Integrated Computing Standard

Bezpieczeństwo

#cyfroweewolucje

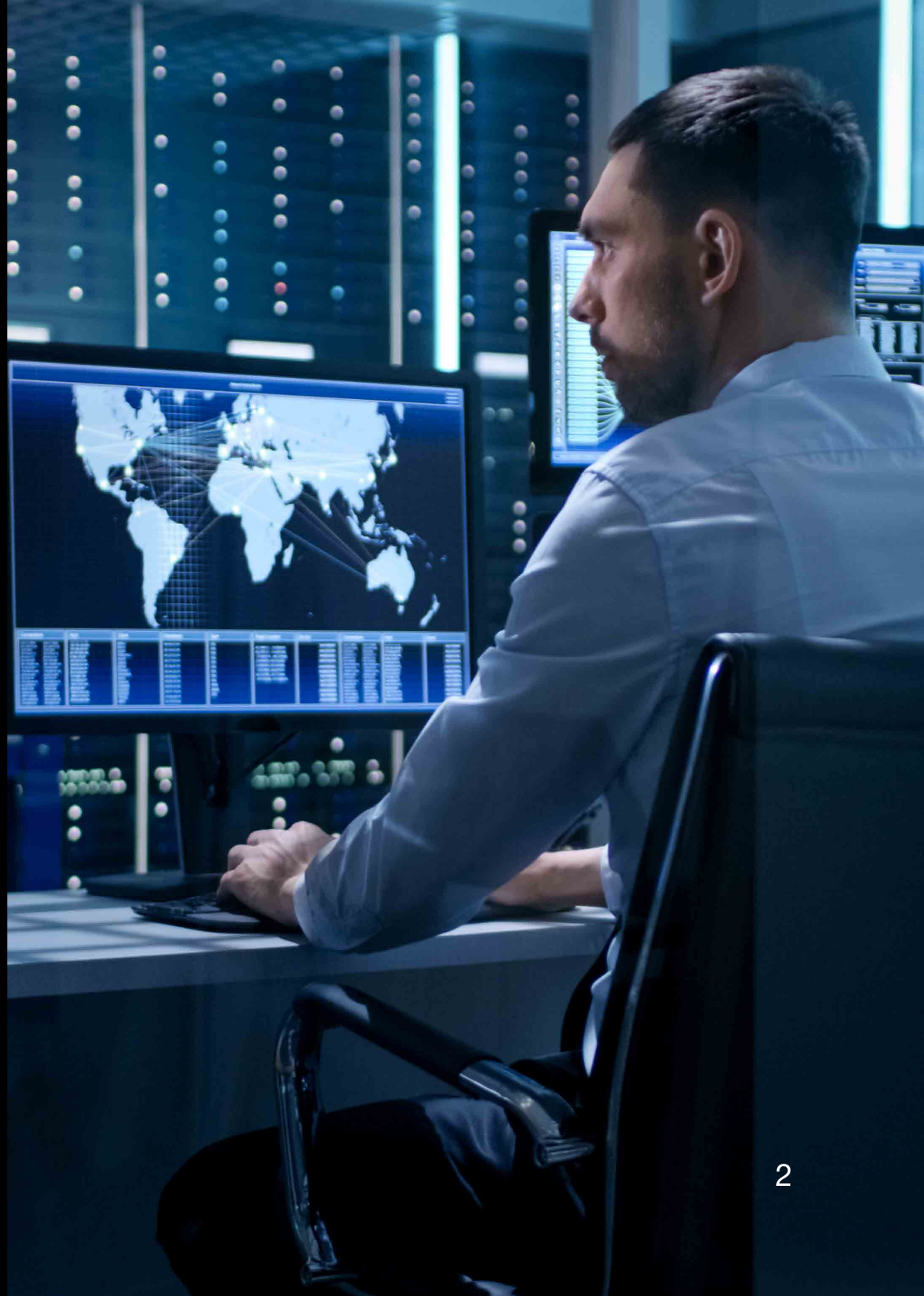
orange™

INTEGRATED SOLUTIONS

Bezpieczeństwo ponad wszystko

Bezpieczeństwo jest jednym z aspektów, które analizują firmy przy budowaniu swoich rozwiązań IT.
W chmurze jest dostępnych wiele narzędzi, dzięki którym możliwe jest zarządzanie bezpieczeństwem w sposób zintegrowany i monitorowanie jego poziomu.

