FORTINET

Redukcja złożoności zabezpieczeń poprzez integrację i automatyzację

4 strategie dla CIO

Spis treści

FORTINET

Streszczenie

Dyrektorzy ds. informatycznych (CIO) przyspieszają cykle biznesowe i tworzą zupełnie nowe możliwości dzięki innowacyjnym narzędziom, takim jak aplikacje chmurowe czy procesy zaawansowanych operacji programistycznych (DevOps). Te same innowacje cyfrowe, które dramatycznie zwiększają wydajność, stwarzają jednak jednocześnie nowe ryzyko. Zwiększając szybkość i złożoność infrastruktury sieciowej, dyrektorzy ds. informatycznych muszą zatem brać pod uwagę także odpowiednie środki w zakresie cyberbezpieczeństwa, które odpowiednio ochronią ich systemy, dane i użytkowników w obliczu szybkich zmian. Fortinet pomaga dyrektorom ds. informatycznych zredukować złożoność zabezpieczeń sieci, a także obniżyć koszty wynikające z ciągłego dodawania coraz większej liczby odizolowanych produktów w odpowiedzi na nowe zagrożenia i ryzyko.

01 Wstęp: złożoność jest wrogiem zabezpieczeń

Nie ma wątpliwości, że dyrektorzy ds. informatycznych wykorzystują innowacje strategiczne jako drogę do większej wydajności i efektywności biznesowej. Transformacyjne technologie cyfrowe stwarzają nowe możliwości i napędzają rozwój we wszystkich branżach. Przełomowe rozwiązania, takie jak aplikacje chmurowe, urządzenia należące do Internetu rzeczy (IoT), a także wewnętrzne lub zewnętrzne usługi związane z operacjami programistycznymi (DevOps) pomagają zwiększyć wydajność, poprawić skalowalność, zmniejszyć koszty i skrócić czas wprowadzania produktów na rynek dzięki automatyzacji.

Wpływ tych zmian na organizacje nie jest jednak wyłącznie pozytywny. Sieci stają się coraz bardziej złożone, a to wpływa na zwiększenie powierzchni ataku oraz skali narażenia na ryzyko. Korzystanie z zabezpieczeń, które są fragmentaryczne i działają w sposób silosowy, jest nieefektywne, kosztowne i nie gwarantuje spełnienia wymagań w zakresie bezpieczeństwa lub zgodności. Według ostatniego badania przeprowadzonego wśród dyrektorów ds. informatycznych w przedsiębiorstwach, 77% organizacji polega w jakimś stopniu na niezintegrowanych, punktowych zabezpieczeniach — w całym systemie bezpieczeństwa pozostają więc luki, które wpływają ujemnie na jego efektywność[1].

Sytuację komplikują dodatkowo wymogi coraz bardziej rygorystycznych przepisów, takich jak unijne rozporządzenie o ochronie danych (RODO) oraz standardy bezpieczeństwa, definiowane na przykład w USA przez Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology, NIST). Organizacje generują ogromne ilości danych, którymi muszą skutecznie zarządzać, dbając o zachowanie zgodności z przepisami. Staje się to jeszcze trudniejsze, jeżeli wziąć pod uwagę prywatne urządzenia pracowników, korzystanie z nieaktualizowanego oprogramowania (zjawisko „Shadow IT") oraz konieczność zarządzania dostawcami lub partnerami, którzy w pewnym zakresie także mają dostęp do sieci organizacji[2].

Te wpływające na siebie wzajemnie i działające często sprzecznie siły sprawiają, że od dyrektorów ds. informatycznych wymaga się coraz lepszej znajomości technologii i przywództwa w tym zakresie[3]. Aby dotrzymać tempa zmianom, mogą oni zacząć rozwiązywać problemy związane ze złożonością zabezpieczeń poprzez skoncentrowanie się na czterech strategicznych obszarach rozwiązań:

- **Zintegrowane zabezpieczenia**
- **Automatyzacja zadań związanych z zabezpieczeniami**
- **Automatyzacja zarządzania zgodnością**
- **Uproszczenie zarządzania ryzykiem**

78%

dyrektorów ds. informatycznych uważa, że skuteczność ich strategii cyfrowej jest co najwyżej umiarkowana[4].

02 Zintegrowane zabezpieczenia

Problemem jest nie tylko zwiększanie się powierzchni ataku. Zaawansowane zagrożenia ukierunkowane na luki w zabezpieczeniach sieci stają się nie tylko coraz liczniejsze, ale także coraz bardziej wyrafinowane. Powszechne stosowanie punktowych zabezpieczeń w celu eliminowania nowych luk w zabezpieczeniach w sposób doraźny i reaktywny powoduje, że w większości organizacji infrastruktura zabezpieczeń jest niezintegrowana.

