FRAUDE TELEFÓNICO

DESTACAR LA NECESIDAD DE ASEGURAR LOS SISTEMAS DE COMUNICACIÓN DE LAS EMPRESAS

NOTA DE APLICACIÓN

Alcatel·Lucent Enterprise

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN

El fraude realizado a proveedores de servicios de telefonía, operadores, abonados y empresas, se está incrementando. Este aumento está motivado por las sumas de dinero que obtienen los estafadores aprovechando la ausencia de una autoridad reguladora internacional eficaz en materia de telecomunicaciones y la falta de mecanismos de refuerzo que las protejan, además de los fallos de seguridad en los sistemas de telecomunicaciones en las organizaciones.

ESCENARIOS DE CLIENTE

1. El director de TI de una compañía detecta un elevado número de llamadas de larga distancia a un país con el que no tienen relaciones comerciales, fuera del horario normal de oficina.
2. El informe de contabilidad mensual de otra compañía muestra un importante volumen de llamadas a números internacionales, realizadas desde un mismo número interno.
3. Una tienda con 20 empleados recibe una factura telefónica mensual por un importe equivalente a su gasto telefónico de los últimos 3 años.
4. Una organización recibe una alerta de fraude de su compañía telefónica, al mismo tiempo que detecta múltiples llamadas cortas regulares a un número con tarifa especial.

Las pérdidas por fraude han aumentado un 15,4 % desde 2011.

¿QUÉ HA PASADO?

Estos escenarios son ejemplos de clientes que han sufrido fraudes telefónicos. Todas las organizaciones, desde pequeñas oficinas a compañías multinacionales son víctimas potenciales, independientemente de su proveedor de sistemas de comunicación. Y el número de ataques está aumentando rápidamente.

El fraude telefónico consiste en el uso no autorizado de un servicio de comunicación por un tercero desconocido. Puede consistir en la reventa ilegal de minutos de llamadas a números de larga distancia a través de una entidad libre de sospecha (a través de centralita). Otro ejemplo consiste en el fraude a números de servicios con tarificación especial, en las que se utiliza un sistema o servicio de comunicación para realizar llamadas a números de servicios con tarifas especiales que aplican cargos por minuto o por llamada al abonado.

El fraude puede ocasionar enormes pérdidas económicas antes de que pueda detectarse, en el peor de los casos, puede transcurrir un mes entero antes de recibir el extracto mensual y que se detecte el fraude. El fraude puede incluso dañar la imagen de marca, ya que se han dado casos en los que clientes han realizado llamadas a sus asesores que han sido desviadas a numeros de tarificación especial sin relación alguna, que podían incluso prestar servicios comprometedores. Además, sobrecargando los recursos del servidor de comunicación, estos fraudes afectan a la disponibilidad de los servicios de telefonía y pueden llegar a causar la pérdida total del servicio.

Pérdidas mensuales estimadas por ataques a centralitas en 2013:

4 400 millones $ (USA)*

¿Por qué aumenta el fraude telefónico?

La expansión de los medios y las redes sociales ha hecho que ahora resulte muy sencillo crear y distribuir materiales, vídeos y tutoriales que explican cómo poner en riesgo los sistemas de comunicación. Se necesita un nivel muy básico de conocimientos en telecomunicaciones para acceder a servicios no autorizados y ganar dinero con las comunicaciones aprovechando los recursos de las compañías atacadas.

Además, aunque hay mecanismos de protección integrados en los sistemas de comunicación, las recomendaciones de seguridad del proveedor no siempre se implantan completamente y las configuraciones no se optimizan por una falta de concienciación sobre el problema. Estos descuidos en la seguridad pueden facilitar los ataques de piratas informáticos.

Finalmente, las compañías con sistemas más anticuados se encuentran potencialmente más expuestas a este tipo de amenazas.

¿Cómo operan los estafadores?

Generalmente, los estafadores obtienen acceso a un sistema de comunicación desde fuera de la compañía debido a irregularidades en el sistema de seguridad. En el pasado, era necesario introducirse en la centralita directamente a través del puerto de mantenimiento, pero los métodos han evolucionado y ahora emplean aplicaciones de desvío de llamadas de voz y engañan a los usuarios de forma que resulta muy difícil rastrear y detectar el fraude pues la llamada se realiza desde una “entidad fiable”.

Los métodos más frecuentes son:

Mantenimiento remoto

Los piratas informáticos detectan el módem conectado al puerto de mantenimiento e intentan conectarse con la contraseña predeterminada que los administradores muchas veces no cambian. Una vez dentro del sistema, los piratas pueden cambiar la configuración, así como los nombres de usuario y contraseñas.