Dzięki zatrudnionym przez operatorów centrów danych profesjonalistom wszystkie systemy teleinformatyczne przygotowane są na zarówno popularne, jak też najbardziej nietypowe rodzaje zagrożeń. Wszystko w celu zagwarantowania nieprzerwanej pracy systemów IT oraz świadczonych przez nie usług.



Gwarancja bezpieczeństwa

Na rynku pracy brakuje wielu ekspertów różnych dziedzin, a szczególnie tych zajmujących się bezpieczeństwem rozwiązań IT (większość tego typu osób zatrudnionych jest przez operatorów dużych centrów danych). Skala napotykanych tam wyzwań odpowiada ich zainteresowaniu, a także warunki zatrudnienia są korzystniejsze niż w przypadku mniejszych przedsiębiorstw.

Ale przewaga kompetencyjna to tylko jeden z elementów gwarancji bezpieczeństwa danych – wśród pozostałych są profesjonalne systemy ochrony sieci przed atakami, narzędzia do wykonywania kopii zapasowych danych oraz wiele rodzajów zabezpieczeń fizycznych przed włamaniem, pożarem czy zalaniem budynku.

Neutralizacja ataków na infrastrukturę przedsiębiorstwa

Działania cyberprzestępcze globalnie przynoszą obecnie większy zysk niż handel narkotykami. Centra danych wydają się idealnym celem ataku – znajduje się w nich wiele cennych dla klientów danych.
Nic więc dziwnego, że nieustannie podejmowane są próby, których celem jest **kradzież informacji** lub zablokowanie dostępu do nich poprzez zaszyfrowanie w celu uzyskania okupu (**ransomware**) lub utrudnienie korzystania z serwisów internetowych (ataki **DDoS**).

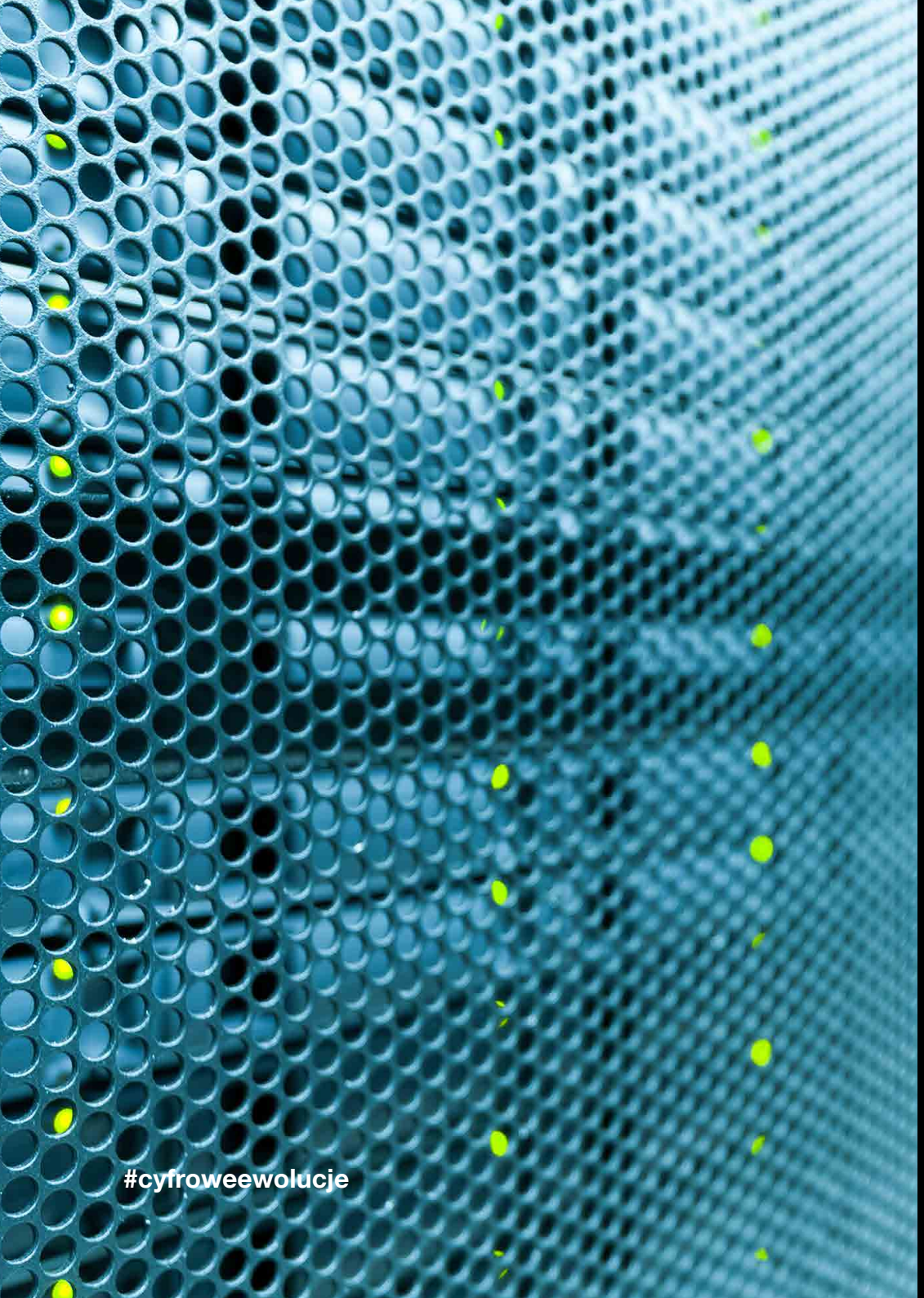
Doświadczeni w boju administratorzy potrafią skutecznie odpierać tego typu ataki, są też wspierani najlepszymi w swojej klasie rozwiązaniami zabezpieczającymi.

