ASOCIACIÓN NACIONAL DE UNIVERSIDADES
E INSTITUCIONES DE EDUCACIÓN SUPERIOR

Dirección General de Administración
Dirección de Tecnologías de la Información y Comunicación

Seguridad en el correo electrónico

Contenido

Importancia de la seguridad en el correo electrónico 3
Riesgos en el uso de correo electrónico 4
Phishing 4
Crecimiento de la ciberdelincuencia y de los ataques phishing 4
Spoofing 6
Email spoofing 6
Uso por spam y gusanos 7
Ransomware 8
Man in The Middle 9
Cómo prevenir los ataques Man in the Middle 9
Consejos para navegar por Internet 9
Recomendaciones de seguridad para uso de correo electrónico 10
Referencias 13

Importancia de la seguridad en el correo electrónico

¿Te has parado a pensar en la cantidad de información confidencial puedes tener en tu correo electrónico? ¿Has pensado como proteges la seguridad de tu correo electrónico?

Día a día enviamos y recibimos cientos de correos, personales y profesionales, con información comprometida, sensible, personal…. etc.

A través del correo electrónico enviamos contraseñas, información sobre clientes, informes del trabajo, contratos, datos bancarios, credenciales, información personal… Toda se envía como un texto plano, echo el cual permite, llegado el caso, que esta información sea leída por el destinatario y por cualquier intermediario.

La mayoría de los usuarios, utilizamos los servicios de mensajería instantánea y correo electrónico de moda, como pueden ser Outlook, Yahoo! o Gmail como opción para comunicarnos.

En el ámbito profesional, el correo electrónico es uno de los canales de comunicación más habitual, para que la empresa interactúe con sus clientes; pero partiendo de esta premisa, no hemos de olvidar que también es uno de los menos seguros.

La mayoría de los usuarios profesionales utilizan el correo electrónico para interactuar y mantener el contacto constantemente con sus clientes, pero es una realidad contrastada según diferentes encuestas, que la mayoría no son conscientes de la importancia de tomar medidas de seguridad en el intercambio de información a través del email.

Pero ¿Cómo se producen los ciberataques y se vulnera la seguridad de tu correo electrónico?

A continuación se mostrarán algunos de los ataques más comunes en los servicios de correo electrónico y algunas recomendaciones para evitarlos.

Riesgos en el uso de correo electrónico

Phishing

Uno de los ataques más fáciles y barato, usado habitualmente por los ciberdelincuentes y quizás el más conocido por los usuarios del mundo digital, es el ataque por **"Phishing".**

El vector de ataque del "Phishing", utiliza una máxima reconocida en el mundo de la ciberseguridad **"el eslabón más débil de la cadena de seguridad siempre es el usuario"** máxima que, trasladada al mundo empresarial, podríamos traducir como "**el eslabón más débil de la cadena de seguridad en una compañía, son sus usuarios y por extensión sus cuentas de correo electrónico"**.

Crecimiento de la ciberdelincuencia y de los ataques phishing

Conscientes de estas máximas, los ciberdelincuentes explotan diferentes oportunidades, algunas de ellas de nueva aparición, para hacer que las campañas de phishing obtengan unos resultados mucho más efectivos.

Por ejemplo, utilizando la Inteligencia Artificial (IA), los ciberdelincuentes pueden descubrir estilos de escritura, comportamiento o tendencias de los empleados en sus mensajes, aspectos personales del empleado… etc.

Con esta información, los ciberdelincuentes, utilizando metodologías y técnicas de ingeniería social, consiguen enviar correos electrónicos "fraudulentos" los cuales resultan tan convincentes, que primo pasan los filtro de seguridad informática de las Compañías, para después cumplir con el objetivo de que los usuarios en base a esa ingeniería social, crean en los mensajes y contenidos del mismo y faciliten al ciberdelincuente, obtener el objetivo final del mismo, el cual no es otro que conseguir atacar maliciosamente la información de la compañía.

En este sentido, los expertos en seguridad y las tecnologías, avanzan de una manera continuada, lo cual hace que constantemente seamos testigos de la aparición de soluciones e innovaciones que dificultan a los ciberdelincuentes la consecución de sus objetivos.

En la actualidad, se están desarrollando, llevando a cabo ensayos y finalmente usando nuevas tecnologías pioneras en muchos casos, tales como la Inteligencia Artificial, para automatizar la detección de phishing.

“Las nuevas tecnologías, contribuyen a crear un amplio abanico de soluciones tecnológicas punteras y especializadas en la prevención de los ataques a través del correo electrónico”.

