Restauración Colectiva
El portal de referencia para los profesionales del sector

Anatomía del *phishing*: los ciberdelincuentes atacan a los correos corporativos

Martes, 21 de mayo 2024

Los ataques de *phishing* están entre las tácticas más extendidas y efectivas utilizadas por los ciberdelincuentes contra empresas. Estos ataques buscan engañar a los empleados para que revelen información sensible, como credenciales de acceso o datos financieros, haciéndose pasar por fuentes legítimas. El *phishing* adopta diversas formas, y a menudo se dirige a los sistemas de correo electrónico corporativo debido a la gran cantidad de información valiosa que contienen.

Según el informe *'The State of Email Security 2023'* de Mimecast, el 83% de los directores de seguridad encuestados ven el correo electrónico como la principal fuente de ciberataques. El caso reciente del Grupo Pepco demostró las graves consecuencias que pueden suponer los ataques de *phishing* en un negocio. A finales de febrero, la empresa minorista informó de que su filial húngara había sido víctima de un sofisticado ataque de *phishing*, perdiendo aproximadamente 15,5 millones de euros en efectivo. Este incidente pone de manifiesto la creciente amenaza que suponen los ciberdelincuentes y subraya la necesidad crítica de que las organizaciones refuercen sus defensas de ciberseguridad.

En respuesta a este problema, desde **Kaspersky** (compañía global de ciberseguridad y privacidad digital) nos mandan este artículo en el que desarrollan la 'anatomía de un ataque de *phishing*' para ayudar a las empresas a protegerse eficazmente contra posibles brechas.

1. **Motivación de los ciberdelincuentes.** Los ataques de *phishing* provienen de ciberdelincuentes motivados por varios factores. Principalmente, buscan ganancias financieras mediante la adquisición ilegal de información sensible como detalles de tarjetas de crédito o credenciales de acceso, que pueden ser vendidas o utilizadas en transacciones fraudulentas. Además, algunos están motivados por agendas políticas o ideológicas, o por fines de espionaje. A pesar de las diferentes motivaciones, estos ataques representan graves riesgos para las empresas.

2. **El acercamiento inicial.** Por lo general, los ataques de *phishing* comienzan con la creación de correos electrónicos fraudulentos diseñados para inducir a los destinatarios a actuar. Estos correos a menudo imitan comunicaciones legítimas de fuentes fiables, como compañeros, socios comerciales u organizaciones reputadas. Para aumentar la credibilidad, los atacantes pueden emplear tácticas como suplantación de direcciones de envío o replicación de la marca corporativa. La situación se agrava aún más con la aparición de ataques de *phishing* impulsados por IA, que utilizan algoritmos sofisticados para crear correos electrónicos de *phishing* altamente convincentes y personalizados. Esto empeora el desafío de detectar y combatir tales amenazas.

3. **Contenido engañoso y técnicas.** El éxito de los ataques de *phishing* radica en la explotación de las vulnerabilidades humanas. Los ciberdelincuentes aprovechan técnicas de manipulación psicológica, obligando a las víctimas a actuar impulsivamente sin evaluar completamente la legitimidad del correo electrónico. Los correos electrónicos de *phishing* emplean diversas estrategias para engañar a los destinatarios y obtener las respuestas deseadas, entre las que destacan:

    - **Falsas premisas:** los correos pueden manifestar urgencia o importancia, instando a los destinatarios a actuar rápidamente para evitar supuestas consecuencias o para aprovechar oportunidades percibidas.
    - **Ingeniería social:** los atacantes personalizan correos electrónicos y adaptan los mensajes a los intereses, funciones o preocupaciones de los destinatarios, lo que aumenta la probabilidad de atraer a la víctima.
    - **Enlaces y archivos adjuntos maliciosos:** a menudo los correos electrónicos de contienen enlaces a páginas web fraudulentas o archivos adjuntos maliciosos diseñados para recopilar credenciales, instalar malware o iniciar transacciones no autorizadas.

4. **Evadir detección.** Para evitar la detección por filtros de seguridad de correo electrónico y soluciones anti-*phishing*, los ciberdelincuentes perfeccionan constantemente sus tácticas y se adaptan a las medidas de ciberseguridad en evolución. Pueden emplear técnicas de ofuscación, métodos de cifrado o redirección de URL para eludir la detección y aumentar la efectividad de sus ataques.

5. **Consecuencias de los ataques de *phishing* exitosos.** Cuando los ataques de *phishing* tienen éxito, las consecuencias pueden ser graves para las organizaciones. Las violaciones de los sistemas de correo electrónico corporativo pueden provocar el acceso no autorizado a datos confidenciales, pérdidas financieras, daños a la reputación e incumplimiento de la normativa. Además, las cuentas de correo electrónico comprometidas pueden servir de punto de apoyo para otros ciberataques, como la suplantación del correo electrónico corporativo o la filtración de datos.

6. **Estrategia de mitigación.** Para protegerse contra los ataques de *phishing* dirigidos a los sistemas de correo electrónico corporativo, las organizaciones deben aplicar medidas de ciberseguridad sólidas y educar a los empleados sobre la concienciación y las mejores prácticas en materia de *phishing*. Las estrategias de mitigación eficaces incluyen formación de los empleados, introducción de la autenticación multifactor, formulación de planes de respuesta a incidentes y despliegue de soluciones avanzadas de filtrado y seguridad del correo electrónico.

Notícias Relacionadas

- ¿Cómo ayuda la IA a las colectividades? Decálogo y dos soluciones a tener en cuenta
- Caso real de digitalización en hospitales: 66% de reducción en llamadas de enfermería a cocina
- Digitalizar el sistema de trazabilidad alimentaria, ¿es imprescindible en todos los casos?
- Digitalización en hospitales: normalizando el servicio de alimentación más allá de las dietas

