

T Business

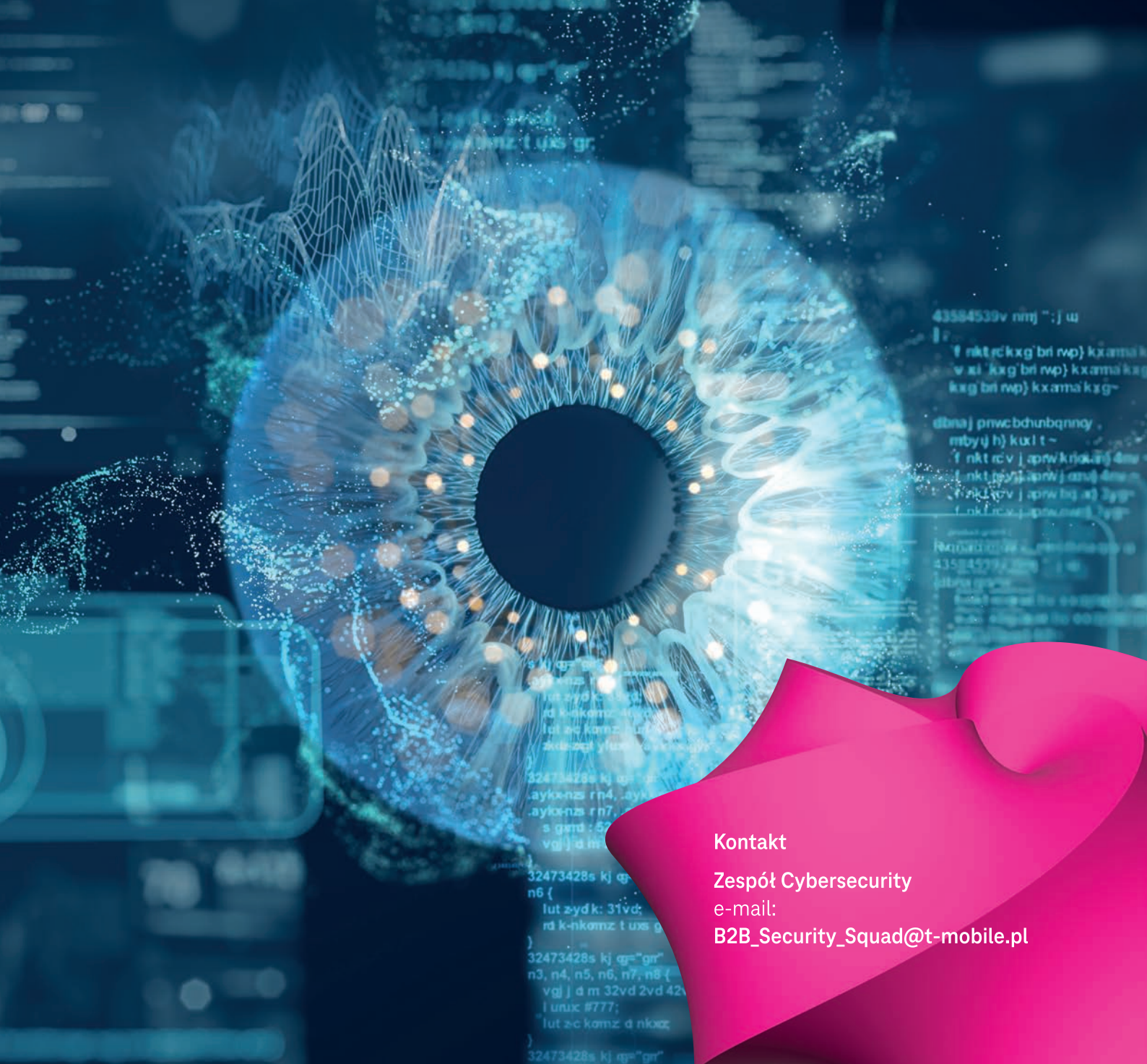
Cybersecurity

BADANIE PODATNOŚCI ORGANIZACJI

**IDENTYFIKACJA
CYBERZAGROŻEŃ**



T



Kontakt

Zespół Cybersecurity

e-mail:

