UNIVERSIDAD TECNOLOGICA DEL VALLE DEL MEZQUITAL

UNIDAD I

AMENEZA PHISHING

DOCENTE:

ING. ALFREDO PEREZ GOMEZ

INTEGRANTES:

MIGUEL ANGEL BASILIO FRANCO

OMAR MENDOZA RAMIREZ

MARIA DEL ROCIO SANCHEZ BARRERA

ÍNDICE

INTRODUCCIÓN

El phishing es una de las amenazas cibernéticas más comunes y peligrosas, que consiste en engañar a las víctimas para que revelen información confidencial, como contraseñas o detalles financieros, a través de correos electrónicos o sitios web fraudulentos. Estos ataques pueden tener graves repercusiones, desde pérdidas económicas hasta daños irreparables en la reputación de una organización. Además, el robo de datos confidenciales y la interrupción de las operaciones pueden impactar significativamente la productividad. Dada su sofisticación creciente, es esencial que tanto los usuarios como las organizaciones adopten medidas preventivas y de respuesta adecuadas para minimizar los riesgos asociados con el phishing.

AMENEZA DE PHISHING

Un ataque de phishing puede tener graves consecuencias para las víctimas, incluyendo:

Consecuencias financieras: Los ataques de phishing pueden llevar a la pérdida de dinero y activos financieros, ya que los delincuentes pueden acceder a información confidencial y utilizarla para realizar transacciones fraudulentas.

Daño a la reputación: Un ataque de phishing puede dañar la reputación de una organización, ya que puede generar una pérdida de confianza entre los clientes y los empleados.

Pérdida de datos: Los ataques de phishing pueden llevar a la pérdida de datos confidenciales, lo que puede tener graves consecuencias para las víctimas.

Impacto en la productividad: Los ataques de phishing pueden interrumpir la productividad y el funcionamiento normal de una organización, ya que los empleados pueden necesitar tiempo y recursos para recuperar la información perdida y restaurar la seguridad.

CASO DE ATAQUE DE PHISHING

UN ATAQUE DE PHISHING AFECTÓ MÁS DE UN MILLÓN DE CUENTAS DE GMAIL EN 2017.

El ataque de phishing afectó aproximadamente a un millón de usuarios de Gmail, lo que equivale a menos del 0.1% de los usuarios del servicio según la declaración de Google. El ataque se esparció rápidamente a través de correos electrónicos falsos, en los que los destinatarios recibían invitaciones para acceder a un supuesto archivo en Google Docs. Este tipo de ataque permitió a la aplicación falsa acceder a la cuenta de los usuarios, leer correos y propagarse a través de los contactos de los afectados.

Daños o repercusiones que generó:

- El ataque llevó a la comprometida de millones de cuentas de Gmail, con los atacantes ganando acceso a información sensible como contraseñas, contactos y correos electrónicos.
- El ataque fue altamente sofisticado, utilizando una combinación de phishing y malware para engañar a los usuarios para divulgar sus credenciales de inicio de sesión.
- El ataque fue llevado a cabo por un grupo de hackers que utilizaron una aplicación de terceros para acceder a los sistemas de Google.
- El ataque fue tan severo que Google emitió una advertencia a todos sus usuarios, instándolos a cambiar sus contraseñas y habilitar la autenticación de dos factores.
-

Acciones tomadas:

Google reaccionó rápidamente una hora después de que el ataque comenzara a propagarse, implementando las siguientes medidas:

- Google lanzó inmediatamente una investigación sobre el ataque y tomó medidas para contener el daño.
- Bloqueo inmediato de los correos de phishing.
- La empresa notificó a los usuarios afectados y les proporcionó orientación sobre cómo asegurar sus cuentas.
- Google también implementó medidas de seguridad adicionales para prevenir ataques similares en el futuro.
- La empresa trabajó con agencias de aplicación de la ley para identificar y procesar a los atacantes.

Cómo se podría haber minimizado o prevenido:

- Mejora en la educación del usuario: Informar a los usuarios sobre cómo identificar correos electrónicos sospechosos, como diferencias en las invitaciones de Google Docs, podría haber frenado la propagación del ataque.
- Los usuarios podrían haber sido más vigilantes y cautos al hacer clic en enlaces o descargar archivos adjuntos de fuentes desconocidas.
- Google podría haber implementado medidas de seguridad más robustas, como la autenticación de dos factores, para prevenir que los atacantes accedieran a las cuentas.
- La empresa podría haber sido más proactiva en monitorear sus sistemas para detectar actividad sospechosa y responder rápidamente a informes de ataques de phishing.
- Los usuarios podrían haber sido más cuidadosos al otorgar acceso a aplicaciones de terceros, y Google podría haber proporcionado más orientación sobre cómo administrar permisos de aplicaciones.

Qué se implementó para prevenirlo:

- Google implementó medidas de seguridad adicionales, como la autenticación de dos factores, para prevenir ataques similares en el futuro.
- La empresa también mejoró sus sistemas de monitoreo y respuesta para detectar rápidamente actividad sospechosa.
- Google proporcionó más orientación a los usuarios sobre cómo asegurar sus cuentas y administrar permisos de aplicaciones.
- La empresa también trabajó con agencias de aplicación de la ley para compartir información y mejores prácticas para prevenir ataques similares.

CONCLUSIÓN

En conclusión, los ataques de phishing representan una amenaza significativa para individuos y organizaciones, con consecuencias que abarcan desde pérdidas financieras hasta daños en la reputación y pérdida de datos. Sin embargo, a través de una combinación de medidas proactivas, como la educación continua de los usuarios, la implementación de autenticación de dos factores y sistemas de monitoreo robustos, es posible minimizar el riesgo de estos ataques. Las lecciones aprendidas de casos anteriores, como el ataque a millones de usuarios de Gmail, destacan la importancia de una respuesta rápida y la colaboración entre las empresas y las agencias de seguridad para mitigar el impacto de futuros incidentes. La prevención sigue siendo el mejor enfoque frente a esta creciente amenaza cibernética.

BIBLIOGRAFÍAS

Benishti, E. (2018, enero 23). *The phishing lures of 2017*. Linkedin.com. https://www.linkedin.com/pulse/phishing-lures-2017-eyal-benishti

CybSafe. (2023, julio 3). *The ripple effect: How one phishing attack can cause disaster across your organization*. CybSafe. https://www.cybsafe.com/blog/how-can-phishing-affect-a-business/

Johnson, A. (2017, mayo 4). *Massive phishing attack targets millions of Gmail users*. CNBC. https://www.cnbc.com/2017/05/04/gmail-google-hack-phishing-attack.html

(S/f). Reddit.com. Recuperado el 27 de septiembre de 2024, de https://www.reddit.com/r/google/comments/692cr4/new_google_docs_phishing_scam_almost_undetectable/?rdt=48749