ZAPEWNIENIE NOWOCZESNYCH MECHANIZMÓW OCHRONY DANYCH NA POTRZEBY RODO

Siedem kwestii do rozważenia i rozwiązania Fortinet

Duże wymogi i wysokie kary pieniężne narzucone przez unijne ogólne rozporządzenie o ochronie danych (RODO) przyciągnęły uwagę osób odpowiedzialnych za zabezpieczenia IT na całym świecie. Dla przedsiębiorstw prowadzących działalność gospodarczą w Unii Europejskiej nadszedł czas na wzmocnienie stosowanych mechanizmów zabezpieczeń.

Przestrzeganie przepisów RODO wymaga stosowania nowoczesnych technologii pozwalających na skuteczną ochronę danych, a zwłaszcza zaawansowanych mechanizmów zapobiegania przypadkom i wykrywania przypadków zagrożeń w celu minimalizowania możliwości naruszenia ochrony danych. Według organizacji non-profit Center for Internet Security (CIS) większość skutecznych ataków wykorzystuje niedociągnięcia w zakresie cyberhigieny[1].

Przedsiębiorstwa objęte przepisami RODO muszą zatem stosować odpowiednie rozwiązania, aby chronić swoje środowiska oraz szybko i efektywnie wykrywać i ograniczać skutki naruszeń ochrony danych. Punktem wyjścia do tych działań jest wdrożenie właściwej architektury bezpieczeństwa.

1. **Pierwsza linia obrony**. Pierwszą linią obrony przed włamaniami mającymi na celu uzyskanie dostępu do danych osobowych jest zapora następnej generacji (NGFW). Jej najbardziej istotne funkcje dla przedsiębiorstw objętych RODO to m.in.:

- Wielowarstwowe zabezpieczenia z zaawansowanymi mechanizmami zapobiegania zagrożeniom, które pozwalają na ochronę całej powierzchni ataku, w tym wszystkich aplikacji, użytkowników i urządzeń. Chronione są zatem m.in. urządzenia wchodzące w skład Internetu rzeczy — z których wiele zaprojektowano bez przywiązywania większej wagi do kwestii zabezpieczeń (z tego względu poprawki zabezpieczeń mogą nie być w tym przypadku skuteczne) — oraz stale zwiększająca się liczba aplikacji SaaS i innych rozwiązań chmurowych.
- Wydajny system zabezpieczeń (ang. security processor, SPU) dla usług warstwy aplikacji, który chroni sieć przedsiębiorstwa oraz wykrywa (za pomocą najszybszego w branży mechanizmu inspekcji) naruszenia ochrony danych mające swoje źródło w ruchu SSL.
- Funkcje zapewnienia widoczności i zarządzania z poziomu jednej konsoli na potrzeby uproszczonego wdrażania i spójnego stosowania zabezpieczeń. Pozwalają one na wymianę informacji o włamaniach w czasie rzeczywistym, co skraca czas wykrycia, neutralizacji i powstrzymania prób naruszenia ochrony danych.
- Segmentacja ruchu sieciowego, która minimalizuje zasięg i głębokość włamań oraz szanse atakującego na uzyskanie dostępu do chronionych danych.

Zapory NGFW Fortinet FortiGate to uznane w branży, idealne rozwiązania służące do ochrony sieci przed włamaniami i naruszeniami ochrony danych. W swoim raporcie Magic Quadrant 2017 firma Gartner uznała Fortinet za lidera w zakresie zapór dla przedsiębiorstw[2], a zapory FortiGate są czwarty rok z rzędu rekomendowane przez firmę NSS Labs[3].

