Spostrzeżenia dotyczące bezpieczeństwa cybernetycznego

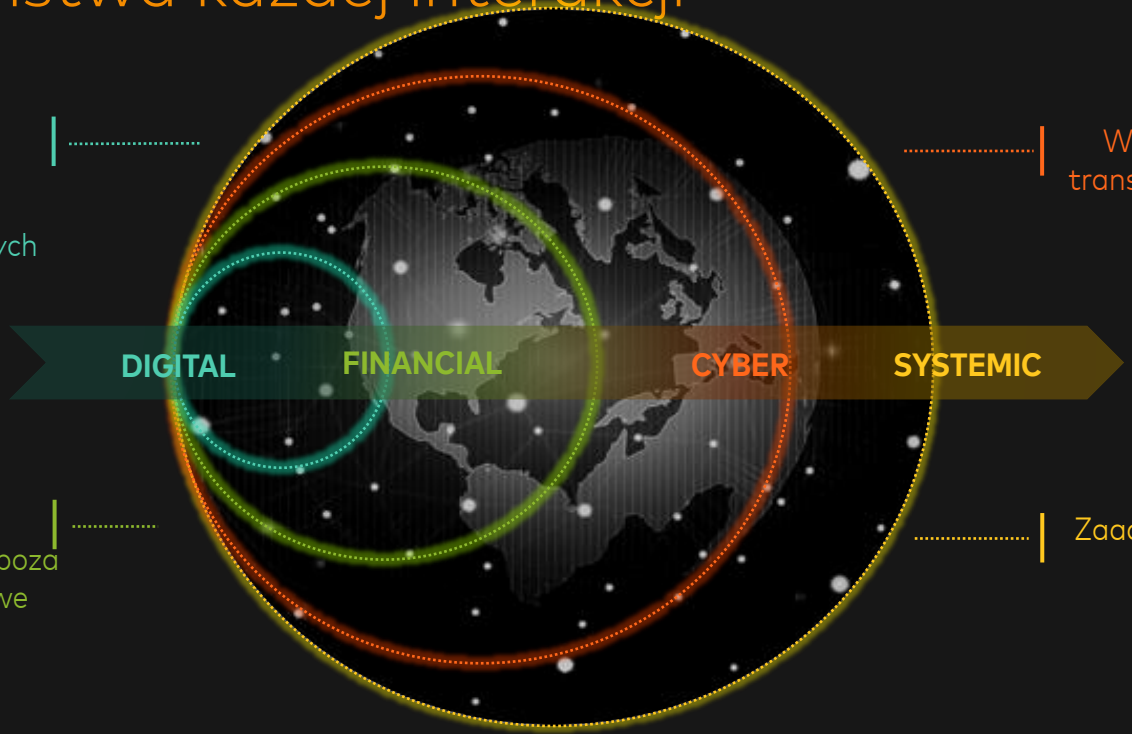
w jednostkach samorządu w Polsce

Czerwiec 2022

Ewoluujemy razem z całym ekosystemem....od zabezpieczania transakcji kartą do zapewnienia bezpieczeństwa każdej interakcji