Taki brak integracji jest dla dyrektorów ds. informatycznych źródłem dwóch istotnych problemów. Po pierwsze sprawia, że wiedza na temat zagrożeń jest ograniczona. Działające w sposób izolowany zabezpieczenia nie pozwalają udostępniać informacji o potencjalnych zagrożeniach w całej organizacji, skoordynowanie reakcji na ataki wielopunktowe odbywa się więc wolno i jest nieefektywne. Po drugie, brak integracji zmusza organizacje do polegania w zbyt dużym stopniu na ręcznie realizowanych procesach, nadzorowanych przez już przeciążonych pracowników zespołu ds. zabezpieczeń. „Ręczne” kompilowanie danych o zagrożeniach i ścieżek audytu niezbędnych dla zachowania zgodności z wymaganiami co do sprawozdawczości jest — w porównaniu z podobnymi funkcjami zautomatyzowanymi udostępnianymi przez zintegrowaną architekturę zabezpieczeń — czasochłonne, kosztowne i podatne na błędy.

Zintegrowana architektura zabezpieczeń łączy różne produkty w spójny system, który w czasie rzeczywistym udostępnia informacje o zagrożeniach we wszystkich częściach organizacji. To natomiast umożliwia:

- Stosowanie wbudowanych interfejsów programistycznych aplikacji (API), a także możliwość szybkiej integracji API spoza architektury z API wykorzystującymi zmianę stanu poprzez reprezentacje (REST).
- Scentralizowane zarządzanie (jedna konsola) zapewniające pełną widoczność danych o stanie sieci oraz stosowanie spójnych zasad kontroli we wszystkich rozwiązaniach w zakresie bezpieczeństwa w całej organizacji.
- Budowę otwartego ekosystemu, który może zawierać rozwiązania innych firm, aby zmaksymalizować zwrot z istniejących inwestycji w bezpieczeństwo.
- Zmniejszenie złożoności i kosztów wynikających z dodawania bardziej izolowanych produktów w odpowiedzi na nowe rodzaje ryzyka.
- Stworzenie podstaw dla automatyzacji funkcji związanych z bezpieczeństwem (co jest chyba najważniejsze).

Brak kompleksowej integracji stanowi obecnie największe zagrożenie bezpieczeństwa dla prawie jednej trzeciej (32%) dyrektorów ds. informatycznych[5].

03 Automatyzacja pracy związanej z zabezpieczeniami

Badanie przeprowadzone niedawno wśród dyrektorów ds. informatycznych z całego świata wykazało, że 65% z nich uważa niedobór wykwalifikowanych pracowników za czynnik hamujący rozwój ich organizacji[6]. Automatyzacja może pomóc rozwiązać ten problem poprzez zmniejszenie obciążenia pracowników zespołów ds. zabezpieczeń oraz skalowanie ograniczonych zestawów umiejętności. Dzięki temu mogą oni skupić się na „miększych" inicjatywach, takich jak zarządzanie ryzykiem i działalnością.

Realizowane ręcznie procesy i zadania, takie jak wdrażanie i udostępnianie, analizowanie ostrzeżeń o zagrożeniach lub zarządzanie dostępem użytkowników i urządzeń, można zautomatyzować i koordynować za pomocą środków kontroli opartych na politykach. Dyrektorzy ds. informatycznych mogą zaspokoić potrzeby w zakresie automatyzacji w dwóch głównych obszarach organizacji pracy związanej z reagowaniem na incydenty.

Potrzeby w zakresie automatyzacji w **centrum zarządzania siecią (NOC)** mogą obejmować:

- kontrolę zabezpieczeń DevOps, która pomaga skrócić (zamiast wydłużyć) czas wprowadzania produktów na rynek;
- bezobsługowe wdrażanie rozwiązań w organizacjach rozproszonych;
- zarządzanie dostępem dla urządzeń i użytkowników;
- wgląd w czasie rzeczywistym w informacje o wydajności sieci w oddziałach, co ułatwia zarządzanie skokami obciążenia, skalowaniem i kierowaniem ruchem w oparciu o priorytety.

Potrzeby w zakresie automatyzacji w **centrum zarządzania bezpieczeństwem (SOC)** mogą obejmować:

- proaktywne wykrywanie zagrożeń;
- korelację zagrożeń i wymianę informacji o nich;
- alerty oraz badania i analizy zagrożeń;
- reagowanie na wydarzenia i łagodzenie ich skutków.