Una compañía, independientemente del sector en el que opere, ha de entender que, para asegurar el correo electrónico corporativo y la información que se alberga adjunta al mismo, es esencial disponer de barreas de seguridad en diferentes niveles y perspectivas, las cuales contribuyan a la defensa en profundidad dichos datos de la compañía.

Estas barreras de seguridad, enfocadas al uso del correo electrónico de una empresa, permiten analizar las redes de comunicación del mismo, entender los patrones y comportamientos de envíos de correos de los usuarios, con el objetivo de poder determinar cuáles son “normales” y cuáles no, detectando así posibles anomalías, ataques y errores.

Para mantener la seguridad de tu correo electrónico, actualmente existen herramientas capaces de generar informes en tiempo real.

En estos informes se reflejan anomalías, ataques y errores en el total de correos que entran y salen a través de los sistemas de información de las Compañías.

Además, estas herramientas, pueden especificar qué acciones se han determinado llevar acabo con los emails anómalos, atacados o erróneos que se hayan detectado; aspecto este, el de auditoria, cada vez más importante, para saber ¿Qué ha pasado? y ¿Por qué ha pasado?

Spoofing

La **suplantación** de identidad (en inglés *spoofing*), hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Se pueden clasificar sus ataques en función de la tecnología utilizada. Entre ellos el más extendido es el IP spoofing, aunque también existe el ARP spoofing, DNS spoofing, Web spoofing o email spoofing. Este último es en el que nos enfocaremos y trataremos de evitar. Todos ellos se engloban en la idea de que cualquier tecnología de red es susceptible de sufrir suplantaciones de identidad.

Email spoofing

Email spoofing es la creación de mensajes de correo electrónico con una dirección de remitente falso. Es fácil de hacer porque los protocolos básicos del servicio de correo electrónico no tienen ningún mecanismo de autenticación. Se puede llevar a cabo desde dentro de la LAN o desde un entorno externo utilizando troyanos. Los correos electrónicos de *spam* y *phishing* suelen utilizar este engaño para inducir a error al destinatario sobre el origen del mensaje.

Detalles técnicos

Cuando se envía un correo electrónico SMTP, la conexión inicial ofrece dos piezas de información de la dirección:

MAIL FROM: - presenta generalmente al destinatario como la cabecera *Return-path:* (ruta de retorno:), pero normalmente no es visible para el usuario final, y por omisión no se hacen chequeos de que el sistema de envío esté autorizado a enviar en nombre de esa dirección.

RCPT TO: - específica a qué dirección de correo electrónico debe entregarse el mensaje, normalmente no es visible para el usuario final, pero puede estar presente en las cabeceras como parte de la cabecera *Received:* ("Recibido:").

En conjunto, se refieren a éstos a veces como el direccionamiento del "sobre", por analogía con un sobre de papel tradicional.

Una vez que el servidor de correo receptor avisa que acepta estos dos artículos, el sistema de origen envía el comando "DATA", y por lo general envía varios elementos de encabezado, incluyendo:

De: Joe Q Doe <joeqdoe@example.com> - la dirección visible para el receptor; pero una vez más, de forma predeterminada no se hacen chequeos de que el sistema de envío esté autorizado a enviar en nombre de esa dirección.

Responder-a: Jane Roe <Jane.Roe@example.mil> - no se comprueba de manera similar

El resultado es que el destinatario de correo electrónico vea el correo electrónico como provenientes de la dirección en la cabecera *From:* veces que puede ser capaz de encontrar la dirección de MAIL FROM; y si responden a la dirección de correo electrónico que va a ir a cualquiera de la dirección presentada en el MAIL FROM: o la Cabecera Responder a: - pero ninguna de estas direcciones son típicamente confiables, por lo que los mensajes de rebote automatizados pueden generar retrodispersión.

Uso por spam y gusanos

Malware como Klez y Sober y muchos ejemplos más modernos a menudo buscan direcciones de correo electrónico en el ordenador que han infectado, y utilizan esas direcciones tanto como objetivos para el correo electrónico, como para crear campos "FROM" creíbles en los correos electrónicos que forjan, por lo que estos correos son más propensos a ser abiertos. Por ejemplo:

1. Alice recibe un correo electrónico infectado el cual ella abre, ejecutando el código del gusano.
2. El código del gusano busca en la libreta de direcciones de correo electrónico de Alice y encuentra las direcciones de Bob y Charlie.
3. Desde el equipo de Alice, el gusano envía un correo electrónico infectado a Bob, pero alterado para aparentar haber sido enviado por Charlie.

En este caso, incluso si el sistema de Bob detecta el correo entrante como conteniendo malware, él ve a la fuente como Charlie, a pesar de que realmente vino de la computadora de Alice; Mientras tanto Alice permanece inconsciente de que su ordenador ha sido infectado con un gusano.