Zwiększanie bezpieczeństwa konsumenta w kanałach cyfrowych

Wyjście poza obszar transakcji finansowych

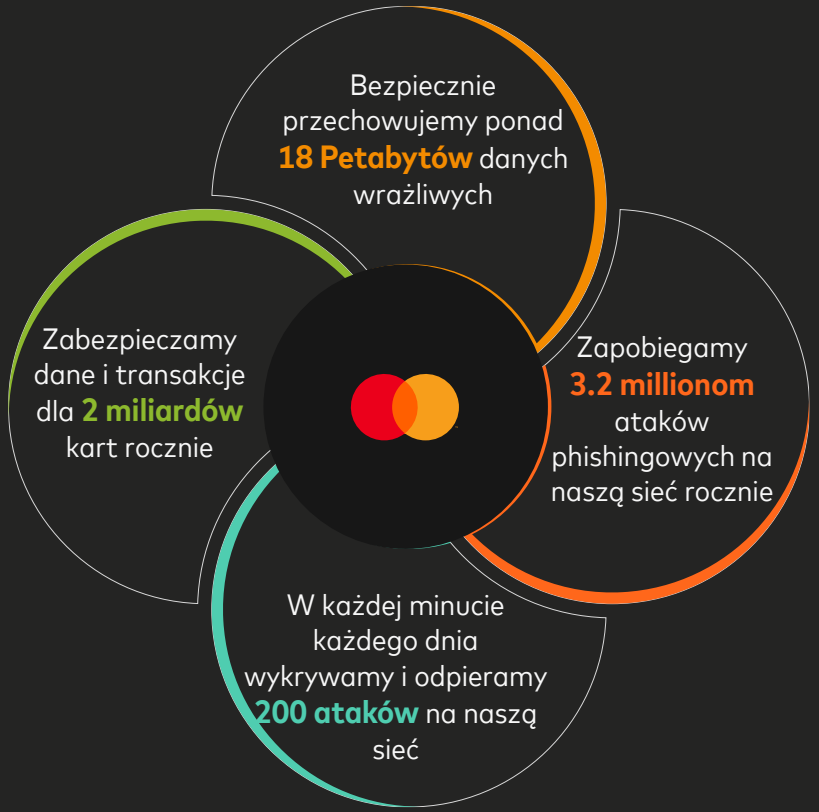


Rozszerzanie bezpieczeństwa poza transakcje kartowe

Zaadresowanie ryzyka systemowego

Jedno zaufane źródło bezpieczeństwa

Od 50 lat Mastercard stosuje zasady bezpieczeństwa cybernetycznego w celu zabezpieczenia globalnej sieci płatności



Na czym polega ocena cyberbezpieczeństwa?

IN CONTEXT

Wyobraźmy sobie złodzieja stojącego po drugiej stronie ulicy i sprawdzającego firmę i oceniającego zarówno zabezpieczenia, jak i potencjalne luki, które można wykorzystać.

RiskRecon robi to samo w środowisku cybernetycznym, pasywnie oceniając zabezpieczenia i luki w zabezpieczeniach organizacji - bez ingerencji w jej działalność - w celu oszacowania ryzyka cybernetycznego.

Zabezpieczenia i luki w zabezpieczeniach są oceniane według kategorii Bezpieczeństwa i Infrastruktury.

Zewnętrzne spojrzenie na sektor samorządowy

Jak działa nasza ewaluacja

Wykorzystując technologię monitorowania ryzyka cybernetycznego firmy Mastercard, wybrana próba organizacji sektora publicznego została poddana ocenie w dziewięciu dziedzinach bezpieczeństwa. Proces rozpoczął się od zidentyfikowania systemów, po czym przeprowadzono zewnętrzne oceny bezpieczeństwa cybernetycznego i wartości aktywów, a w efekcie uzyskano kompleksowy i kontekstowy obraz ryzyka cybernetycznego organizacji.

Na podstawie otrzymanych wyników organizacje są oceniane i przypisywany jest im rating ryzyka cybernetycznego dla każdej z dziewięciu domen. Ocena odzwierciedla wyniki uzyskane przez wybrane gminy.

Dla otrzymanych wyników określono średnią ocenę, a także najniższe i najwyższe wyniki. Podawane są również średnie wyniki wszystkich organizacji monitorowanych przez Mastercard, aby zapewnić wgląd w ocenę całego sektora publicznego.

Co robimy...

Głęboka eksploracja baz danych rejestrów sieciowych	Analiza logów rozwiązywania DNS oraz IP na nazwę hosta
Zapytania DNS	Lekkie przeglądanie stron internetowych, stosując się do instrukcji robots.txt
Analiza publicznie dostępnego kodu, treści, konfiguracji	Monitorowanie i analiza komercyjnych i otwartych źródeł informacji o reputacji IP
Analizowanie Internetu w poszukiwaniu istotnych informacji, takich jak ślady zdarzeń związanych z utratą danych	Analizowanie danych dotyczących skanowania portów internetowych pochodzących od komercyjnego dostawcy.

Czego nie robimy...