B2B_Security_Squad@t-mobile.pl

SPIS TREŚCI

1. Badanie bezpieczeństwa i zabezpieczeń aplikacji WEB	3
2. Badanie wrażliwości infrastruktury teleinformatycznej	4
3. Ocena stanu Kultury Bezpieczeństwa	5
4. Weryfikacja sposobu ochrony systemów pocztowych	6
5. Analiza nadzoru nad punktem styku z Internetem	7

BADANIE BEZPIECZEŃSTWA I ZABEZPIECZEŃ APLIKACJI WEB

OCENA WRAŻLIWOŚCI BEZPIECZEŃSTWA APLIKACJI WEB

Aplikacje WEB-owe to częsty cel działania cyberprzestępców ze względu na fakt, że na ogół wystawione są w sieci Internet jako interfejs komunikacyjny dla użytkownika zewnętrznego. Poza standardową konfiguracją na etapie wdrożenia i utrzymania rzadko mają dodatkowe warstwy ochrony, pozwalające na detekcję oraz zabezpieczenie przed zagrożeniami. **Podatności i błędy aplikacji WEB-owych to jedna z podstawowych przyczyn występowania incydentów zagrożenia bezpieczeństwa teleinformatycznego**, związanych z kompromitacją serwisów, wyciek danych klientów, pracowników, której skutkiem jest uzyskanie punktu dostępowego do zasobów organizacji, a następnie traktowanie go jako pośrednika komunikacyjnego do dalszych działań cyberprzestępczych.

AUTORSKA METODYKA BADANIA WRAŻLIWOŚCI

Dokonaj oceny wrażliwości na zagrożenia, badając stan i poziom zabezpieczeń aplikacji WEB-owych oraz systemów ochronnych WAF.

Badanie to ma na celu:

- Aktywne sprawdzanie podatności aplikacji WEB-owych pod kątem znanych podatności.
- Ocenę skuteczności WAF w zakresie wykrywania i blokady zagrożeń.
- Dynamiczną analizę kodu źródłowego aplikacji w celu identyfikacji błędów programistycznych.
- Identyfikację złośliwego oprogramowania i treści, które mogą być osadzone w serwisach WEB-owych.



Wynikiem przeprowadzonego badania będzie raport zawierający:

- Ocenę stanu zabezpieczeń, błędów konfiguracyjnych i podatności.
- Informację o wykrytych zagrożeniach.
- Wytyczenie odnośnie do kierunku rozwoju oraz zmian koniecznych, aby zwiększyć poziom bezpieczeństwa organizacji.
- Rekomendację działań naprawczych.

DLACZEGO TWOJA FIRMA POTRZEBUJE TAKIEGO BADANIA?



- Wzrost poziomu cyberbezpieczeństwa w organizacji.
- Podniesienie poziomu ochrony danych Klientów i pracowników.
- Normy i regulacje (np. ustawa o prawie telekomunikacyjnym, KNF-D, dyrektywa NIS – ustawa o krajowym systemie cyberbezpieczeństwa).
- Audyt (wewnętrzny, zewnętrzny).
- Usprawnienie czynności związanych z procesem zarządzania incydentami zagrażającymi cyberbezpieczeństwu.

BADANIE WRAŻLIWOŚCI INFRASTRUKTURY TELEINFORMATYCZNEJ

OCENA WRAŻLIWOŚCI INFRASTRUKTURY TELEINFORMATYCZNEJ

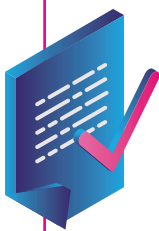
Infrastruktura teleinformatyczna jest elementem niezbędnym do prawidłowego funkcjonowania każdej organizacji. **Sieci teleinformatyczne to wielowarstwowe, skompilowane komponenty, tworzące całość.** Część z nich widać od strony sieci Internet, przez co narażone są bezpośrednio na cyberzagrożenia i ataki. Podatności infrastruktury to jedna z podstawowych przyczyn występowania incydentów naruszania bezpieczeństwa teleinformatycznego, które wynikają z nieaktualnego oprogramowania oraz błędów konfiguracyjnych, powstałych na etapie wdrożenia i utrzymania.

AUTORSKA METODYKA BADANIA WRAŻLIWOŚCI

Dokonaj oceny wrażliwości na zagrożenia, badając stan infrastruktury teleinformatycznej.