Ransomware

El ransonmware es un tipo de malware muy peligroso que es capaz de **bloquear el acceso a nuestro equipo quitándonos el control y cifrando nuestros archivos,** para luego pedir un **rescate económico para liberarlos**.

Cualquier dispositivo puede ser objeto de ataque, ya sea un ordenador, una tablet o teléfono móvil.

Las cantidades solicitadas son bastante variables, aunque, por lo general, no suelen ser demasiado abultadas. De esta forma, consiguen un volumen alto de dinero procedente de muchas víctimas, haciendo muy rentable este tipo de ataques.

Nunca debes ceder al chantaje y pagar el rescate ya que lo más seguro es que jamás recuperes los archivos. Además, el pago sentaría un precedente y puedes volver a ser objeto de nuevos ataques pues, los ciberdelincuentes saben que estás dispuesto a pagar.

Actúa siempre con calma y **no te dejes llevar por el pánico.** Lo primero que debes hacer es salvaguardar el resto de dispositivos que estén conectados en la misma red, por lo que **desconecta inmediatamente el equipo infectado** de la red (cable o WiFi) para evitar que se expanda a otros equipos y servicios compartidos.

Como medida preventiva, ten **una buena política de backup** que esté aislada del entorno del dispositivo infectado. Si te atacan siempre podrás restaurarlos en otro ordenador.

Mantén siempre tus dispositivos actualizados con los últimos parches de seguridad, ya que es crítico para evitar que este tipo de malware se aproveche de vulnerabilidades existentes para perpetrar el ataque.

Man in The Middle

En el mundo de la seguridad informática, un ataque **«*man in the middle*«** o si lo traducimos literalmente a «hombre en el medio», es un tipo de amenaza que se aprovecha de un intermediario. El atacante en este caso, tiene la habilidad de **desviar o controlar las comunicaciones entre dos partes**. Por ejemplo, si se tratase de un ataque MITM a tu correo, el perpetrador podría desviar todos los e-mails a una dirección alterna para leer o alterar toda la información antes de enviarla al destinatario correcto.

Digamos que te conectas a una red WiFi en la calle para revisar tus redes sociales y tu email tranquilamente. Un *hacker* malintencionado puede interceptar las comunicaciones entre tu computadora o tu *smartphone* y la red WiFi, teniendo acceso a todo lo que haces. Si la red WiFi no está cifrada, y el atacante está cerca del rango de la conexión, se puede insertar a sí mismo como «el hombre en el medio». Siempre que el atacante pueda autenticarse como los dos lados de la comunicación, tendrá todo el acceso.

Cómo prevenir los ataques Man in the Middle

Por norma general es casi imposible que los afectados puedan reconocer la presencia de un ataque de intermediario, por lo que la prevención se convierte en la mejor forma de protección. A continuación, presentamos una recopilación de los consejos más importantes para que los usuarios de Internet y operadores de páginas web puedan minimizar el riesgo de convertirse en blanco de un ataque MITM.

Consejos para navegar por Internet

Nadie está libre de pecado y haber cometido un error que cree más de un problema, o estar cerca de cometerlo. Para ello, si quieres prevenir y limitar al mínimo las posibilidades de ser atacado, sigue estos consejos de seguridad cuando entres en la Red:

- Asegúrate de acceder siempre a cualquier web que utilice un certificado SSL. Las direcciones que empiezan con “https” son seguras y puedes acceder a ellas con plena libertad, mientras que las que solo tienen “http” pueden provocarte quebraderos de cabeza.

- Tener siempre actualizado tu navegador a la última versión disponible además de tener el sistema operativo también al día.
- Evita usar redes VPN de acceso libre o servidores proxy.
- Actualiza tus contraseñas y utiliza diferentes claves para cada web.
- Evita conectarte, en la medida de lo posible, a redes wifi abiertas (hoteles, estaciones de tren, tiendas, etc.).
- Evita descargar información confidencial o transmitir datos de inicio de sesión en redes públicas, y por supuesto no uses tu tarjeta de crédito en estas redes.
- Si ves un correo electrónico cuyo remitente no te suena, elimínalo. Pueden contener malware y fastidiarte el día.

Recomendaciones de seguridad para uso de correo electrónico

El uso del email en las empresas es algo que ha cambiado la forma en la que nos comunicamos. Es barato, rápido, puedes enviarlo a varias personas, adjuntar archivos, etc. Los ciberdelincuentes detectaron hace ya unos años el incremento de este uso y no tardaron en crear diferentes tipos de infracciones en la red para obtener beneficios. Por esta razón, debemos tener cuidado con el uso que hacemos del correo electrónico, ya que los delitos informáticos han experimentado una tendencia creciente durante los últimos años en todo el mundo.

