ENTHEC

qondar

Ciberseguridad Individual para Personas Relevantes.

Su vulnerabilidad es un riesgo corporativo

qondar

Índice

PAG.

INTRODUCCIÓN

En el entorno digital, la protección de la información se ha convertido en una prioridad crítica para las organizaciones. Las estrategias de ciberseguridad corporativa se diseñan pensando en asegurar los datos y sistemas de la organización y en evitar las brechas de seguridad que puedan propiciar un ataque que los ponga en riesgo.

Sin embargo, en su mayoría, las estrategias de ciberseguridad corporativas dejan fuera la protección de datos y activos digitales personales de las personas con capacidad de decisión y actuación dentro de la organización.

Los C-Levels, directivos, socios y VIPs de una empresa manejan información altamente confidencial y tienen capacidad total de actuación corporativa. Si se ve comprometidas, las consecuencias pueden ser devastadoras tanto para el individuo como para la organización.

La información personal sensible incluye datos como números de identificación, detalles financieros, información de contacto y otros datos privados que pueden ser utilizados para realizar fraudes, extorsiones o ataques dirigidos. Con esta información personal, un ciberatacante puede acceder a esa información confidencial o capacidad de actuación dentro de la organización.
Por eso, protección de esta información es esencial no solo para salvaguardar la privacidad e integridad de los individuos, sino también para mantener la seguridad y la reputación de la organización.

INTRODUCCIÓN

En un entorno donde las ciberamenazas son cada vez más sofisticadas, es imperativo que las organizaciones implementen medidas robustas de seguridad para proteger a sus líderes y figuras clave.

En este documento exploramos las diversas amenazas que afectan a los activos personales digitales de los altos ejecutivos y figuras clave dentro de una organización, así como la importancia de protegerlos. Además, descubrimos las estrategias más efectivas para controlar y mitigar los riesgos asociados a este tipo de información.

Suplantación

Los datos personales de C-Levels y personas relevantes de la organización pueden servir para suplantarlos y llevar a cabo en su nombre acciones que perjudiquen a la reputación o a las finanzas corporativas.

Chantaje y extorsión

La información personal confidencial de C-Levels, socios y VIPs de una organización puede ser utilizada por los ciberdelincuentes como moneda de cambio con la que llevar a cabo chantajes y extorsiones para no poner en peligro la reputación personal del afectado, pero, también, la de la organización al que está ligado y a la que representa.

Amenazas emergentes

La irrupción de las nuevas tecnologías ha propiciado nuevas soluciones de ciberseguridad pero, también técnicas de ciberataque más sofisticadas difíciles de sortear.

Ataques como el fraude del CEO basan su éxito en la utilización de información personal de cargos ejecutivos de las organizaciones para mimetizar su estilo de comunicación, comprender su entorno e, incluso, tomar el control de sus cuentas profesionales para llevar a cabo el engaño.

qondar

PERSONAS RELEVANTES:

PERFILES E INFORMACIÓN SENSIBLE

Los C-Levels, directivos, socios y VIPs son figuras clave dentro de cualquier organización. Ocupan posiciones de liderazgo y toma de decisiones y su influencia y responsabilidad son fundamentales para el éxito de la empresa.

PERSONAS RELEVANTES

PERFILES

Dentro de una organización encontramos diferentes perfiles relevantes que tienen en común la capacidad de tomar decisiones y llevar a cabo acciones vinculantes y de ejercer la representación de esta.

C-LEVELS

Incluyen posiciones como CEO (Chief Executive Officer), CFO (Chief Financial Officer), COO (Chief Operating Officer), CTO (Chief Technology Officer), entre otros. Estos ejecutivos son responsables de la dirección estratégica y operativa de la organización.

DIRECTIVOS

Incluyen gerentes de alto nivel y directores de departamentos que supervisan áreas específicas de la empresa, como marketing, recursos humanos, ventas, etc.