Badanie to ma na celu:

- Identyfikację i inwentaryzację zasobów infrastruktury teleinformatycznej.
- Wykazanie podatności, luk bezpieczeństwa oraz błędów konfiguracyjnych.
- Proaktywne działanie wobec zidentyfikowanych zagrożeń, wskazujące kierunek działań naprawczych.
- Wykazanie ryzyka oraz obszarów krytycznych, które powinny być potraktowane priorytetowo i zlikwidowane.



Wynikiem przeprowadzonego badania będzie raport zawierający:

- Ocenę stanu zabezpieczeń, błędów konfiguracyjnych i podatności.
- Informację o wykrytych zagrożeniach.
- Wytyczne odnośnie do kierunku rozwoju oraz zmian koniecznych w celu zwiększania poziomu cyberbezpieczeństwa organizacji.
- Rekomendację działań naprawczych.

DLACZEGO TWOJA FIRMA POTRZEBUJE TAKIEGO BADANIA?



- Wzrost poziomu cyberbezpieczeństwa w organizacji.
- Normy i regulacje (np. ustawa o prawie telekomunikacyjnym, KNF-D, dyrektywa NIS – ustawa o krajowym systemie cyberbezpieczeństwa).
- Audyt (wewnętrzny, zewnętrzny).
- Usprawnienie czynności związanych z procesem zarządzania incydentami zagrażającymi cyberbezpieczeństwu.

OCENA STANU KULTURY BEZPIECZEŃSTWA

OCENA WRAŻLIWOŚCI PRACOWNIKÓW

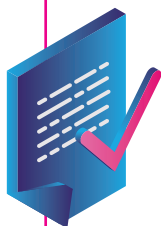
Pracownicy to istotny element systemu bezpieczeństwa w każdej organizacji. Z powodu słabej świadomości zagrożeń oraz niewielkiej wiedzy w zakresie ich identyfikowania często bywają najsłabszym ogniwem systemu. **Przyczyną incydentów krytycznych są na ogół bezpośrednio błędy człowieka**, spowodowane niewłaściwym przetworzeniem otrzymanych informacji.

Cyberprzestępcy to często wykwalifikowani specjaliści, których jedynym celem jest osiągnięcie zamierzonych korzyści. Obierając za cel pracowników wybranej organizacji, uzyskują zdecydowaną przewagę. Brak programów podnoszących świadomość w zakresie cyberbezpieczeństwa oraz ćwiczeń polegających na symulacji poszczególnych przypadków to jedna z podstawowych przyczyn występowania incydentów zagrożenia bezpieczeństwa teleinformatycznego.

AUTORSKA METODYKA BADANIA WRAŻLIWOŚCI

Dokonaj oceny odporności na zagrożenia, badając podatność pracowników na ataki socjotechniczne z wykorzystaniem:

- Symulacji realnych kampanii phishingowych.
- Bezinwazyjnych ataków ukierunkowanych na wybrane grupy pracowników.
- Personalizacji treści wiadomości za pomocą dedykowanych szablonów.



Wynikiem przeprowadzonego badania będzie raport zawierający:

- Wrażliwość systemu na próby przestania spreparowanych, szkodliwych wiadomości e-mail.
- Rekomendacje w zakresie zastosowania mechanizmów podnoszących poziom bezpieczeństwa poczty elektronicznej.
- Wytyczenie kierunku rozwoju oraz zmian koniecznych w celu zwiększania poziomu cyberbezpieczeństwa organizacji.
- Rekomendację działań naprawczych.

DLACZEGO TWOJA FIRMA POTRZEBUJE TAKIEGO BADANIA?



- Wzrost poziomu cyberbezpieczeństwa w organizacji.
- Normy i regulacje (np. ustawa o prawie telekomunikacyjnym, KNF-D, dyrektywa NIS – ustawa o krajowym systemie cyberbezpieczeństwa).
- Audyt (wewnętrzny, zewnętrzny).
- Usprawnienie czynności związanych z procesem zarządzania incydentami zagrożenia cyberbezpieczeństwa.

