Autenticación, basada en dominios para mensajes, informes y conformidad (DMARC)

La autenticación basada en dominios para mensajes, informes y conformidad (DMARC) es una medida de autenticación de correo electrónico que protege contra actores maliciosos que utilizan direcciones de correo electrónico falsas, disfrazadas para parecer correos electrónicos legítimos provenientes de fuentes confiables. DMARC hace que sea más fácil para los remitentes y receptores de correo electrónico determinar si un correo electrónico se originó legítimamente o no por parte remitente identificado. Además, DMARC brinda al usuario instrucciones para manejar correo electrónico que sea fraudulento.

¿Por qué los funcionarios electorales estatales y locales deberían estar interesados en DMARC?

Los funcionarios electorales estatales y locales se enfrentan a un gran volumen de ataques de correo basura (*spam*) y fraudes informáticos (*phishing*) en sus sistemas accesibles por Internet. Los correos electrónicos fraudulentos son fáciles de diseñar y baratos de enviar, lo que brinda a los actores maliciosos un incentivo para usar ataques de correo electrónico repetidos. Desafortunadamente, los empleados suelen ser el punto de falla de estos ataques, cuando se ven obligados a determinar repetidamente si los correos electrónicos son legítimos o falsos. DMARC proporciona una solución automatizada a este problema, lo que facilita la identificación de mensajes de *spam* y *phishing* antes de que lleguen a la bandeja de entrada de un empleado.

¿Cómo funciona DMARC?

DMARC elimina el riesgo. por parte de quien recibe el mensaje, de tener que adivinar cómo manejar correos electrónicos fallidos, limitando o eliminando la exposición del usuario a mensajes potencialmente fraudulentos y dañinos. Las medidas DMARC permiten que un remitente indique que sus correos electrónicos están protegidos por el marco de política del remitente (SPF, por sus siglas en inglés) y/o el mensaje identificado por claves de dominio (DKIM, por sus siglas en inglés), los cuales son técnicas de autenticación de correo electrónico reconocidas en la industria. DMARC también proporciona instrucciones sobre cómo el receptor debe manejar los correos electrónicos que no pasan la autenticación SPF o DKIM. Las opciones suelen incluir enviar el correo electrónico a cuarentena o rechazarlo por completo. Por último, DMARC proporciona al receptor una dirección de correo electrónico para mandar comentarios al remitente. Los posibles comentarios pueden incluir que el receptor rechazó o puso en cuarentena el correo electrónico del remitente o que un actor malicioso está intentando imitar el dominio del remitente.

¿Cómo puedo adoptar DMARC en mi dominio?

La adopción de DMARC no es una transición fluida y requiere que los departamentos de IT trabajen con empleados sin experiencia técnica para garantizar que todos reciban los mensajes que necesitan. A continuación, se presentan una serie de pasos que las organizaciones pueden tomar poco a poco con el fin de facilitar el uso de DMARC.

1. Implemente DKIM y SPF. Tiene que cubrir primero las partes básicas.
2. Asegúrese de que sus anuncios publicitarios alineen correctamente a los identificadores apropiados.
3. Publique un registro DMARC con el indicador "ninguno" para las medidas, lo cual requiere informes de datos.
4. Analice los informes de datos y modifique sus flujos de correo según corresponda.
5. Modifique los indicadores de sus medidas DMARC de "ninguno" a "cuarentena" a "rechazar" cuando ya haya adquirido experiencia.