Cyberbezpieczeństwo

Reakcja na incydenty bezpieczeństwa

Potrzeba biznesowa

Utrata własności intelektualnej, danych klientów i innych poufnych informacji, a także zakłócenia w realizacji podstawowych działań biznesowych mogą prowadzić do poważnych strat zarówno finansowych, jak i reputacyjnych.

Skala cyberprzestępstw podkreśla rosnącą złożoność cyberataków oraz umiejętności współczesnych cyberprzestępców, którym dziś muszą stawić czoła organizacje.

W świetle coraz większej liczby cyberataków dotykających organizacje, właściwym pytaniem nie jest CZY ale KIEDY nastąpi cyberatak.

Radzenie sobie z incydentami może być dużym wyzwaniem dla organizacji. KPMG w Polsce kompleksowo wspiera przedsiębiorstwa przed, w trakcie i po cyberataku.

Usługi KPMG

Przygotowanie

- KPMG pomaga skutecznie projektować, wdrażać i ograniczać szkody wynikające z naruszeń bezpieczeństwa poprzez skuteczne planowanie i reagowanie na incydenty.
- KPMG oferuje usługi budowania i oceny bieżących zdolności organizacji do reagowania na incydenty, testowania go za pomocą odpowiednio dopasowanych ćwiczeń i gier oraz uzupełnienia braków poprzez usprawnienie procesów, pomoc w implementacji narzędzi, wybór partnerów strategicznych oraz personelu szkoleniowego.
- Dodatkowo, KPMG może przeprowadzić kompleksową ocenę kompromitacji infrastruktury sieciowej w wyniku przeprowadzenia aktywnej identyfikacji zagrożeń w sieci wewnętrznej organizacji.

Reakcja

- KPMG pomaga w rozwiązywaniu problemów związanych z incydentami cyberbezpieczeństwa zapewniając pełną obsługę w zakresie łagodzenia skutków incydentów – zabezpieczanie danych, analiza plików systemowych i logów, zarządzanie incydentami.
- KPMG może świadczyć usługi w trybie pilnej reakcji na incydent. Przed realizacją takich prac rekomendowane jest dokonanie oceny aktualnych możliwości organizacji, w celu identyfikacji elementów uniemożliwiających KPMG skuteczną reakcję na incydent (np. niewystarczające rejestrowanie zdarzeń systemowych).
- Globalni klienci korzystają z zasięgu KPMG, ponieważ w razie niebezpieczeństwa KPMG może mieć wykwalifikowanego profesjonalistę dostępnego pod telefonem w ciągu 4 godzin lub mniej i lokalnie w większości krajów w ciągu 24-48h.

Działania powłamaniowe

- W następstwie cyber incydentu ważne jest, aby ustalić, czy przyczyny tego zdarzenia zostały prawidłowo zidentyfikowane, a środki mitygujące wdrożone. Jeśli naruszenie dotyczy danych osobowych, mogą istnieć prawne zobowiązania do zgłaszania incydentu bezpieczeństwa do regulatora.
- KPMG może pomóc klientom w zrozumieniu głównych przyczyn incydentów, ocenić, czy zastosowane środki mitygujące były skuteczne oraz zapewnić pomoc w komunikacji z regulatorem. KPMG może zaproponować dodatkowe środki mitygujące oraz wsparcie ekspertów w celu rozwiązania zidentyfikowanych problemów.
- KPMG może również tymczasowo wzmocnić zdolność wykrywania i reagowania klienta, ponieważ cyberprzestępcy mogą nadal być obecni w sieci organizacji.

Korzyści

Organiczenie ryzyka operacyjnego poprzez:

+ Wsparcie organizacji w przygotowaniu na nieuniknione incydenty związane z cyberbezpieczeństwem poprzez ocenę obecnych możliwości reakcji, przetestowanie ich oraz zaprojektowanie wymaganych usprawnień.
+ Kompletne wsparcie organizacji w trakcie trwania incydentu – od zarządzania incydentami oraz zabezpieczenia danych po pomoc w kontaktach z regulatorem.
+ Pomoc po wystąpieniu incydentu, dzięki czemu operacje biznesowe mogą powrócić do normalnego trybu pracy przy jak najniższym koszcie i wpływie na organizację.

Dlaczego KPMG?