SOCIOS

En algunas organizaciones, especialmente en firmas de consultoría, bufetes de abogados y empresas de capital riesgo, los socios son propietarios parciales de la empresa y tienen un papel activo en la gestión y toma de decisiones.

VIPs

Incluye a clientes importantes, inversores, miembros del consejo de administración y otras figuras influyentes que tienen un impacto significativo en la organización.

qondar

PERSONAS RELEVANTES:

RIESGOS Y AMENAZAS DE LA INFORMACIÓN PERSONAL SENSIBLE

La información personal sensible se refiere a datos que, si se divulgan sin autorización, pueden causar daño o perjuicio a la persona a la que pertenecen. Cuando esa persona ocupa un cargo relevante dentro de una organización, la pérdida de esos datos puede también afectar gravemente a la seguridad corporativa.

RIESGOS ASOCIADOS A LA FALTA DE PROTECCIÓN

Robo de identidad:

Los ciberdelincuentes utilizan información personal para hacerse pasar por la víctima y cometer fraudes o ejecutar técnicas de ingeniería social que perjudiquen a la organización.

Extorsión:

La información sensible se utiliza para extorsionar a los individuos, amenazando con divulgar datos comprometedores, entre los que pueden encontrarse información confidencial de la organización.

Daños a la reputación:

La amenaza que supone la utilización fraudulenta de información personal sensible para la reputación personal del alto directivo es también una amenaza para la reputación de la organización a la que representa y en cuyo nombre actúa.

Consecuencias legales:

Las organizaciones enfrentan gastos y sanciones legales derivadas del uso fraudulento de los datos personales sensibles de alguno de sus C-Levels o VIPs.

AMENAZAS

Phishing:

Los atacantes envían correos electrónicos fraudulentos que parecen provenir de fuentes confiables para engañar a los ejecutivos y obtener información confidencial o credenciales de acceso.

Spear phishing:

Una forma más dirigida de phishing, donde los atacantes personalizan los correos electrónicos para hacerlos más convincentes y específicos para la víctima.

Whaling:

Spear phishing que se dirige a los altos ejecutivos (las “ballenas”) con el objetivo de obtener acceso a información valiosa o realizar transferencias de dinero fraudulentas.

Ataques de ingeniería social:

Los atacantes manipulan a los individuos para que divulguen información confidencial o realicen acciones que comprometan la seguridad de la organización, como la descarga inconsciente de malware.

DATOS:

El 70% de empresas y organizaciones en España ha sido objeto de ataques BEC.

*Proofpoint: State of the Phish 2024

La incidencia de ataques relacionados con phishing, el fraude y la estafa subió tres puntos porcentuales en 2023 respecto al año anterior, representando la mayor subida entre las diferentes amenazas.

*Identity Theft Resource Center (ITRC): 2023 Business Impact Report

PERSONAS RELEVANTES
VULNERABILIDADES EN LA PROTECCIÓN DE DATOS

DATOS:

Un 33% de los ataques y vulneraciones a organizaciones están relacionados con datos en la sombra fuera del control corporativo.

*Ponemon Institute & IBM: Cost of a Data Breach Report 2024

Contraseñas débiles:

El uso de contraseñas fáciles de adivinar o la reutilización de contraseñas en múltiples cuentas facilitan el acceso no autorizado.

Falta de actualizaciones de seguridad:

No mantener los sistemas y software actualizados con los últimos parches de seguridad deja puertas abiertas para los atacantes.

Acceso no controlado:

La falta de controles adecuados sobre quién tiene acceso a qué información puede derivar en la exposición de datos sensibles.

Dispositivos no seguros:

El uso de dispositivos personales no seguros para acceder a información corporativa aumenta el riesgo de brechas de seguridad.

Falta de concienciación:

La falta de formación y concienciación sobre ciberamenazas entre altos los ejecutivos conduce a errores humanos que comprometan la seguridad.

Falta de conocimiento de la información expuesta:

La web, deep web, dark web, las redes sociales y los foros están llenos de datos en la sombra filtrados y expuestos a causa de brechas de seguridad que han escapado del control corporativo.