Manipulowanie parametrami, wstrzykiwanie kodu	Wykonywanie cross site scripting
Wstrzykiwanie zapytania SQL	Próba ominięcia uwierzytelniania lub kontroli bezpieczeństwa
Wykonywanie testów przepełnienia pamięci	Wypełnianie pól formularzy
Zgadywanie danych dostępowych	Wykorzystanie luk w zabezpieczeniach

Identyfikacja Systemów → Ocena podatności → Ocena wartości aktywów → Ocena ryzyka → Ocena poziomu cyberbezpieczeństwa

Wyniki w różnych domenach bezpieczeństwa

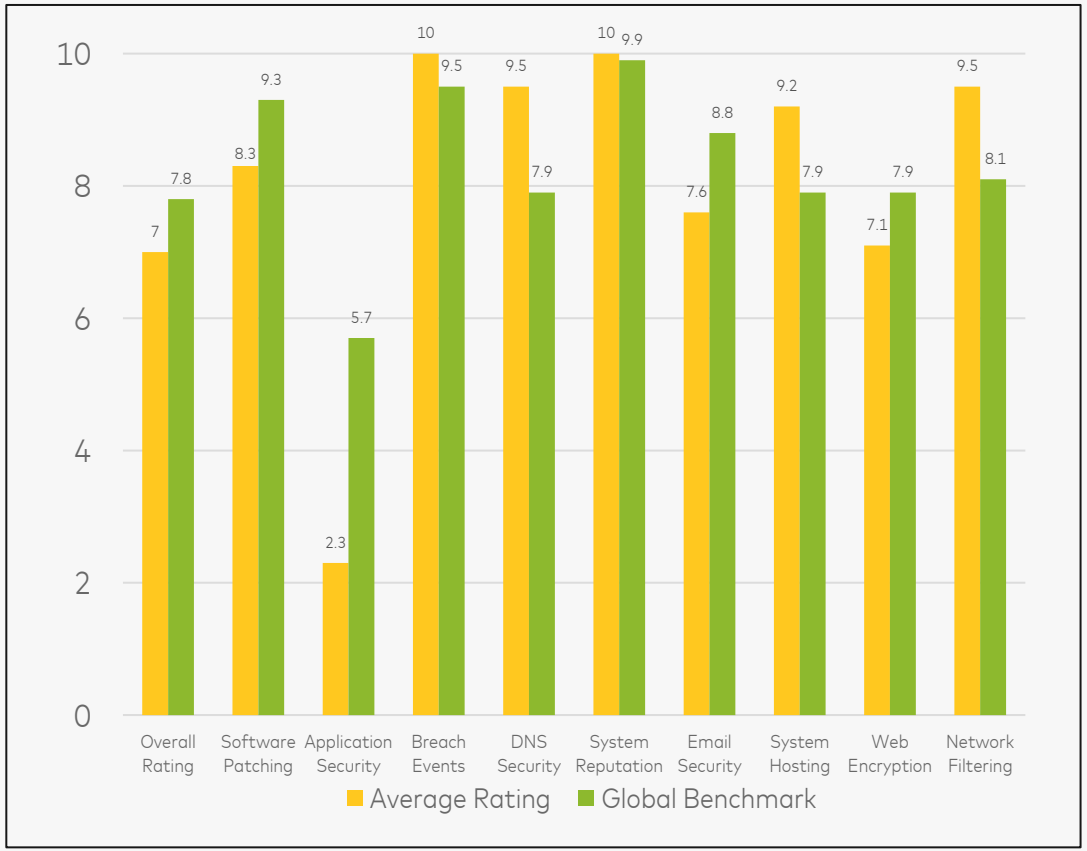
Oceniliśmy 53 domeny internetowe i 276 nazw hostów na wybranej próbie 22 polskich samorządów – gmin.

Stwierdziliśmy, że ogólna średnia ocena wyniosła 7,0 na 10 (na granicy oceny C i B), co jest wynikiem gorszym od globalnego wyniku sektora publicznego, wynoszącego 7,8 na 10 (ocena B).

Wyniki w zakresie cyberbezpieczeństwa w porównaniu ze średnimi globalnymi

Oceniliśmy **ponad 50 000** globalnych organizacji sektora publicznego i porównaliśmy je z naszą próbą .

Stwierdziliśmy, że w czterech z dziewięciu domen bezpieczeństwa przykładowe organizacje uzyskały niższe wyniki niż przeciętna organizacja sektora publicznego.

