyjnego”?

Automatyzacja

- Czy dane rozwiązanie udostępnia narzędzia służące do naprawy wykrytych problemów (na przykład funkcje automatycznego instalowania poprawek)?
- Czy można ustawić zasady automatycznej reakcji na zagrożenia polegającej na przykład na wysyłaniu powiadomień, stosowaniu kwarantanny lub wdrażaniu innych mechanizmów kontroli dostępu?

Otwarty ekosystem

- Czy dane rozwiązanie można bezproblemowo zintegrować z rozwiązaniami innych producentów?

SIEDZIBA GŁÓWNA
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
Stany Zjednoczone
Tel.: +1.408.235 7700
www.fortinet.com/sales

BIURO SPRZEDAŻY — REGION EMEA
905 rue Albert Einstein
06560 Valbonne
Francja
Tel.: +33 4 8987 0500

BIURO SPRZEDAŻY — REGION APAC
8 Temasek Boulevard #12-01
Suntec Tower Three
Singapur 038988
Tel: +65-6395-7899
Faks: +65-6295-0015

CENTRALA — AMERYKA ŁACIŃSKA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel.: +1 954 368 9990

POLSKA
ul. Złota 59
Budynek Lumen II (6 piętro)
00-120 Warszawa
Polska

226136-0-0-PL 15 marca, 2019 11:06 AM

Endpoint-Solution-MOFU-ebook-final