PERSONAS RELEVANTES:

EL FRAUDE DEL CEO

Es uno de los fraudes de ingeniería social más efectivos y extendidos de los últimos años. Implica a los altos ejecutivos, utilizando su información personal sensible interceptada, y lleva aparejadas importantes pérdidas financieras para las organizaciones.

DATOS:

El 68% de las brechas de seguridad corporativas están relacionadas con un factor humano no malicioso, como ser víctima de un engaño.

*Verizon 2024 Data Breach Investigations Report (DBRI)

En 2021, el Centro de Denuncias de Delitos en Internet (IC3) recibió denuncias relacionadas con BEC con pérdidas reclamadas que superaron los 2.4 mil millones de dólares. Estos fraudes se detectaron en empresas y organizaciones grandes y pequeñas en todos los estados de EEUU y en más de 150 países de todo el mundo.

*FBI 2022 Congressional Report on BEC and Real Estate Wire Fraud

PERSONAS RELEVANTES

EL FRAUDE DEL CEO

Técnica de ingeniería social en la que los atacantes se hacen pasar por altos ejecutivos de una empresa para engañar a los empleados y obtener información confidencial o transferencias de dinero.

El FBI llama a este tipo de estafa **Business Email Compromise (BEC)** y lo define como "una estafa sofisticada dirigida a empresas que trabajan con proveedores extranjeros y/o empresas que realizan pagos mediante transferencias bancarias con regularidad. La estafa se lleva a cabo comprometiendo cuentas de correo electrónico corporativas legítimas mediante ingeniería social o técnicas de intrusión informática para realizar transferencias de fondos no autorizadas".

CASOS:

FACC (2016)

La empresa austríaca Fischer Advanced Composite Components AG (FACC) perdió alrededor de 42 millones de euros por transferencia debido a un fraude del CEO.

Mattel (2015)

La famosa empresa de juguetes fue víctima de un fraude del CEO en el que los atacantes lograron transferir 3 millones de dólares a una cuenta bancaria en China.

Cáritas Luxemburgo (2024)

Todavía bajo investigación, el hundimiento financiero de Cáritas Luxemburgo debido a las transferencias, a lo largo de cinco meses, de 61 millones de euros a 14 cuentas bancarias diferentes se achaca a un fraude del CEO que consiguió engañar a la directora financiera de la organización.

Grupo Farmacéutico Zendal (2020)

En España, inmersos en la pandemia, el director financiero del grupo transfirió 9 millones de euros siguiendo la supuesta orden urgente y confidencial del CEO de la compañía, cuyo correo electrónico había sido intervenido por un ciberdelincuente.

qondar

PERSONAS RELEVANTES:

IMPACTO DE LA UTILIZACIÓN FRAUDULENTA DE DATOS PERSONALES SENSIBLES

DATOS: Los ataques tipo BEC causaron a las empresas de EEUU pérdidas por valor de 3.000 millones de dólares.

*FBI Internet Crime Report 2022

qondar

DAÑO A LA REPUTACIÓN

El daño a la reputación es una consecuencia indirecta, pero grave, de la utilización fraudulenta de datos personales sensibles de altos ejecutivos.

Junto con su reputación personal, según sea el delito cometido, también puede quedar dañada la reputación corporativa. Además, con frecuencia, se produce una pérdida de confianza en las estrategias de seguridad de la organización, que se asocia a la de su directivo. De esta forma, la confianza de los clientes, inversores y socios comerciales se ve afectada.

La cobertura mediática negativa y la difusión en redes sociales amplifican el impacto, haciendo que la recuperación de la reputación sea un proceso largo y costoso.
Para los C-Levels, directivos y VIPs, la exposición de su información personal tiene repercusiones personales y profesionales que pueden ser duraderas.

PÉRDIDAS FINANCIERAS

Son las más directas y graves, ya que el objetivo mayoritario de los ataques es el enriquecimiento ilícito del ciberdelincuente.