67%

dyrektorów ds. informatycznych planuje wykorzystać automatyzację, aby wyeliminować potrzebę zatrudniania dodatkowych osób[7].

04 Automatyzacja zarządzania zgodnością

Dyrektorzy ds. informatycznych powinni szukać sposobów automatyzacji zarządzania zgodnością. Skumulowane obciążenia związane z ręcznym śledzeniem i raportowaniem, wynikające z wymogów standardów branżowych oraz przepisów dotyczących ochrony prywatności, są dla organizacji czasochłonne i kosztowne.

Ponieważ na organizacje naruszające RODO nałożono już pierwsze wysokie kary[8], kwestią priorytetową dla kadry kierowniczej i zarządu powinno być zachowanie zgodności z przepisami. Większość organizacji musi udostępniać ścieżki audytu, aby dowieść zachowania zgodności z przepisami dotyczącymi prywatności danych, w tym RODO, nową ustawą o ochronie prywatności konsumentów w Kalifornii (California Consumer Privacy Act, CCPA), a także obowiązującymi przepisami branżowymi, takimi jak standard zabezpieczeń obowiązujący w sektorze kart płatniczych (Payment Card Industry Data Security Standard, PCI DSS), ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (Health Insurance Portability and Accountability Act, HIPAA) oraz ustawa Sarbanesa-Oxleya (SOX).

Zapewnienie zgodności z wymogami dotyczącymi prywatności danych w całym cyklu ich życia jest dla firm korzystne: organizacje mogą dzięki temu wykazać, że zasługują na zaufanie klientów[9]. Dyrektorzy ds. informatycznych niezmiennie ponoszą zaś odpowiedzialność za zachowanie prywatności danych klientów — bezpośrednio lub pośrednio[10]. Problemy z wglądem w dane (np. zjawisko Shadow IT, czyli korzystanie z rozwiązań niezatwierdzonych przez dział IT firmy) stają się coraz bardziej powszechne. Zapewnienie i utrzymanie zgodności staje się więc zadaniem coraz bardziej złożonym: dyrektorzy ds. informatycznych muszą zapewnić, że informacje poufne nie będą przechowywane w systemach stron trzecich bez odpowiedniego nadzoru[11].

Warto szukać rozwiązań w zakresie bezpieczeństwa, które zapewniają zarówno wgląd w dane, jak i sprawność (zwinność) pozwalającą na ich skalowanie w rosnącej i zmieniającej się sieci. System obrony musi być także elastyczny, aby można było dostosować go do zmieniających się wymagań w zakresie bezpieczeństwa i zgodności z przepisami bez modernizowania architektury infrastruktury bezpieczeństwa. Obejmuje to sprawozdawczość uwzględniającą wszystkie elementy rozwiązania w celu wyeliminowania procesów ręcznego pobierania plików dziennika i marnowania czasu pracowników. Zautomatyzowane funkcje śledzenia i raportowania w zakresie zgodności pozwalają udostępniać niestandardowe pulpity osobom na konkretnych stanowiskach kierowniczych i zarządowi, co ułatwia sprawowanie nadzoru wewnętrznego.

69%

firm uważa, że wymogi w zakresie zgodności powodują wzrost wydatków[12].

05 Uproszczenie zarządzania ryzykiem

Dyrektorzy ds. informatycznych muszą także przestrzegać norm bezpieczeństwa stosowanych w celu zarządzania ryzykiem i jego oceny, definiowanych przez **NIST**, **Międzynarodową Organizację Normalizacyjną (International Organization for Standardization, ISO)** czy **Center for Internet Security (CIS)**. Wiele z nich staje się de facto normami państwowymi. Szacuje się na przykład, że do 2020 r. około 50% wszystkich organizacji amerykańskich wdroży wymogi NIST dotyczące oceny, śledzenia i raportowania stanu bezpieczeństwa. Dotyczy to podmiotów działających w branżach opieki zdrowotnej, handlu detalicznego, usług finansowych i we wszystkich sektorach infrastruktury krajowej o kluczowym znaczeniu[13].

Narzędzia i usługi służące do **oceny ryzyka w oparciu o analizy** oferują dynamiczne oceny luk w zabezpieczeniach i zestawienia porównawcze, które pomagają dyrektorom ds. informatycznych wizualizować aktualny stan narażenia na zagrożenia w całej organizacji. Punktowa ocena ryzyka zapewnia mierzalne punkty odniesienia i pomaga sformułować konkretne zalecenia dotyczące konfiguracji, ułatwiające zarządzanie wskaźnikami ryzyka oraz doskonalenie podejścia do bezpieczeństwa w firmie. Wieloczynnikowa ocena ryzyka może uwzględniać w szczególności potencjalne luki w zabezpieczeniach. Odbywa się to poprzez analizę częstotliwości dostępu, aktywności użytkowników, sposobu rozprzestrzeniania się i skali zagrożeń, co pozwala na priorytetowe traktowanie kwestii prywatności na podstawie ryzyka[14].