2. **Ochrona punktów końcowych.** Jeśli zapory stanowią pierwszą linię obrony, zabezpieczenia punktów końcowych tworzą drugą linię obrony. W miarę jak sieci przedsiębiorstw obejmują coraz większą liczbę różnych typów punktów końcowych stosowanie nowoczesnych zabezpieczeń tych punktów ma kluczowe znaczenie w kontekście ochrony danych, w tym danych osobowych. Tradycyjne oprogramowanie chroniące wyłącznie przed wirusami i złośliwym oprogramowaniem nie jest już wystarczające. Rozwiązanie Fortinet FortiClient nie tylko zwiększa możliwości przedsiębiorstwa w zakresie zapobiegania naruszeniom ochrony danych, ale również pozwala spełnić określone w RODO wymogi dotyczące zgłaszania ewentualnych przypadków takich naruszeń. Istotne funkcje tego rozwiązania to m.in.:

- Mechanizmy ochrony przed zaawansowanymi zagrożeniami mogącymi prowadzić do naruszenia ochrony danych, w tym mechanizm monitorowania pamięci, dzięki któremu FortiClient może wykrywać i blokować ataki na istniejące luki w zabezpieczeniach aplikacji.
- Natywna integracja z architekturą zabezpieczeń Fortinet Security Fabric na potrzeby przeprowadzanych w czasie rzeczywistym aktualizacji danych o pojawiających się zagrożeniach. Skuteczne powstrzymywanie ataków i zapobieganie włamaniom sprawia, że z dużym wyprzedzeniem eliminowane jest ryzyko naruszenia ochrony danych.
- Dobra widoczność stanu zabezpieczeń wdrożonych w punktach końcowych w całym przedsiębiorstwie oraz ewentualnych luk w zabezpieczeniach wykrytych na powierzchni ataku. Wszelkie aktualizacje są dostępne za pośrednictwem ostrzeżeń e-mail i konsoli pozwalającej na śledzenie luk w zabezpieczeniach. Uzyskanie zdolności do zarządzania zabezpieczeniami punktów końcowych pozwala przedsiębiorstwu na szybsze i skuteczniejsze zapobieganie oraz ograniczanie skutków ataków, a także na przeciwdziałanie samym atakom.

Podobnie jak w przypadku zapory NGFW FortiGate, FortiClient również zyskał uznanie branży i m.in. w 2017 r. był rekomendowany przez firmę NSS Labs w kategorii zaawansowanych mechanizmów ochrony punktów końcowych[4].

3. **Ochrona poczty e-mail.** Zabezpieczenie poczty elektronicznej jest bardzo ważne, z ostatnich danych wynika bowiem, że to za jej pomocą na komputerach instalowane jest dwie trzecie złośliwego oprogramowania[5]. Jeśli przedsiębiorstwo chce zabezpieczyć swoją sieć i dane przed cyberatakami, musi wdrożyć bezpieczną bramę poczty e-mail (SEG). Zaawansowana brama SEG Fortinet FortiMail chroni przedsiębiorstwo przed oprogramowaniem szyfrującym dane w celu wymuszenia okupu (ang. ransomware attack), phishingiem i innymi zagrożeniami dla bezpieczeństwa danych osobowych za pomocą rożnych technologii, z których najważniejsze to m.in.:

- Wielowarstwowa technologia antyspamowa korzystająca z ponad dwunastu technik inspekcji nadawców, protokołów i treści (w tym technik oceny numerów IP i domen, weryfikacji odbiorców oraz kontroli w ramach systemu SPF) w celu ochrony sieci i użytkowników przed niechcianymi, masowymi wiadomościami e-mail. Wiadomości takie często zawierają w sobie programy wykorzystujące luki w zabezpieczeniach, należy zatem uniemożliwić im dostanie się do sieci pocztowej przedsiębiorstwa.
- Oprogramowanie chroniące przed złośliwym oprogramowaniem, które korzysta m.in. ze statycznych i dynamicznych technik opartych na analizie sygnatur, zachowań i algorytmów heurystycznych. Podobnie jak w przypadku technologii antyspamowej, tutaj również chodzi o to, aby złośliwe oprogramowanie nie dostało się do skrzynek odbiorczych użytkowników, a tym samym do sieci przedsiębiorstwa.
- Zaawansowany zestaw funkcji ochrony danych, w tym mechanizmy ochrony przed utratą danych oraz funkcje szyfrowania i archiwizowania wiadomości e-mail. Każde przedsiębiorstwo, które chce uchronić się przed naruszeniami ochrony danych, musi dopilnować, aby użytkownicy szyfrowali wiadomości e-mail zawierające dane osobowe oraz nie wysyłali pocztą e-mail żadnych poufnych i prywatnych danych.