WERYFIKACJA SPOSOBU OCHRONY SYSTEMÓW POCZTOWYCH

OCENA WRAŻLIWOŚCI BEZPIECZEŃSTWA SYSTEMÓW POCZTOWYCH

Poczta e-mail to najpopularniejszy kanał dystrybucji złośliwych treści i najprostszy sposób, aby dostały się one do organizacji. Podstawowe przyczyny takiego stanu rzeczy to **ogólna dostępność adresów skrzynek pocztowych, niewiedza pracowników i brak odporności na ataki socjotechniczne**. Kolejny element to bardzo skuteczne metody przedostawania się spreparowanych wiadomości przez bramki pocztowe, które mało skutecznie analizują i interpretują treści. Pojedyncza warstwa ochrony systemów poczty to główna przyczyna występowania incydentów zagrożenia bezpieczeństwa teleinformatycznego.

AUTORSKA METODYKA BADANIA WRAŻLIWOŚCI

Dokonaj oceny odporności na zagrożenia, badając mechanizmy ochrony infrastruktury pocztowej.

Badanie ma na celu:

- Zidentyfikowanie natywnych mechanizmów ochrony, polityk i konfiguracji systemów ochrony poczty przez generowanie specjalnych wiadomości e-mail, symulujących popularne techniki ataków.
- Generowanie wiadomości e-mail zawierających zagrożenia w postaci złośliwych adresów URL i załączników w celu sprawdzenia możliwości ich identyfikacji i zablokowania.



Wynikiem przeprowadzonego badania będzie raport zawierający:

- Wrażliwość systemu na próby przesyłania spreparowanych, szkodliwych wiadomości e-mail.
- Rekomendacje w zakresie zastosowania mechanizmów podnoszących poziom cyberbezpieczeństwa systemu pocztowego.
- Wytyczenie kierunku rozwoju oraz zmian koniecznych w celu zwiększenia poziomu cyberbezpieczeństwa w organizacji.
- Rekomendację działań naprawczych.

DLACZEGO TWOJA FIRMA POTRZEBUJE TAKIEGO BADANIA?



- Wzrost poziomu cyberbezpieczeństwa w organizacji.
- Normy i regulacje (np. ustawa o prawie telekomunikacyjnym, KNF-D, dyrektywa NIS – ustawa o krajowym systemie cyberbezpieczeństwa).
- Audyt (wewnętrzny, zewnętrzny).
- Usprawnienie czynności związanych z zarządzaniem incydentami zagrożenia cyberbezpieczeństwa.

ANALIZA NADZORU NAD PUNKTEM STYKU Z INTERNETEM

OCENA WRAŻLIWOŚCI BEZPIECZEŃSTWA PUNKTU STYKU Z INTERNETEM

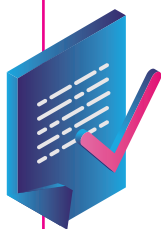
Punkt styku z siecią Internet pełni podstawową rolę w zapewnieniu cyberbezpieczeństwa oraz identyfikacji zagrożeń. To pośrednik w ruchu komunikacyjnym, łączący ze światem zewnętrznym, który powinien być ściśle nadzorowany i traktowany jako punkt graniczny. Bezpośredni nadzór nad ruchem wychodzącym oraz przychodzącym to jeden z filarów skutecznego monitoringu infrastruktury teleinformatycznej. **Brak właściwego monitoringu i analizy zdarzeń na styku z Internetem to jedna z podstawowych przyczyn występowania incydentów zagrożenia bezpieczeństwa teleinformatycznego.**

AUTORSKA METODYKA BADANIA WRAŻLIWOŚCI

Dokonaj oceny wrażliwości na zagrożenia, badając infrastrukturę brzegową.

Badanie ma na celu:

- Analizę architektury brzegowej.
- Weryfikację możliwości wykrywania w ruchu sieciowym aplikacji i treści o wysokim ryzyku.
- Sprawdzenie funkcjonalności IPS – wykrywanie i blokowanie znanych zagrożeń typu exploit.
- Wykrywanie zagrożeń na poziomie modułów funkcjonalnych firewall.



Wynikiem przeprowadzonego badania będzie raport zawierający:

- Wrażliwość systemu na próby przesyłania szkodliwej zawartości w ruchu sieciowym.
- Identyfikację zagrożeń na brzegu z siecią Internet.
- Wytyczenie kierunku rozwoju oraz zmian koniecznych w celu zwiększania poziomu cyberbezpieczeństwa organizacji.