Dodatkowo – jeśli dostawca świadczy usługi integratorskie – klient może liczyć na pomoc w doborze bezpiecznych rozwiązań i przeprowadzenie przez instalację zabezpieczeń jego aplikacji.

Ochrona przed kradzieżą

Podczas gdy dla większości osób priorytetem jest zabezpieczenie środowiska IT przed cyberatakami, nie można zapominać, że na świecie wiele danych wyciekało w wyniku zwykłej kradzieży sprzętu. W tym zakresie przewaga profesjonalnych centrów danych jest nie do przecenienia: dostęp do budynku chroniony jest nie tylko przez uzbrojonych strażników, ale też skomplikowane systemy elektroniczne uwierzytelniania każdej osoby osoby przekraczającej drzwi kluczowe dla bezpieczeństwa danych. Oprócz tego sam sprzęt zainstalowany jest w profesjonalnie zabezpieczonych szafach komputerowych. Dane na twardych dyskach są szyfrowane, więc ewentualne wejście w posiadanie takich nośników nie przyniesie złodziejowi żadnej korzyści.

#cyfroweewolucje



Z dala od katastrofy

Co prawda wiele argumentów dotyczących katastrof naturalnych stosowanych w innych częściach globu nie znajduje zastosowania w Polsce (trzęsienie ziemi, tsunami), ale w ciągu ostatnich dziesięcioleci mieliśmy do czynienia z rozległymi powodziami, trudnymi do opanowania pożarami czy przypadkami katastrof budowlanych. Projektanci obiektów, w których znajdują się centra danych, zadbali o to, aby zminimalizować prawdopodobieństwo wystąpienia każdej z tych sytuacji. Ryzyko poważnego pożaru powinno być neutralizowane przez wdrożenie profesjonalnego i bardzo skutecznego systemu wykrywania i gaszenia gazem, który nie jest szkodliwy ani dla ludzi, ani dla znajdujących się w macierzach dyskowych i w serwerach danych. Budynki, w których znajdują się centra danych, zlokalizowane są z dala od terenów zalewowych, zaś ich konstrukcja praktycznie eliminuje możliwość zawalenia się.

Jak chronimy zasoby naszych klientów?

Inżynierowie Orange i Integrated Solutions na co dzień dbają o to, aby żadne dane klientów nie przedostały się w niepowołane ręce. W tym celu korzystają nie tylko ze swojej eksperckiej wiedzy, ale także z wielu rodzajów zaawansowanych narzędzi stworzonych przez liderów rynku cyberbezpieczeństwa.