Rozwiązanie FortiMail jest cenione za wyjątkowo skuteczne wykrywanie zagrożeń i uzyskało m.in. wydawany przez firmę ICSA Labs certyfikat Advanced Threat Defense (po zablokowaniu w teście laboratoryjnym niemal 750 niepowtarzalnych, nowych i mało znanych zagrożeń)[6].

4. **Ochrona aplikacji sieciowych.** Aby uczynić z aplikacji sieciowych bramy dostępowe do sieci przedsiębiorstwa, hakerzy stosują wiele zaawansowanych technik takich jak wstrzyknięcie kodu SQL, osadzenie w treści atakowanej strony fałszywego kodu (ang. cross-site scripting), przepełnienie bufora i zatrucie plików cookie. Ochrona danych osobowych przed tymi zagrożeniami wymaga wielowarstwowego podejścia do bezpieczeństwa aplikacji sieciowych. Zapory aplikacji sieciowych FortiWeb chronią przedsiębiorstwa przed złośliwymi włamaniami na wiele różnych sposobów, z których najważniejsze to:

- Zastosowanie wielu warstw zabezpieczeń identyfikujących zagrożenia m.in. za pomocą funkcji analizy reputacji adresu IP, ochrony przed atakami DDoS, weryfikacji protokołów, analizy sygnatur ataków, ochrony antywirusowej i ochrony przed utratą danych. W tym przypadku celem jest również prewencyjne powstrzymanie prób włamania, aby wyeliminować możliwość naruszenia ochrony danych.
- Użycie mechanizmu wykrywania zagrożeń na podstawie zachowań odbiegających od typowych wzorców obserwowanych w ruchu sieciowym. Ma to szczególne znaczenie w przypadku identyfikowania nieznanych zagrożeń.
- Macierzysta integracja z architekturą Fortinet Security Fabric, która pozwala na regularne otrzymywanie oraz dalszą wymianę najnowszych informacji na temat pojawiających się zagrożeń. Jak już wspomniano, cyberhigiena jest podstawą każdej strategii ochrony przed włamaniami (IPS) i wykrywania włamań.

Podobnie jak inne omówione tu rozwiązania Fortinet, zapory FortiWeb w 2017 r. również były rekomendowane przez firmę NSS Labs w kategorii zapór aplikacji sieciowych[7].

5. **Kompleksowe zarządzanie i raportowanie.** W 2016 r. cyberprzestępca, który naruszył sieć przedsiębiorstwa, miał średnio 107 dni na dokonanie spustoszeń, zanim fakt takiego włamania został wykryty[8]. Ograniczenie czasu dostępnego włamywaczowi na poruszanie się po sieci zmniejsza jego szanse na naruszenie ochrony danych. Szybkość, z jaką przedsiębiorstwo jest zdolne do wykrycia i ograniczenia skutków włamania, odgrywa zatem kluczową rolę w procesie zapobiegania utracie danych.

   Aby skutecznie zamknąć ewentualnym przestępcom takie „okno możliwości", przedsiębiorstwo musi dopilnować, aby wszystkie jego zabezpieczenia działały nieprzerwanie. W związku z powyższym Fortinet oferuje pakiet produktów (FortiManager, FortiAnalyzer, FortiSIEM i FortiCloud), które wdrożone razem pozwalają scentralizować zarządzanie zabezpieczeniami w ramach całej sieci. Jego podstawowe funkcje to m.in.:

