DIEZ AMENAZAS DE CIBERSEGURIDAD QUE LAS EMPRESAS DEBEN INTEGRAR EN SUS SISTEMAS DE COMPLIANCE

22 de julio de 2021

Bonatti Compliance destaca que las empresas deben fomentar acciones de formación y concienciación que se adapten a un entorno de riesgo que cambia a gran velocidad.

La irrupción de la pandemia provocada por el Covid-19 y las intensas medidas de restricción social derivadas, han empujado a casi todas las empresas hacia modelos de teletrabajo que, en muchas ocasiones, no estaban planificados previamente. Este cambio forzado ha facilitado un extraordinario incremento de la ciberdelincuencia, que ha sabido aprovechar que millones de empleados de todo tipo de empresas y Administraciones Públicas se han visto obligados a seguir trabajando desde su hogar sin disponer todavía de los conocimientos o medios tecnológicos más adecuados para este cambio de modelo.

"*La extraordinaria amenaza que supone la ciberdelincuencia ha puesto en valor los Sistemas de Compliance de las empresas, como la herramienta más adecuada para formar y concienciar al personal sobre estas graves amenazas, impulsando así comportamientos mucho más seguros en contextos de teletrabajo. Sin embargo, la amenaza no deja de crecer, y en este bienio 2020-2021 los ciberataques no sólo han crecido en número, sino también en su variedad y calidad, buscando explotar todas las rendijas que les ofrecen las empresas, sus empleados y directivos",* explica Francisco Bonatti, socio director de Bonatti Compliance, que señala que conocer el riesgo es la mejor forma de afrontarlo y ofrece cinco amenazas que deben combatir las compañías desde sus Sistemas de Compliance:

1. **Ramsomware**: el secuestro de información mediante malware que encripta el contenido de unidades, discos duros y servidores se ha convertido en uno de los riesgos estrella. La mejora de los algoritmos de encriptación y el recurso a los criptoactivos como medio de pago que evita el rastreo posterior son alicientes adicionales para los cibercriminales.

2. **Estafas del CEO**: la suplantación de la identidad de los directivos para engañar a los empleados que tienen las claves y códigos para realizar transferencias bancarias se ha incrementado exponencialmente con la pandemia.

3. **Ataques a servidores y bases de datos**: los delincuentes explotan brechas de seguridad para acceder a los servidores y sustraer los datos que contienen. Los datos son el petróleo del siglo XXI y es uno de los grandes tesoros que poseen las empresas.

4. **Ataques Botnet:** los equipos y servidores de empresa son convertidos en zombies a través de Botnets, que gestionan los cibercriminales para evitar ser rastreados, eludir las listas de SPAM o para realizar transferencias económicas ilícitas, envíos masivos de correos o ataques DDoS.

5. **Sustracción de las credenciales**: el acceso a las credenciales y contraseñas de los empleados y directivos facilita a los cibercriminales un amplio abanico de delitos a costa de la empresa: desde el acceso a los fondos depositados en las cuentas bancarias hasta el robo de secretos de empresa, el acceso a la intimidad de los empleados y directivos, a las cámaras de seguridad o la sustracción de bases de datos.

En este escenario, Francisco Bonatti, socio director de Bonatti Compliance, reflexiona sobre cinco debilidades que debemos proteger a través del Compliance:

1. **Ingeniería social**: todavía hoy un número ingente de ataques informáticos se producen porque las empresas, empleados o directivos se dejan engañar y voluntariamente envían los datos, abren enlaces o ejecutan las acciones pretendidas por los cibercriminales. La ingeniería social es una actividad delictiva muy depurada, imprescindible, por ejemplo, para ejecutar la estafa del CEO y se debe combatir desde Compliance con sólidas acciones de formación y concienciación del personal, ayudándoles a que nunca 'bajen la guardia'.

2. **Debilidades internas**: los delincuentes aprovechan en muchas ocasiones las propias debilidades, derivadas de usos inadecuados de los equipos por los empleados, que acaban infectados por error, negligencia o ignorancia; o bien, por comportamientos maliciosos de empleados desleales o insatisfechos. El análisis de riesgos y la implantación de protocolos y procedimientos de usos tecnológicos consistentes debe reforzarse con medidas para asegurar su eficaz aplicación por todos los empleados.

3. **Uso de equipos personales y teletrabajo desde el hogar:** una de las debilidades estrella de la pandemia procede del uso de equipos personales compartidos con el resto de la familia, que pueden desvirtuar todas las medidas de protección empresarial si los padres, hijos o pareja hacen un uso inadecuado del mismo equipo. El propio espacio familiar, como entorno de trabajo, puede ofrecer mucha información a ciberdelincuentes para diseñar ataques de ingeniería social, al igual que ocurre con la información que pueden obtener de las redes sociales (RRSS), una vez han identificado el hogar del empleado o directivo y al resto de su familia.

4. **Phishing**: en 2020 se ha multiplicado el volumen y la complejidad de los ataques de phishing para distribuir botnets y malware de todo tipo, robar credenciales o acceder a las cámaras y micrófonos de los equipos. Las técnicas se han sofisticado, aprovechando fenómenos coyunturales como el incremento del uso de los correos electrónicos durante la pandemia o saltándose los mecanismos de protección a través de nuevos canales de phishing como son el SMS (smishing) o el uso de PDF infectados que, inconscientemente, relacionamos con una actividad empresarial. Junto con las medidas de ciberseguridad más adecuadas,

nuevamente Compliance debe aportar procesos y procedimientos de conducta adecuados y acciones de formación y concienciación dinámicas, que se adapten a un entorno de riesgo que cambia a gran velocidad.

5. **Deepfakes**: no puede faltar una de las grandes novedades que comienza a ofrecer usos ilícitos. Se trata de técnicas de edición de vídeo que sustituyen a una persona por otra mediante la inteligencia artificial alcanzando resultados altamente realistas, que ofrecen a los cibercriminales nuevos recursos para sofisticar sus procesos de hackeo social o quebrantar contraseñas biométricas.

Fuente: www.elderecho.com