¿Utilizas con seguridad tu correo electrónico? Para evitar estar expuesto a estos ciberataques, sigue estos consejos para utilizar tu correo electrónico con seguridad:

1. Si **no conoces la procedencia** de un correo electrónico y te llegan varios correos electrónicos al día, llévalo a la carpeta de SPAM.

2. Deshabilita la carga de imágenes automática.
3. ¡Cuidado con los archivos adjuntos! Si desconoces la procedencia del remitente procura no abrirlos y menos cuando tengan la **extensión .exe**
4. **Borra el historial**, la caché de tu navegador periódicamente y evita marcar la opción de guardar contraseñas.
5. Utiliza **diferentes contraseñas** para las cuentas de correo electrónico a las que tienes acceso, y modifica las contraseñas con cierta frecuencia (4-6 meses).
6. No abras correos con ofertas, regalos o falsas promociones del tipo: "Te ha tocado un viaje a Nueva York con todos los gastos pagados".
7. Pasa el cursor del ratón sobre los enlaces del email antes de abrirlos, para que puedas comprobar si la dirección URL es correcta.
8. La **técnica de Phising** es una práctica muy habitual entre los cibercriminales que afecta cada vez a más empresas. Este crimeware (ciberdelito con fines fiscales) consiste en suplantar la identidad para obtener un beneficio económico. Evita dar tus datos personales, bancarios o contraseñas a través de correos electrónicos.
9. Asegúrate de **cerrar la sesión de correo** cada vez que terminas de trabajar.
10. Cuidado con las redes wifi públicas (normalmente sin contraseña). Estás expuesto a que alguien esté capturando información de todos tus datos personales o esté observando tu correo electrónico.
11. Utiliza la **copia oculta BCC o CCO** cuando envíes correos a varias personas, de esta manera se ocultarán sus correos a los demás.
12. Utiliza una **solución de correo electrónico con cifrado** para controlar toda tu información confidencial.

13. No publiques tu correo electrónico en sitios web, foros, redes sociales o espacios donde se comparte contenido, ya que estos se han convertido en los principales escenarios de acción de los envíos masivos de spam.
14. Ten actualizados tus programas y tu sistema operativo. En las actualizaciones, muchas veces se incluyen mejoras de seguridad. Con tu software actualizado cerrarás posibles puntos de entrada que ya se conozcan.
15. Por otro lado, también es importante llevar a cabo un **periodo de formación y educación del usuario** en cuanto a seguridad en Internet se refiere, puesto que todo el mundo está capacitado para enviar un correo electrónico, pero no todas las personas saben protegerse de las amenazas no deseadas que hay presentes en la red.

El tiempo corre en contra de los usuarios; por lo que resulta importante que tanto usuarios domésticos como empresariales, se conciencien y comprendan la evolución de la ciberdelincuencia entorno al uso de email; así como la continua aparición de herramientas y soluciones, los cuales de una u otra manera nos ayudan a protegernos de los ataques dirigidos contra el correo electrónico.

Cada vez son más las compañías que se están dando cuenta de la necesidad de establecer medidas de seguridad contra estas prácticas; ya no solo por asegurar la privacidad de los datos que residen en la misma; sino también pensando en sus clientes.

Es más común en las compañías, que las partidas presupuestarias destinadas a la ciberseguridad, aumenten considerablemente año a año. De igual modo, es cada vez más habitual que los CEO sientan mayores preocupaciones con todos los temas relacionados con las TIC y la ciberseguridad.

Así es que, teniendo en cuenta el escenario ¿cómo te preocupas tu o tu compañía para protegerte de los ciberataques dirigidos al correo electrónico doméstico o corporativo?

Referencias

Rodríguez, A. (2019, octubre 24). ¿Qué es una ataque Man in the Middle? Recuperado 29 de mayo de 2020, de https://es.godaddy.com/blog/que-es-una-ataque-man-in-the-middle/

colaboradores de Wikipedia. (2019, octubre 4). Email spoofing - Wikipedia, la enciclopedia libre. Recuperado 29 de mayo de 2020, de https://es.wikipedia.org/wiki/Email_spoofing

Tecteco, P. (2019, marzo 11). El phishing y otras formas de ataque a través del email. Recuperado 29 de mayo de 2020, de https://www.tecteco.com/el-phishing-y-otras-formas-de-ataque-a-traves-del-email/

CIC Consulting Informático. 2020. ¿Cómo Garantizar La Seguridad De Tu Correo Electrónico?, Recuperado de 29 mayo de 2020, de https://www.cic.es/seguridad-de-correo-electronico