SAILINGBYTE

Dlaczego monitorowanie ustawień poczty dla domeny jest kluczowe

Zapewnienie, że ustawienia poczty w domenie są prawidłowo skonfigurowane i regularnie monitorowane, ma zasadnicze znaczenie dla ochrony komunikacji e-mail. Bez odpowiedniego monitorowania domena jest podatna na szereg zagrożeń, w tym phishing, spoofing i nieautoryzowane użycie domeny. Regularne sprawdzanie ustawień poczty pomaga utrzymać reputację domeny, zapewnia, że legalne wiadomości e-mail docierają do miejsca przeznaczenia i chronią użytkowników przed potencjalnymi zagrożeniami.

Zajmowałem się tematem używania rekordów domeny w celu zapewnienia dostarczalności wiadomości e-mail dla Twojej firmy, ale zacznijmy od podsumowania i szybkiego przypomnienia podstawowych definicji, które mogą być wymagane później.

Jak SPF chroni Twoją domenę

Sender Policy Framework (SPF) jest krytycznym narzędziem w arsenale bezpieczeństwa poczty elektronicznej Twojej domeny. Jego działanie polega na określeniu, które serwery pocztowe są upoważnione do wysyłania wiadomości e-mail w imieniu domeny. Po otrzymaniu wiadomości e-mail serwer pocztowy odbiorcy sprawdza rekord SPF domeny wysyłającej. Jeśli serwer jest wymieniony jako autoryzowany nadawca, wiadomość e-mail jest akceptowana; jeśli nie, jest oznaczana jako podejrzana lub odrzucana. Ten prosty, ale skuteczny protokół pomaga zapobiegać wykorzystywaniu domeny przez spamerów do wysyłania fałszywych wiadomości e-mail.

Przykładowa składnia SPF w rekordzie TXT: v=spf1 +a +mx -all

Jak DKIM chroni Twoją pocztę e-mail i domenę

DomainKeys Identified Mail (DKIM) dodaje dodatkową warstwę zabezpieczeń, umożliwiając serwerowi wysyłającemu cyfrowe podpisywanie wiadomości e-mail. Podpis ten jest dołączany do nagłówka wiadomości e-mail i weryfikowany przez serwer pocztowy odbiorcy przy użyciu klucza publicznego opublikowanego w rekordach DNS domeny. Jeśli podpis jest zgodny, potwierdza to, że wiadomość e-

mail nie została zmodyfikowana podczas przesyłania i że rzeczywiście pochodzi z żądanej domeny. Pozwala to również uzyskać lepsze wyniki w filtrach antyspamowych, co oznacza, że jest bardziej prawdopodobne, że wiadomości nie zostaną przekierowane do folderu SPAM odbiorcy. Chroni to Twoją pocztę i domenę przed atakami phishingowymi i spoofingowymi, zapewniając, że Twoi odbiorcy mogą ufać integralności otrzymywanych wiadomości.

.

Jak DMARC współpracuje z SPF i DKIM

Domain-based Message Authentication, Reporting, and Conformance (DMARC) opiera się na SPF i DKIM, aby zapewnić kompleksową ochronę domeny. Określa ona, w jaki sposób domena obsługuje wiadomości e-mail, które nie przeszły kontroli SPF lub DKIM. Zasady DMARC można ustawić tak, aby monitorowały, poddawały kwarantannie lub odrzucały takie wiadomości e-mail, pomagając zapobiegać nieautoryzowanemu korzystaniu z domeny. Dodatkowo, DMARC dostarcza informacji zwrotnych w postaci raportów, które szczegółowo opisują, w jaki sposób obsługiwane są wiadomości e-mail Twojej domeny, co pozwala na dostosowanie ustawień bezpieczeństwa poczty elektronicznej.

Wypełniając rekord DMARC w swojej domenie, informujesz serwer odbiorczy, jak często chcesz otrzymywać raporty XML z informacjami o tym, ile wiadomości e-mail otrzymanych przez ten serwer przeszło SPF i DKIM, a ile nie przeszło kontroli.

Kto jest Postmasterem?

Postmaster to osoba lub zespół odpowiedzialny za zarządzanie i utrzymywanie serwerów poczty e-mail dla domeny. Rola ta obejmuje konfigurowanie i monitorowanie ustawień poczty e-mail, obsługę problemów z dostarczaniem poczty oraz zapewnienie, że praktyki związane z pocztą e-mail w domenie są zgodne ze standardami i przepisami branżowymi. Postmaster jest również osobą kontaktową do odbierania i rozwiązywania problemów związanych z dostarczaniem poczty i bezpieczeństwem domeny.

Postmaster email określony w ustawieniach DMARC będzie otrzymywał wszystkie automatyczne raporty DMARC z innych serwerów pocztowych.

SAILINGBYTE

Jakie są dostępne ustawienia DMARC?

DMARC (Domain-based Message Authentication, Reporting, and Conformance) zapewnia szereg ustawień, które pozwalają właścicielom domen określić, w jaki sposób ich wiadomości e-mail są uwierzytelniane i w jaki sposób chcą otrzymywać raporty o aktywności poczty elektronicznej ich domeny.