- Usprawniony wgląd w zasady zabezpieczeń i funkcje zarządzania urządzeniami. FortiManager pozwala pracownikom zajmującym się siecią i zabezpieczeniami na inicjowanie i synchronizowanie skoordynowanej reakcji na wykryte zagrożenia oraz zarządzanie zasadami bezpieczeństwa w ramach wszystkich urządzeń (w tym urządzeń Fortinet i urządzeń innych producentów) wchodzących w skład architektury Fortinet Security Fabric. Ponadto FortiManager zapewnia najlepszą w branży skalowalność, umożliwiając zarządzanie z poziomu jednej konsoli nawet 100 tys. urządzeń Fortinet (z wyłączeniem urządzeń innych producentów), które wchodzą w skład wspomnianej architektury. W tym przypadku od szybkości reakcji na incydenty często zależy powstrzymanie lub zminimalizowanie skutków naruszenia ochrony danych, co ma kluczowe znaczenie w kontekście RODO.
- Scentralizowana widoczność danych z rejestrów i informacji o zdarzeniach przesyłanych przez mechanizmy zabezpieczeń wdrożone w całym przedsiębiorstwie. Rozwiązanie FortiAnalyzer automatycznie pobiera i analizuje rejestry zabezpieczeń i powiadamia (za pomocą odpowiednich pulpitów i alertów) osoby odpowiedzialne za zabezpieczenia IT o ewentualnie wykrytych oznakach naruszeń. Również w tym przypadku zdolność do szybkiej reakcji na incydenty ma kluczowe znaczenie w kontekście RODO.
- Narzędzia analityczne służące do agregacji i krzyżowej korelacji informacji pochodzących z różnych źródeł takich jak dzienniki, dane o wydajności i zdarzenia (SNMP Trap). Rozwiązanie FortiSIEM w sposób dynamiczny automatycznie wykrywa fizyczne i wirtualne systemy podłączone do sieci i przesyła informacje o konfiguracji tych systemów do centralnej bazy danych do zarządzania konfiguracją (CMDB). Dzięki wspomnianej krzyżowej korelacji tych danych FortiSIEM zapewnia całościowy widok zagrożeń na całej powierzchni ataku.
- Widoczność systemów zabezpieczeń z dowolnego miejsca na świecie. FortiCloud udostępnia panel zarządzania, który umożliwia centralne sterowanie, lub nawet wdrażanie, wszystkich urządzeń obsługujących architekturę Fortinet Security Fabric, w tym urządzeń Fortinet i urządzeń innych producentów. Zdolność do tak szybkiego wdrażania urządzeń i zarządzania nimi może decydować o powodzeniu lub niepowodzeniu włamania lub naruszenia ochrony danych.

6. **Warstwa bezpiecznego dostępu.** Liczba i typy urządzeń podłączonych do sieci przedsiębiorstw nadal rośnie w postępie geometrycznym. Użytkownicy tych urządzeń chcą korzystać z szybkich sieci Wi-Fi, ale przedsiębiorstwa również muszą zabezpieczyć dostęp bezprzewodowy do swoich sieci, aby zmniejszyć prawdopodobieństwo włamania i późniejszego naruszenia ochrony danych. Funkcje oferowane w tym zakresie przez rozwiązania Fortinet Secure Access to m.in.:

- Scentralizowane zarządzanie tożsamością i identyfikowanie użytkowników. Rozwiązanie FortiAuthenticator korzysta z szeregu metod identyfikacji użytkowników, aby zapewnić, że urządzenia podłączone do sieci przedsiębiorstwa otrzymują wyłącznie uprawnienia dostępu przypisane do konkretnej roli.
- Bezpieczne przełączniki dostępowe zapewniające dodatkową warstwę zabezpieczeń. Rozwiązania FortiSwitch korzystają z funkcji wykrywania urządzeń, wykrywania nieautoryzowanych serwerów DHCP (ang. DHCP snooping) i zbierania danych z dzienników systemowych w celu skuteczniejszego zapobiegania włamaniom i lepszej ochronie danych w ramach zapór NGFW FortiGate.
- Rozwiązania z serii FortiToken generują zgodne ze standardami OATH, oparte na algorytmie TOTP tokeny służące jako przystępny cenowo drugi składnik systemu uwierzytelniania dwuskładnikowego. W ten sposób przedsiębiorstwa mogą dopilnować, że tylko osoby uprawnione będą mieć dostęp do określonych aplikacji.