Buzón de voz

Este método ataca el buzón de voz, al que acceden gracias a un deficiente control de contraseñas. Generalmente, el ataque tiene por objeto utilizar el sistema de buzón de voz para realizar llamadas al exterior a un número con tarifa especial o de larga distancia. Los puertos de conferencia con capacidad para multiconferencia de varias líneas suelen ser el principal objetivo de este tipo de ataques.

Restricción selectiva de llamadas salientes

Además del deficiente control de contraseñas, los piratas informáticos se aprovechan de la ineficacia de los sistemas de control de llamadas, que fácilmente permite que mediante un software de war dialing se realicen llamadas ilimitadas a números de tarificación especial o larga distancia.

DISA (Acceso directo al sistema)

Este servicio, diseñado para empleados que trabajan de forma remota, les permite acceder a los servicios telefónicos internos desde localizaciones remotas. La centralita se puede controlar parcial o totalmente de forma remota por usuarios malintencionados si el servicio DISA no está lo suficientemente protegido (por ejemplo, con un solo código de acceso o no dispone de control sobre la identidad del llamante).

Transferencia y desvío de llamadas al exterior

Los permisos para llamadas internacionales, si no se configuran adecuadamente, hacen posible que los piratas informáticos puedan desarrollar fácilmente sus actividades fraudulentas. Algunos de estos fraudes requieren, no obstante, la complicidad de alguien dentro de la compañía.

¿CUÁLES SON LAS MOTIVACIONES DEL ESTAFADOR?

Aunque el fraude puede utilizarse para dañar económicamente a una compañía o dañar la reputación de un competidor, la motivación más frecuente es obtener un ingreso económico. En Alcatel-Lucent hemos visto casos en los que los estafadores han obtenido 20 000 $ (USA) en cuatro horas: dinero fácil y rápido. Los estafadores pueden incluso estar dentro de la compañía, empleados poco honrados atraídos por la perspectiva de utilizar recursos de la compañía en su propio beneficio.

El principal método de fraude en auge es el ataque a centralitas*

EVALUACIÓN DE LA VULNERABILIDAD DE SU ORGANIZACIÓN

¿Utiliza las mismas contraseñas en su sistema durante más de un año?

¿Utilizan los usuarios la contraseña predeterminada para el buzón de voz?

¿Están conectados los módems al servidor de comunicación?

¿Tienen todos los usuarios acceso a prefijos internacionales?

¿Proporciona acceso a los servicios de telefonía a usuarios que se encuentran fuera de la compañía?

¿Ha habido recientemente cambios en el personal del equipo de administración de sistemas?

SI CONTESTA AFIRMATIVAMENTE A ALGUNA DE ESTAS PREGUNTAS EXISTE UN RIESGO POTENCIAL.

PROTECCIÓN DE LOS SISTEMAS DE COMUNICACIÓN

La aplicación de los mecanismos de protección y buenas prácticas de Alcatel-Lucent Enterprise contribuye a optimizar la configuración y seguridad de los sistemas y evita muchas situaciones de riesgo.

Tome las medidas de seguridad adecuadas

- Restricción selectiva de llamadas salientes: restrinja las llamadas externas fuera del horario de trabajo, establezca contraseñas para llamadas a larga distancia y prohíba las llamadas a números de tarificación especial.
- Revise las normas relativas a las contraseñas: cambiar las contraseñas predefinidas y continuar cambiándolas regularmente (por ejemplo, mensualmente).
- Implemente la protección para transferencia y desvío de llamadas al exterior.
- Revise las responsabilidades y permisos de administración.
- Actualice la base de datos del sistema eliminando la información de usuarios anteriores.

Refuerce la concienciación sobre el problema en la compañía

- Informe a sus empleados sobre prácticas de seguridad básicas e impactos derivados de su incumplimiento (riesgos legales y económicos), así como de sus obligaciones y responsabilidades.
- Recuerde a los empleados algunas normas de confidencialidad de sentido común, como no proporcionar nunca datos técnicos sobre los sistemas de información y comunicación a desconocidos (por ejemplo: códigos personales, nombres, Sistemas de Respuesta Interactiva de Voz (IVR) con números de acceso directo a los buzones de voz).
- Realice campañas informativas sobre el fraude telefónico: anime a los empleados a informar de cualquier incidencia o actividad inusual del servicio de telefonía, incluido algún mensaje extraño en el buzón de voz, líneas ocupadas por la mañana o registros de llamadas realizadas fuera de las horas de oficina.

Aproveche la experiencia de su Business Partner y Alcatel-Lucent Enterprise

- Mantenga actualizadas sus aplicaciones de software para beneficiarse de las últimas mejoras y evoluciones tecnológicas de los productos.
- Refuerce las soluciones implantando buenas prácticas de seguridad.
- Aplique los parches de seguridad del proveedor.
- Evalúe regularmente la vulnerabilidad del sistema ante los diferentes métodos de fraude telefónico.

* Fuente: Communications Fraud Control Association, Informe 2013

Alcatel·Lucent Enterprise