1. **`v` (Version)**: Określa wersję DMARC, zazwyczaj `DMARC1`.
2. **`p` (Policy)**: Określa, w jaki sposób wiadomości e-mail, które nie przejdą kontroli SPF/DKIM powinny być obsługiwane (`brak`, `kwarantanna` lub `odrzuć`). Te ustawienia dają ci kontrolę nad tym, jak twoja domena obsługuje podejrzane wiadomości e-mail, pozwalając ci zrównoważyć bezpieczeństwo z dostarczalnością wiadomości e-mail.
3. **`sp` (Subdomain Policy)**: Ustawia oddzielną politykę dla subdomen, zastępując główną politykę domeny.
4. **`rua` (Aggregate Report URI)**: Wyznacza adres e-mail lub URI, na który mają być wysyłane raporty zbiorcze.
5. **`ruf` (Forensic Report URI)**: Określa adres e-mail lub URI do otrzymywania szczegółowych raportów kryminalistycznych (awarii).
6. **`pct` (Percentage)**: Wskazuje procent wiadomości e-mail, do których powinna mieć zastosowanie polityka DMARC.
7. **`adkim` (DKIM Alignment Mode)**: Określa, jak ściśle DKIM musi być wyrównany z domeną w nagłówku “From” (`relaxed` lub `strict`).
8. **`aspf` (SPF Alignment Mode)**: Kontroluje, jak ściśle SPF musi wyrównać się z domeną w nagłówku “From” (`relaxed` lub `strict`).
9. **`fo` (Forensic Options)**: Konfiguruje warunki generowania raportów kryminalistycznych na podstawie niepowodzeń SPF/DKIM.
10. **`rf` (Report Format)**: Określa format raportów kryminalistycznych, zazwyczaj `afrf`.

    .

11. **`ri` (Report Interval)**: Ustawia częstotliwość, w sekundach, otrzymywania raportów zbiorczych.

Przykładowy rekord domeny DMARC: v=DMARC1; p=quarantine; sp=none; rua=mailto:dmarc-reports@yourdomain.com; ruf=mailto:dmarc-errors@yourdomain.com; pct=100; adkim=s; aspf=s; ri=86400;

Kto otrzymuje raporty DMARC?

Raporty DMARC są zazwyczaj wysyłane na adresy e-mail określone w rekordzie polityki DMARC. Raporty te mogą być odbierane przez administratorów domeny, administratorów poczty lub innych wyznaczonych odbiorców, którzy są odpowiedzialni za monitorowanie i analizowanie ruchu e-mail i bezpieczeństwa domeny.

Kto otrzymuje raporty DMARC?

Jak filtrować raporty DMARC – DARMOWA automatyzacja!

Raporty DMARC są wysyłane nawet wtedy, gdy wszystkie kontrole SPF i DKIM zostały zaliczone. Może to spowodować przytłaczającą ilość wiadomości e-mail na skrzynce pocztowej postmastera. Z drugiej strony są one niezbędne do wczesnego wykrywania prób phishingu lub nieprawidłowych ustawień domeny, więc nie należy rezygnować z ich otrzymywania.

Raporty DMARC mogą być przytłaczające ze względu na samą ilość zawartych w nich danych. Aby usprawnić ten proces, można filtrować i analizować tylko niezbędne informacje. Jednym ze sposobów na to jest korzystanie z automatycznych przepływów pracy, takich jak bezpłatne rozwiązanie dostępne tutaj na stronie n8n automation workflow. Stworzyłem ten DARMOWY przepływ pracy N8N Automation, aby usprawnić analizę moich raportów DMARC, a teraz dzielę się nim z Tobą! Ten przepływ pracy automatycznie analizuje raporty DMARC, zapisuje je w bazie danych i powiadamia o wszelkich błędach DKIM lub SPF. Pozwala to skupić się na krytycznych kwestiach bez konieczności ręcznego przeszukiwania obszernych danych.

Podsumowanie: Automatyzacja w Sailing Byte i Twojej firmie

W Sailing Byte wykorzystujemy różne automatyzacje, aby usprawnić procesy i zwiększyć bezpieczeństwo naszych klientów. Niezależnie od tego, czy jest to rozwój oprogramowania, czy automatyzacja procesów biznesowych, jesteśmy zaangażowani w pomoc w osiąganiu celów. Automatyzacja zadań, takich jak analiza

raportów DMARC, nie tylko oszczędza czas, ale także zapewnia szybkie rozwiązywanie potencjalnych problemów. Nasza wiedza wykracza poza oprogramowanie— rozumiemy potrzeby biznesowe stojące za tymi rozwiązaniami i możemy dostosować nasze usługi do Twoich unikalnych wymagań.

Współpracując z Sailing Byte, zyskujesz partnera, który może pomóc Ci poruszać się po złożoności automatyzacji, zapewniając, że Twoja firma jest zarówno bezpieczna, jak i wydajna.