Ataques de Ingeniería Social y COVID-19

Los criminales cibernéticos están aprovechando el brote del coronavirus para explotar el eslabón más débil de la seguridad cibernética: el elemento humano. Aon Cyber Solutions ofrece algunos consejos para ayudar a las empresas a mantenerse seguras ante esta nueva amenaza.

A medida que evoluciona la pandemia del COVID-19, ha surgido una nueva área de riesgo cibernético y, como siempre, los atacantes cibernéticos buscan cada oportunidad para aprovechar la situación.

El brote de coronavirus ha creado un cambio inesperado en la forma en que normalmente hacemos negocios. El autoaislamiento, las políticas de trabajo remoto desde el hogar y las limitaciones impuestas sobre las reuniones presenciales han creado una dependencia más fuerte de lo normal en canales virtuales y electrónicos. Además, los empleados también hacen uso de esos canales para obtener información, asesoramiento y obtener soluciones a los desafíos prácticos a los que se enfrentan constantemente.

Si bien la mayoría de las empresas cuentan con mejores prácticas y planes de continuidad de negocio, estos a menudo se centran en los sistemas claves del negocio, procesos y entornos de trabajo, y frecuentemente suponen una interrupción relativamente limitada, ya sea en términos de duración de la interrupción, la geografía o el sistema. Las empresas no deben pasar por alto que los atacantes cibernéticos aprovechan activamente la psicología humana para engañar a las personas de forma que estas les faciliten el robo de información confidencial, dinero y acceso a sistemas privados.

Sabemos, debido a nuestra vasta experiencia manteniendo a las organizaciones seguras y respondiendo a grandes acontecimientos cibernéticos y violaciones de datos, que la mayoría de los incidentes de seguridad tienen un elemento humano –ya sea por un simple error, un error honesto o por negligencia. Sin embargo, también sabemos que un pequeño error humano podría ocasionar pérdidas y daños dolorosos a un negocio y a su reputación. Los siguientes son algunos ejemplos a tener en cuenta a medida que el brote de coronavirus continúa evolucionando.

Anejos maliciosos y “malware”:

- Los anejos, enlaces maliciosos y cómo detectarlos son parte de cada programa de capacitación en seguridad cibernética, pero esa capacitación normalmente se lleva a cabo en un entorno controlado. Los empleados preparados, al recibir estas amenazas, generalmente elegirán la acción correcta y, ¡no harán ‘click’ al archivo adjunto! Sin embargo, hemos visto numerosos informes sobre "campañas salubristas" que han difundido correos electrónicos con archivos maliciosos pretendiendo ser fuentes oficiales con orientación e información sobre el coronavirus. Organizaciones como la Organización Mundial de la Salud (OMS) han emitido advertencias sobre delincuentes que se hacen pasar por la OMS para llevar a cabo ataques y estafas. Los delincuentes cibernéticos también están explotando la necesidad de información de las personas sobre el coronavirus contando con que la velocidad y la frecuencia con la que las personas desean información les induzca a hacer cosas que no harían en otro tipo escenario.
- Los empleados buscan y esperan este tipo de información de parte de su empleador y podrían confiar en las comunicaciones que parezcan auténticas y que aparentan brindar información que desean escuchar. Imagine que un atacante envía un correo electrónico a sus empleados titulado, 'La oficina cerrará por dos semanas, vea el documento adjunto para más detalles' o 'Como resultado del COVID-19, todos los viajes de negocios están cancelados - aquí un enlace a nuestro sitio de reservaciones de viajes para hacer cambios". Fuera de un entorno de oficina controlado, y conteniendo información que la gente está desesperada por obtener, se podrían cometer errores.

Descubra cómo nuestras soluciones de ciberseguridad pueden ayudarle.

Visite:
aon.com/cyber-solutions
o llame al **787.754.8787**.