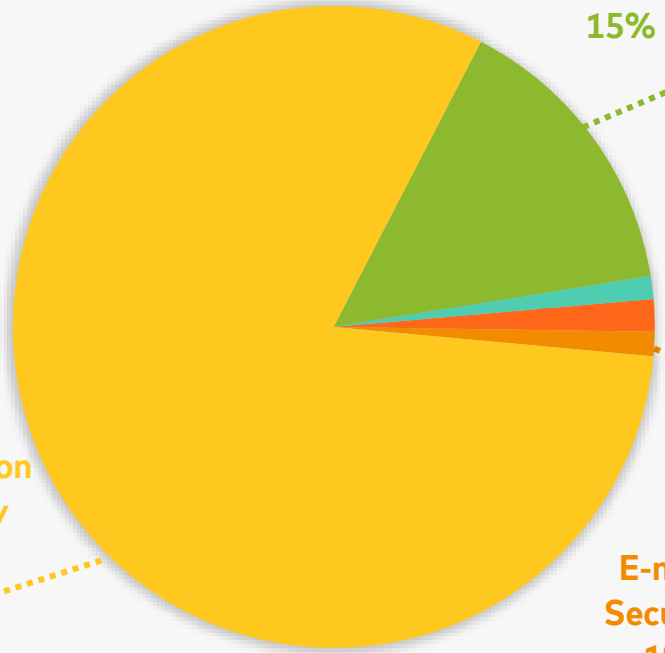


Zaobserwowane podatności

Spośród organizacji poddanych ocenie i analizie wykryliśmy 11 poważnych problemów dotyczących aktywów o wysokiej wartości w dziewięciu domenach bezpieczeństwa.

Najbardziej krytyczne problemy dotyczyły korzystania z oprogramowania wycofanego z eksploatacji oraz udostępniania niezabezpieczonych usług sieciowych w Internecie.

Wykres po prawej stronie przedstawia wszystkie 1 473 błędy wykryte podczas oceny.



Invalid Certificate Subject

- Zaobserwowano witryny z nieprawidłowym podmiotem certyfikatu szyfrowania X.509. Systemy z nieprawidłowym podmiotem certyfikatu nie są godne zaufania i powodują wyświetlanie przez przeglądarkę ostrzeżeń o zabezpieczeniach dla użytkownika.

Email Authentication (SPF or DKIM)

- Domeny bez zaimplementowanego uwierzytelniania poczty elektronicznej. Stwarza to pole do oszustw opartych na wiadomościach e-mail.

Email Encryption (STARTTLS)

- Zaobserwowano serwery poczty elektronicznej, na których nie zastosowano szyfrowania wiadomości e-mail co powoduje, że serwery poczty elektronicznej wysyłają wiadomości bez szyfrowania, narażając je na przechwycenie podczas transmisji.

Accessible CMS Authentication

- Zaobserwowany publicznie dostępny interfejs administracyjny, co umożliwia przejęcie kontroli nad systemami zarządzania treścią za pomocą interfejsu administracyjnego poprzez kradzież i zgadywanie danych uwierzytelniających.

Missing HTTP Security Headers

- W witrynach internetowych zaobserwowano brak implementacji ważnych nagłówków bezpieczeństwa HTTP. Nagłówki bezpieczeństwa zawierają instrukcje dla przeglądarki dotyczące bezpiecznej interakcji z serwerem WWW

Dziękuję za uwagę!

Łukasz Krzykwa
Digital Solutions Manager
Cyber & Intelligence

Lukasz.krzykwa@mastercard.com

riskrecon
mastercard

Załącznik A

Gminy, których domeny internetowe zostały przeanalizowane na potrzeby tej prezentacji

Gmina Błonie	Miasto Płońsk
Gmina Brwinów	Gmina Podkowa Leśna
Gmina Gniewoszów	Gmina Słupno
Gmina Grodzisk Mazowiecki	Miasto Sochaczew
Gmina Kozienice	Gmina Sochaczew
Gmina Lesznowola	Miasto Sokołów Podlaski
Gmina Łosice	Gmina Węgrów
Gmina Milanówek	Gmina Wołomin
Gmina Mszczonów	Gmina Wyszków
Gmina Osieck	Gmina Żabia Wola
Gmina Piastów	Gmina Teresin