La utilización fraudulenta de datos personales de un alto ejecutivo puede tener consecuencias desastrosas para su patrimonio personal, pero, también, para los recursos financieros de la organización, ya que, en la mayoría de los ataques, el objetivo último son los fondos de la compañía que dirige o representa.

Un ejemplo de esto son las cuantiosas pérdidas de fondos corporativos que el fraude del CEO ha provocado y sigue provocando en todo el mundo.

IMPLICACIONES LEGALES Y REGULATORIAS

Las empresas están sujetas a una variedad de leyes y regulaciones que protegen la información personal y sensible.

Una brecha de seguridad provocada por una deficiente protección de la información personal de altos ejecutivos que filtre datos custodiados por la organización implica el incumplimiento de estas normativas, lo que conduce a sanciones legales y regulatorias.

Además, la suplantación de identidad puede hacer que los ejecutivos y VIPs y la organización se enfrenten a demandas de responsabilidades que conlleven un costoso proceso legal para demostrar el delito de suplantación.

PERSONAS RELEVANTES

IMPACTO DE LA UTILIZACIÓN FRAUDULENTA DE DATOS PERSONALES SENSIBLES

qondar

PERSONAS RELEVANTES:

ESTRATEGIAS DE PROTECCIÓN DIGITAL

- POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD
- TECNOLOGÍAS Y HERRAMIENTAS TRADICIONALES DE PROTECCIÓN
- FORMACIÓN Y CONCIENCIACIÓN DEL PERSONAL
- IA Y NUEVAS TECNOLOGÍAS

PERSONAS RELEVANTES

ESTRATEGIAS TRADICIONALES

POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

Establecer políticas y procedimientos de seguridad claros y bien definidos es fundamental para proteger la información sensible. Estas políticas deben incluir directrices sobre la información personal sensible de los altos cargos, incluyendo la de su uso personal fuera de la organización. Incluyendo el acceso a la información, la gestión de contraseñas, el uso de dispositivos personales y la respuesta a incidentes de seguridad. Es esencial que estas políticas sean revisadas y actualizadas regularmente para adaptarse a las nuevas amenazas y tecnologías emergentes. Además, es crucial que todos los empleados, especialmente los C-Levels y directivos, comprendan y sigan estas políticas.

TECNOLOGÍAS Y HERRAMIENTAS TRADICIONALES DE PROTECCIÓN

La implementación de tecnologías y herramientas avanzadas de protección es esencial para salvaguardar la información sensible. Esto incluye el uso de cifrado para proteger los datos en tránsito y en reposo, la implementación de firewalls y sistemas de detección de intrusiones y el uso de soluciones de autenticación multifactor para asegurar el acceso a los sistemas. Además, es importante utilizar software de gestión de dispositivos móviles (MDM) para proteger los dispositivos personales y corporativos que acceden a la información sensible.

FORMACIÓN Y CONCIENCIACIÓN DEL PERSONAL

La formación y concienciación del personal es una de las estrategias más efectivas para prevenir brechas de seguridad. Los empleados deben recibir formación regular sobre las mejores prácticas de seguridad, las amenazas comunes y cómo identificar y reportar actividades sospechosas. Es especialmente importante que los C-Levels, directivos y VIPs comprendan los riesgos específicos a los que están expuestos y las medidas que deben tomar para proteger su información personal. La creación de una cultura de seguridad dentro de la empresa contribuye a garantizar que todos los empleados tomen en serio la protección de su información personal sensible.

PERSONAS RELEVANTES

ESTRATEGIAS EVOLUCIONADAS

DATOS:

El ahorro medio de costes para las organizaciones que utilizan de manera amplia la IA y la automatización de seguridad en la prevención de ciberataques es de 2,22$.