Jesteśmy **światowym liderem** w obszarze usług doradczych w zakresie cyberbezpieczeństwa (wg badania Forrester Wave™: Information Security Consulting Services, Q3 2017)

Nasi polscy eksperci zrealizowali **kilkaset projektów** w obszarze cyberbezpieczeństwa dla polskich i zagranicznych przedsiębiorstw z różnych branż

Wiedzę naszych konsultantów potwierdzają **liczne certyfikaty**

W trakcie realizowanych projektów zidentyfikowaliśmy kilkadziesiąt podatności typu **zero-day**

Rozumiemy procesy biznesowe, przez co nasze rekomendacje są dostosowane do rzeczywistych potrzeb i wnoszą realną wartość

Obecność w globalnej sieci zespołów cyber bezpieczeństwa KPMG, to **bogate zasoby wiedzy**, narzędzi i nowatorskich rozwiązań

Globalna sieć to również gwarancja ciągłości współpracy oraz możliwość świadczenia usług w wielu krajach jednocześnie

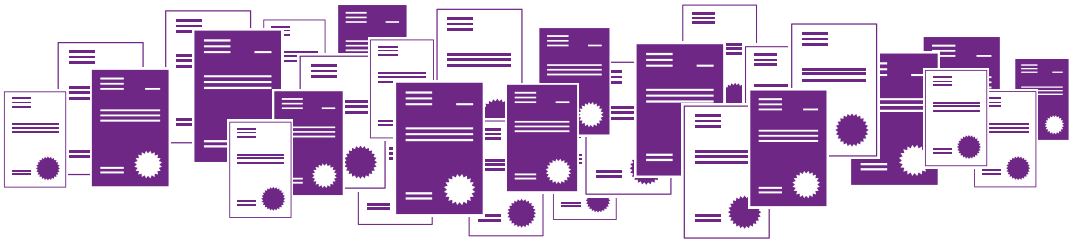
Aktywnie działamy w organizacjach branżowych (m.in. w zarządzie **OWASP Poland**)

Nasza **wiedza jest doceniana** przez wiodące organizacje edukacyjne – np. wspieramy SANS Institute w roli mentora w zakresie bezpieczeństwa aplikacji

Jesteśmy **niezależni** od producentów rozwiązań bezpieczeństwa, dzięki czemu jesteśmy w stanie optymalnie doradzać

Jesteśmy **elastyczni** i dostosowujemy się do zmieniających się dynamicznie potrzeb klientów

Nasze wybrane certyfikaty:



- CISM (Certified Information Security Manager)
- CISSP (Certified Information Systems Security Professional)
- CISA (Certified Information Systems Auditor)
- OSCP (Offensive Security Certified Professional)
- LPT (Licensed Penetration Tester)
- CEH (Certified Ethical Hacker)
- GWAPT (GIAC Web Application Penetration Tester)
- GREM (GIAC Reverse Engineering Malware)
- GMOB (GIAC Mobile Device Security Analyst)
- CRISC (Certified in Risk and Information Systems Control)
- CCSP (Cisco Certified Security Professional)
- CCSA (Check Point Security Administrator)
- GCWSA (GIAC Certified Windows Security Administrator)
- MCTS (Microsoft Certified Technology Specialist)
- RHCE (Red Hat Certified Engineer Red Hat Enterprise Linux 6)
- RHCSA (Red Hat Certified System Administrator Red Hat Enterprise Linux 6)
- GCUX (GIAC Certified UNIX Security Administrator)
- LPI LPIC-1 Certified Linux Administrator
- SUSE Certified Administrator
- GSSP-JAVA (GIAC Secure Software Programmer – JAVA)
- ECSA (Certified Security Analyst)
- Information Systems Security (INFOSEC) Professional
- ISO 27001 Information Security Management System Lead Auditor
- GAWN (GIAC Auditing Wireless Networks Certified Professional)
- CCNA (Cisco Certified Network Associate)
- PMP (Project Management Professional)
- CIA (Certified Internal Auditor)

Kontakt

KPMG Advisory
Spółka z ograniczoną
odpowiedzialnością sp. k.
ul. Inflancka 4A
00-189 Warszawa
T: +48 22 528 11 00
F: +48 22 528 10 09
E: kpmg@kpmg.pl

Michał Kurek
Partner
Usługi doradcze
Cyberbezpieczeństwo
T: +48 22 528 13 69
K: +48 660 440 041
E: michalkurek@kpmg.pl

Łukasz Staniak
Menedżer
Usługi doradcze
Cyberbezpieczeństwo
T: +48 22 528 34 52
K: +48 605 511 286
E: lstaniak@kpmg.pl

Dostępne w App Store

KPMG Poland

Zeskanuj kod, aby przejść do strony kpmg.pl