LIFE IS FOR SHARING.

Kontakt

Zespół Cybersecurity
e-mail: B2B_Security_Squad@t-mobile.pl

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 (wewnętrzy, zewnętrzny).
- Usprawnienie czynności związanych z zarządzaniem incydentami zagrożenia cyberbezpieczeństwa.