AON
Empower Results®

Robo de identidad por “phishing”, “vishing” y “smishing”:

- Estos ataques son intentos hechos a través de correos electrónicos (“phishing”), llamadas de voz (“vishing”) o SMS (“smishing”) por un actor malicioso para obtener las credenciales de un individuo u otra información confidencial. Muchos actores maliciosos se aprovecharán del COVID-19 al tratar de engañar a los empleados a dar sus credenciales, convenciéndolos de que están brindando información requerida por su empresa. Los atacantes buscarán información de código abierto (“open-source”) sobre las empresas y sobre empleados particulares para identificar vulnerabilidades que puedan explotar, tales como: información de la empresa, los roles de las personas, y así adivinar las direcciones de correo electrónico con precisión.
- Un atacante podría hacerse pasar por un proveedor externo de confianza como, por ejemplo, un socio de viajes del cual se espera el negocio se apoye durante este momento crítico. También podrían pretender proporcionar un servicio que la empresa necesita para su Plan de Continuidad de Negocio; una llamada maliciosa podría ocultarse entre la ola de solicitudes promocionales que los empleados bien podrían recibir como parte de sus funciones. De igual manera, los empleados pueden recibir un mensaje de texto SMS de alguien que dice ser de IT, validando que todos los empleados tienen acceso VPN. De tener éxito, el atacante podría obtener acceso a información confidencial o credenciales, y posiblemente, tener acceso a su red y sistemas críticos.

Trabajo remoto y trabajo desde casa:

- Estos ataques son intentos hechos a través de correos electrónicos (“phishing”), llamadas de voz (“vishing”) o SMS (“smishing”) por un actor malicioso para obtener las credenciales de un individuo u otra información confidencial. Muchos actores maliciosos se aprovecharán del COVID-19 al tratar de engañar a los empleados a dar sus credenciales, convenciéndolos de que están brindando información requerida por su empresa. Los atacantes buscarán información de código abierto (“open-source”) sobre las empresas y sobre empleados particulares para identificar vulnerabilidades que puedan explotar, tales como: información de la empresa, los roles de las personas, y así adivinar las direcciones de correo electrónico con precisión.
- Los empleados dependerán de la voz, texto u otros canales alternos como las redes sociales, que no son familiares en este contexto, permitiendo una mayor posibilidad de ingeniería social y estafas por robo de identidad. Incluso, podrían buscar soluciones alternas a las mejores prácticas y políticas de IT, como conectarse a las redes corporativas desde dispositivos personales o usar dispositivos corporativos en casa que contienen grandes cantidades de información personal y de negocios, al buscar información sobre el coronavirus. El alto costo social de "trabajar desde casa" puede llevar a los empleados a conectarse a redes inalámbricas nuevas y potencialmente inseguras desde sus hogares, cafeterías, o desde la calle, en cantidades proporcionalmente mayores a las que las empresas se hayan encontrado antes. El Servicio de Asistencia de IT también estaría bajo presión para suavizar políticas y los empleados que trabajan desde casa podrían pedir que se les suavicen las restricciones como, por ejemplo, permitirles el uso de dispositivos USB para imprimir documentos en una imprenta cercana. Es fácil imaginar que la presión de trabajar desde casa podría resultar en tal compromiso, eliminando controles que previamente habrían sido efectivos.

La preparación es clave, y una buena resistencia cibernética incluye mantener a sus empleados informados sobre las últimas tendencias en amenazas.

Usted puede ayudar a sus empleados a reconocer los escenarios emergentes con los que podrían encontrase en las próximas semanas y meses, y debe continuar enviando el mensaje de que deben tratar con precaución las comunicaciones de los remitentes que no reconocen, ni abrir enlaces, ni ingresar credenciales o abrir archivos o anejos de un remitente no confiable.

En momentos de mayor estrés empresarial y tecnológico, recomendamos a las empresas a que revisen sus ciberdefensas y mantengan a su personal informado de las amenazas en evolución para que sean menos propensos a ser víctimas de otro ataque de robo de identidad por “phishing”, “trickbot” o por secuestro de datos (“ransomware trojan”).

Sobre Cyber Solution: Las soluciones cibernéticas de Aon ofrecen una gestión holística del riesgo cibernético, habilidades de investigación sin igual y tecnologías patentadas para ayudar a los clientes a descubrir y cuantificar los riesgos cibernéticos, proteger los activos críticos y recuperarse de incidentes cibernéticos.

Sobre Aon: Aon plc (NYSE: AON) es una empresa líder mundial de servicios profesionales que ofrece una amplia gama de soluciones de riesgo, retiro y salud. Nuestros 50,000 colegas en 120 países potencian los resultados para los clientes mediante el uso de datos y análisis patentado, para brindar información que reduzca la volatilidad y mejore el rendimiento.

Empower Results®