Web Application Protection – ochrona serwerów WWW klienta przed zagrożeniami lub cyberatakami z internetu nakierowanymi na aplikacje WWW. Ataki te mają na celu kradzież danych, kradzież pieniędzy, złośliwe zakłócenie ciągłości działania, narażenie prestiżu klienta.

DDoS Protection – ochrona przed atakami typu „odmowa usługi" Distributed Denial of Service (DDoS). Zapewnia większe bezpieczeństwo korzystania z internetu poprzez monitorowanie przez operatora w sposób ciągły ruchu sieciowego i redukcję negatywnych skutków ataków.

Trzy opcje ochrony:

- **DDoS Protection Basic** – usługa ochrony przed atakami DDoS bazująca na automatycznej mitygacji ataku, wykorzystująca technologię FlowSpec BGP do zablokowania ataku.

- **DDoS Protection Standard** – usługa ochrony przed atakami DDoS bazująca na automatycznej mitygacji ataku, do czyszczenia ataku wykorzystywane jest tzw. scrubbing center.

- **DDoS Protection Premium** – zakres Standard rozszerzony o wsparcie Security Operations Center. Umożliwia ocenę przez SOC w porozumieniu z klientem, czy zagrożenie jest związane z rzeczywistym atakiem DDoS oraz tzw. „ręczną" mitygację ataku DDoS.

SOC/SIEM aaS + SOAR – zapewnia kompleksowe wsparcie procesów zarządzania bezpieczeństwem operacyjnym u klienta. Wysoko wykwalifikowany zespół ekspertów Orange SOC zapewnia całodobowe (24/7/365) monitorowanie bezpieczeństwa procesów biznesowych oraz powiązanych z nimi systemów technologicznych.

Cloud security – usługa platformowa zapewniająca kompleksowe mechanizmy zarządzania bezpieczeństwem w środowiskach chmurowych i centrach przetwarzania danych. Eliminuje potrzebę stosowania wielu rozwiązań w środowiskach hybrydowych.

Agent Guardicore zainstalowany na serwerach kontroluje i pilnuje bezpieczeństwa, w razie potrzeby blokując niepożądane działania, np. komunikację intruza z kolejnym serwerem. Wizualizacja stanu bieżącego i zarządzanie agentami są realizowane przy użyciu prostej w obsłudze konsoli.

Usługi profesjonalne

Testy penetracyjne – analiza wskazanych przez klienta stron WWW i/lub infrastruktury IT pod kątem występowania potencjalnych błędów bezpieczeństwa spowodowanych niewłaściwą konfiguracją bądź pozostawieniem niezałatanych podatności. Na zakończenie prac klientowi przedstawiany jest raport zawierający informacje o wykrytych podatnościach wraz z rekomendacjami dotyczącymi ich usunięcia.

Testy socjotechniczne – symulacja ataku phishingowego, która sprawdzi czujność i świadomość pracowników w zakresie zagrożeń ze strony cyberprzestępców. Przegląd i doradztwo w zakresie SZBI - polega na wsparciu w zabezpieczaniu procesów u klienta lub ich przeglądach pod kątem ich zgodności z np. ISO 27001, ISO 22301, ustawą o Krajowym Systemie Cyberbezpieczeństwa i RODO. Oprócz wyszukiwania potencjalnych luk nasi eksperci mogą pomóc w ich późniejszym usuwaniu, zabezpieczając organizacje przed różnorodnymi zagrożeniami.

Budowanie świadomości w zakresie cyberbezpieczeństwa – eksperci zadbają o kompleksową edukację pracowników. Usługa polega na okresowym wykorzystywaniu różnych form komunikacji, by rozwinąć wśród grup odbiorców potrzebę codziennego stosowania praktyk bezpieczeństwa.

Wsparcie eksperta bezpieczeństwa – wsparcie w zakresie ochrony informacji przez zespół ekspertów. Obejmuje m.in. planowanie i prowadzenie programów bezpieczeństwa, identyfikację ryzyk, tworzenie wymagań bezpieczeństwa, wsparcie w audycie dostawców, utwardzanie procesów, a także zarządzanie incydentami.

Dodatkowe informacje o usłudze znajdziesz na:
www.orange.pl/poradnik-dla-firm/