*Ponemon Institute & IBM: Cost of a Data Breach Report 2024

IA Y NUEVAS TECNOLOGÍAS

La IA junto con el aprendizaje automático pueden analizar grandes volúmenes de datos en tiempo real para detectar patrones y anomalías que podrían indicar una brecha de seguridad. Por ejemplo, los algoritmos de aprendizaje automático son capaces de identificar comportamientos inusuales en el acceso a datos, lo que permite a las empresas tomar medidas preventivas antes de que ocurra un incidente. Además, la IA ayuda a clasificar y etiquetar datos sensibles, asegurando que se apliquen sobre ellos las políticas de seguridad adecuadas.

La automatización de procesos de seguridad reduce la intervención humana, minimizando el riesgo de errores y aumentando la eficiencia. Los sistemas automatizados pueden gestionar tareas como la actualización de software, la aplicación de parches de seguridad y la monitorización continua de redes y sistemas. Esto es especialmente importante para proteger los datos de altos ejecutivos, que a menudo son objetivos de ataques dirigidos.

Utilizando IA y aprendizaje automático, las empresas pueden predecir y prevenir amenazas antes de que ocurran. Los modelos predictivos pueden identificar vulnerabilidades y recomendar acciones para fortalecer la seguridad.

qondar

PERSONAS RELEVANTES:

RECOMENDACIONES Y MEJORES PRÁCTICAS

RECOMENDACIONES

Evaluación de riesgos:

Realizar una evaluación exhaustiva de riesgos para identificar las vulnerabilidades y amenazas específicas a la información personal sensible. Incluye la revisión de políticas, procedimientos y tecnologías actuales.

Autenticación de doble factor:

Adoptar la autenticación multifactor (MFA) para todos los accesos a sistemas y datos sensibles. MFA añade una capa adicional de seguridad al requerir múltiples formas de verificación.

Cifrado de datos:

Utilizar cifrado robusto para proteger los datos tanto en tránsito como en reposo. Esto asegura que la información sensible esté protegida incluso si es interceptada.

Actualizaciones y parcheo:

Mantener todos los sistemas y software actualizados con los últimos parches de seguridad para proteger contra vulnerabilidades conocidas.

Localización y monitorización de brechas:

Utilizar soluciones de monitoreo y detección de amenazas para identificar y responder rápidamente a cualquier actividad sospechosa o no autorizada.

DATOS: Los ciberataques que utilizaron credenciales robadas o comprometidas aumentaron un 71% interanual.

*IBM X-Force Threat Intelligence Index 2024

MEJORES PRÁCTICAS

Cultura de ciberseguridad:

Fomentar una cultura de seguridad dentro de la organización donde todos los empleados, desde el nivel más bajo hasta los C-Levels, comprendan la importancia de proteger la información sensible, incluyendo la suya personal, y sigan las mejores prácticas de seguridad.

Formación continua:

Proporcionar formación continua en ciberseguridad para todos los empleados, con un enfoque especial en los riesgos y amenazas específicos a los que están expuestos los C-Levels y directivos.

Políticas de seguridad claras:

Establecer y comunicar políticas de seguridad claras y comprensibles que aborden la protección de la información personal. Estas políticas deben ser revisadas y actualizadas regularmente.

Gestión de accesos:

Implementar una gestión de accesos estricta que asegure que solo el personal autorizado tenga acceso a la información sensible. Utilizar el principio de privilegio mínimo para limitar el acceso a los datos.

Simulacros de incidentes:

Realizar simulacros de incidentes de seguridad y ataques tipo el fraude del CEO para preparar a la organización para responder eficazmente.

PERSONAS RELEVANTES

RECOMENDACIONES Y MEJORES PRÁCTICAS DE PROTECCIÓN DIGITAL

PERSONAS RELEVANTES:

IMPORTANCIA DE LA MONITORIZACIÓN CONTINUA DE AMENAZAS

La monitorización continua y automatizada de amenazas se ha convertido en la estrategia de ciberseguridad corporativa proactiva esencial para contrarrestar con éxito la creciente sofisticación de los ciberataques. Entre los muchos activos que protege, está la información personal sensible de los altos ejecutivos de las empresas.