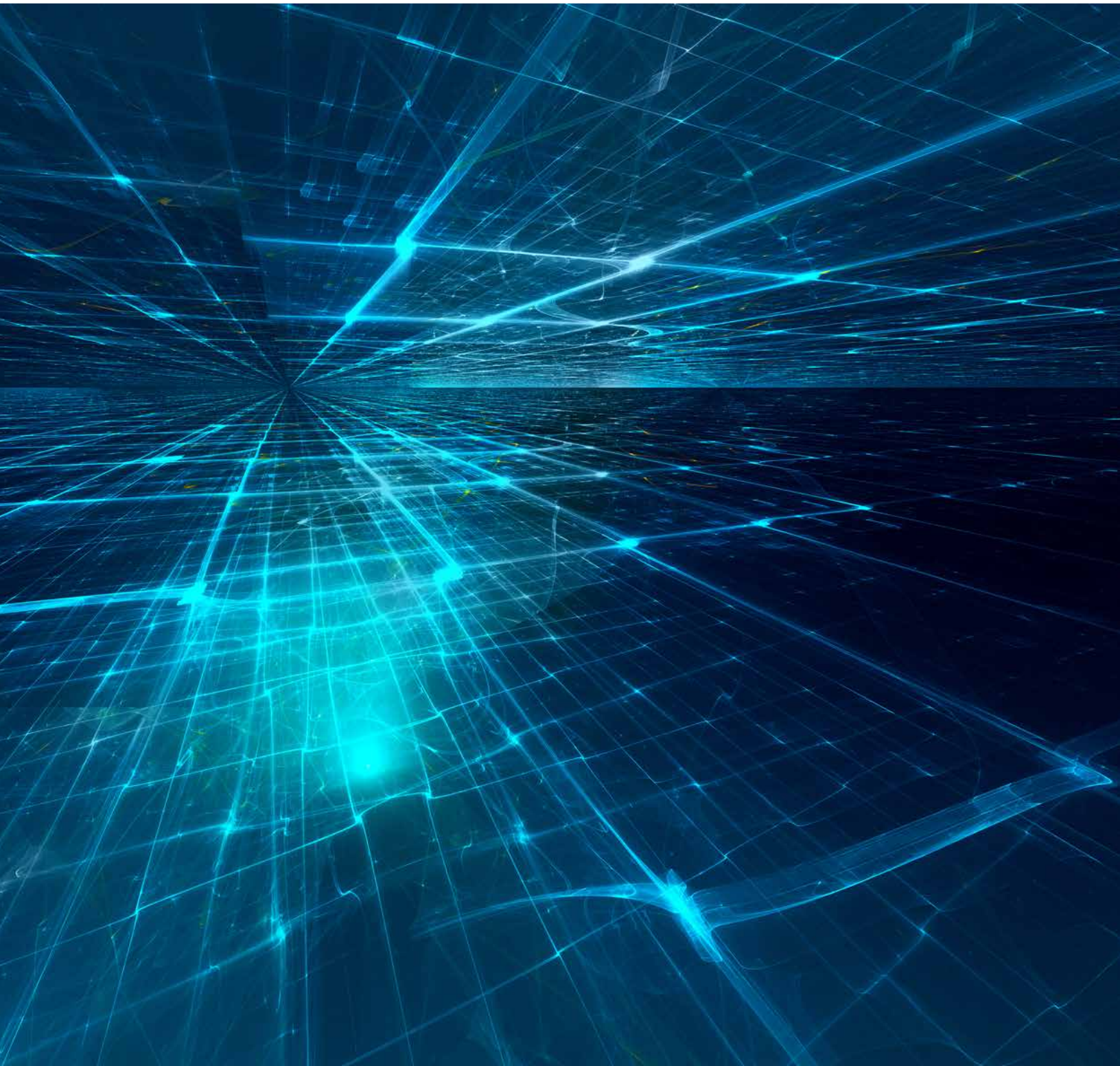
7. Zaawansowane funkcje ochrony przed zagrożeniami i wykrywania zagrożeń. Aby skutecznie chronić się przed włamaniami i je wykrywać oraz reagować na incydenty naruszenia ochrony danych, przedsiębiorstwa potrzebują odpowiednich narzędzi. Narzędzia te można podzielić na dwie grupy:

- **Narzędzia służące do informowania o zagrożeniach.** Systemy zabezpieczeń przedsiębiorstwa muszą w czasie rzeczywistym otrzymywać najnowsze, zaawansowane informacje o pojawiających się zagrożeniach, aby odpowiednio na takie zagrożenia reagować. Informacje takie może przesyłać zespół ekspertów z FortiGuard Labs, który korzysta w tym celu z dostępnych wyników specjalistycznych badań dotyczących nowych zagrożeń. Wszelkie aktualizacje produktów i poprawki są publikowane na bieżąco (priorytet mają konkretne ataki), co pozwala szybko usuwać wykryte luki w zabezpieczeniach.
- **Sandboxing.** Sandboxing to coraz częściej stosowana metoda eliminowania luk w zabezpieczeniach w drodze identyfikacji nieznanych wcześniej ataków. Za pomocą rozwiązania FortiSandbox przedsiębiorstwa nie tylko otrzymują automatyczne aktualizacje dotyczące pojawiających się zagrożeń, ale mogą również przesyłać w czasie rzeczywistym do swoich systemów zabezpieczeń własne aktualizacje. Wdrożenie rozwiązania FortiSandbox zapewnia dodatkową warstwę ochrony przed zagrożeniami w ramach całej architektury Fortinet Security Fabric. Podobnie jak inne produkty Fortinet, FortiSandbox to również dobry wybór, rekomendowany na przykład przez firmę NSS Labs w kategorii systemów wykrywania naruszeń bezpieczeństwa[9].

PODSUMOWANIE

Przedsiębiorstwa objęte przepisami RODO nie mają czasu do stracenia. Stosowanie punktowych produktów i platform zabezpieczeń nie jest dobrym rozwiązaniem w przypadku, gdy potrzebne są kompleksowe rozwiązania służące do wykrywania przypadków i zapobiegania przypadkom włamań i naruszenia ochrony danych. W tym kontekście najlepszym wyborem jest architektura Fortinet Security Fabric, której poszczególne składniki są najlepsze w swojej klasie, a po połączeniu zapewniają odpowiedni efekt synergii.

Wspomniana architektura zapewnia przedsiębiorstwu nie tylko widoczność i mechanizmy kontroli w czasie rzeczywistym, ale również możliwość całodobowego korzystania z usług FortiCare 360 obejmujących zaawansowaną pomoc techniczną oraz możliwość szybkiej wymiany sprzętu na wypadek ewentualnej awarii. Ma to szczególne znaczenie w kontekście naruszeń ochrony danych objętych przepisami RODO.



[1] John M. Gilligan, „It Is Time to Get Serious About Securing Our Nation's Critical Infrastructure", Center for Internet Security blog, 30 października 2017 r.

[2] Adam Hils, Jeremy D'Hoinne i Rajpreet Kaur, „Magic Quadrant for Enterprise Network Firewalls", Gartner, 10 lipca 2017 r.

[3] „Next Generation Firewall", NSS Labs, ocena dokonana 5 grudnia 2017 r.

[4] „Advanced Endpoint Protection", NSS Labs, ocena dokonana 5 grudnia 2017 r.

[5] „2017 Data Breach Investigations Report", Verizon, ocena dokonana 5 grudnia 2017 r.

[6] „Advanced Threat Defense Certification Testing Report", ICSA Labs, 2 października 2017 r.

[7] Matthew Chips, „Web Application Firewall Test Report", NSS Labs, 11 kwietnia 2017 r.

[8] „2017 Trustwave Global Security Report", czerwiec 2017 r.

[9] „Breach Detection System", NSS Labs, ocena dokonana 5 grudnia 2017 r.

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

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
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

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

150565-A-0-EN lutego 15, 2018 12:55 PM
Checklist_updated_GDPR_PL