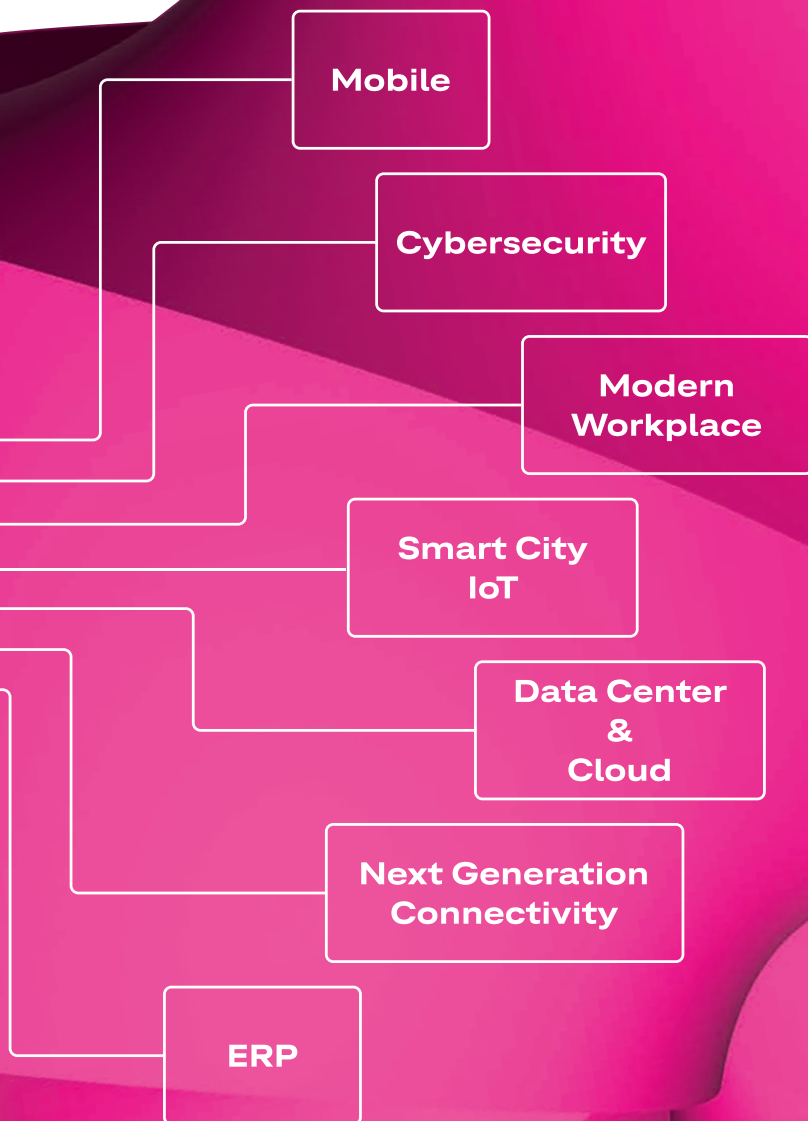
DLACZEGO TWOJA FIRMA POTRZEBUJE TAKIEGO BADANIA?



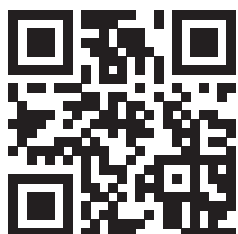
- Wzrost poziomu cyberbezpieczeństwa w organizacji.
- Normy i regulacje (np. ustawa o prawie telekomunikacyjnym, KNF-D, dyrektywa NIS – ustawa o krajowym systemie cyberbezpieczeństwa).
- Audyt (wewnętrzny, zewnętrzny).
- Usprawnienie czynności związanych z procesem zarządzania incydentami zagrożenia cyberbezpieczeństwa.

KOMPLEKSOWE USŁUGI

DLA DUŻYCH I ŚREDNICH FIRM



Dowiedz się więcej



T-Mobile Polska S.A.
ul. Marynarska 12, 02-674 Warszawa

Więcej informacji o usługach: www.biznes.t-mobile.pl