VENTAJAS DE LA MONITORIZACIÓN CONTINUA DE AMENAZAS

Detección temprana de amenazas

La monitorización continua y automatizada permite la detección temprana de amenazas, lo que es esencial para prevenir ataques antes de que causen daños significativos. Respecto a los datos personales sensibles de los altos ejecutivos, la monitorización continua en la red, las redes sociales, foros, la deep web y la dark web permite detectar en tiempo real filtraciones y exposiciones de esos datos para neutralizar el riesgo.

Reducción de riesgos

Los altos ejecutivos tienen y manejan información crítica que, si se ve comprometida, puede tener consecuencias devastadoras para la empresa. La monitorización continua y automatizada de filtraciones y exposiciones de datos personales sensibles ayuda a identificar y mitigar estos riesgos al proporcionar una visión en tiempo real de las amenazas potenciales.

Cumplimiento normativo

Las regulaciones de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos, exigen que las empresas implementen medidas adecuadas para proteger la información personal en poder de las organizaciones. La monitorización continua permite neutralizar la utilización fraudulenta de los datos personales sensibles filtrados de altos ejecutivos que pueden poner en peligro la custodia de esa información protegida.

Protección contra ataques dirigidos

Los altos ejecutivos son a menudo el objetivo de ataques dirigidos, como el spear phishing y el whaling. La monitorización continua y automatizada de las conversaciones en redes sociales y foros, así como de las diferentes webs, permite detectar la preparación de ataques dirigidos, para neutralizarlos antes de que sean ejecutados.

Mejora de la respuesta a incidentes

La capacidad de responder rápidamente a un incidente de seguridad es crucial para minimizar el impacto de una brecha de datos personales sensibles de altos ejecutivos. La monitorización continua y automatizada proporciona la información necesaria para una respuesta rápida y efectiva, permitiendo a las empresas contener y remediar las amenazas de manera más eficiente.

Visibilidad y control

La monitorización continua ofrece una visibilidad completa del estado de protección de la empresa y la efectividad de su estrategia de ciberseguridad, lo que permite un control más efectivo sobre los datos sensibles. Esto es especialmente importante para los altos ejecutivos, ya que su información personal y profesional debe estar protegida en todo momento. La visibilidad en tiempo real permite a las empresas identificar y abordar vulnerabilidades antes de que sean explotadas por los atacantes.

qondar

Qondar Personal Watchbots es la plataforma desarrollada por Enthec que proporciona a las personas información en tiempo real sobre su identidad, datos personales y activos digitales y las actividades en curso relacionadas con ellos, para que puedan controlar su seguridad online.

Qondar proporciona información relacionada con la persona protegida sobre:

- Móvil: Personal y profesional
- Email: Personal y profesional
- Tarjeta de crédito
- Cuenta bancaria
- Wallet: Bitcoin, Ethereum
- Documentación: DNI, pasaporte, carnet de conducir, tarjeta sanitaria

FUNCIONALIDADES

- Búsqueda de Bizum, WhatsApp, Teléfono móvil en leaks.
- Búsqueda de email en leaks / cuentas de Paypal en venta.
- Búsqueda de la tarjeta de crédito en leaks.
- Búsqueda del wallet.
- Búsqueda de la cuenta bancaria.
- Rastreo de documentación personal.

BENEFICIOS PARA LA PERSONA PROTEGIDA

- Protección del patrimonio personal
- Protección de las comunicaciones personales y profesionales
- Protección de la reputación
- Protección frente a amenazas activas que impliquen riesgos personales o patrimoniales
- Protección frente a la suplantación de identidad digital

BENEFICIOS PARA LA ORGANIZACIÓN

- Protección frente al fraude del CEO, BEC y técnicas de ingeniería social.
- Protección de la información confidencial y sensible corporativa.
- Protección de las operaciones corporativas de alto nivel
- Protección financiera.

ENTHEC

#WeAlreadyKnow

ENTHEC©

@enthec

@enthecsolutions

qondar