Możliwości dostępne dzięki **segmentacji ukierunkowanej na cele** (ang. intent-based segmentation) pomagają natomiast „przełożyć” intencje biznesowe na konkretne zasady dotyczące miejsca, sposobu i zakresu segmentacji zabezpieczeń („gdzie”, „jak” i „co”), pozwalające kontrolować dostęp do danych wrażliwych i systemów o szczególnym znaczeniu. Segmentacja ukierunkowana na cele umożliwia szczegółową kontrolę dostępu, dostosowywaną na podstawie systematycznie prowadzonej oceny zaufania do użytkowników. W ramach zintegrowanej architektury zabezpieczeń segmentacja tego typu może skutecznie poprawić „zdolności obronne” organizacji, złagodzić ryzyko, ułatwiać zachowanie zgodności z przepisami, a także zwiększyć wydajność operacyjną.

W przeprowadzonym niedawno badaniu dyrektorzy ds. informatycznych deklarowali, że główną miarą ich sukcesu jest zarządzanie ryzykiem w zakresie cyberbezpieczeństwa[15].

06 Zmniejszanie złożoności zabezpieczeń (lista kontrolna z podsumowaniem)

Rozwijając architekturę zabezpieczeń w celu zwiększenia prostoty i skuteczności, dyrektorzy ds. informatycznych powinni — w obrębie czterech omówionych wyżej ogólnych obszarów — szukać sześciu konkretnych możliwości:

- ☐ Integracja łącząca zróżnicowane produkty w spójną, inteligentną architekturę zabezpieczeń.
- ☐ Zarządzanie z poziomu jednej konsoli: scentralizowany wgląd w informacje i kontrola całej infrastruktury zabezpieczeń.
- ☐ Funkcje lub rozwiązania, które pozwalają zautomatyzować procesy w celu uproszczenia zadań takich jak wdrażanie, zarządzanie dostępem i analizowanie zagrożeń pod kątem zwiększenia świadomości kontekstowej.
- ☐ Zautomatyzowane funkcje śledzenia i sprawozdawczości w zakresie zgodności.
- ☐ Ocena ryzyka oparta na analizach wykorzystywana do pomiaru stopnia narażenia na zagrożenia oraz do zarządzania nimi w czasie rzeczywistym.
- ☐ Segmentacja ukierunkowana na cele, umożliwiająca opartą na politykach kontrolę wewnętrznego ruchu sieciowego.

[1] „State of the CIO and Security Report". Fortinet, marzec 2019 r.

[2] Jennifer Lonoff Schiff, „5 biggest IT compliance headaches and how to address them", CIO, 9 maja 2018 r.

[3] „Role Of CIO Is Changing And Growing In Importance, Say New Forbes Insights Studies", Forbes, 28 marca 2018 r.

[4] „CIO Survey 2018: The Transformational CIO", Harvey Nash and KPMG, 25 maja 2018 r.

[5] „State of the CIO and Security Report", Fortinet, marzec 2019 r.

[6] „CIO Survey 2018: The Transformational CIO", Harvey Nash and KPMG, 25 maja 2018 r.

[7] „CIO Survey 2018: The Transformational CIO", Harvey Nash and KPMG, 25 maja 2018 r.

[8] Adam Satariano, „Google Is Fined $57 Million Under Europe's Data Privacy Law", The New York Times, 21 stycznia 2019 r.

[9] Nancy Couture, „How data governance can support data privacy compliance", CIO, 7 lutego 2019 r.

[10] „State of the CIO and Security Report", Fortinet, marzec 2019 r.

[11] „CIO Survey 2018: The Transformational CIO", Harvey Nash and KPMG, 25 maja 2018 r.

[12] Josh Fruhlinger, „Top cybersecurity facts, figures and statistics for 2018", CSO, 10 października 2018 r.

[13] Jonathan Nguyen-Duy, „The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About", Fortinet, 21 sierpnia 2018 r.

[14] Nancy Couture, „How data governance can support data privacy compliance", CIO, 7 lutego 2019 r.

[15] „State of the CIO and Security Report", Fortinet, marzec 2019 r.

www.fortinet.com

323378-0-A-PL

listopada 18, 2019 11:45 AM

ebook-untangling-security-complexity_PL