Separados por un mismo lenguaje

¿Puede la alta dirección descifrar y actuar ante la amenaza real de los ciberataques?

kaspersky

Contenido

Introducción

"El lenguaje es muy poderoso. El lenguaje no sólo describe la realidad. El lenguaje crea la realidad que describe" Arzobispo Desmond Tutu

El lenguaje es importante.

El lenguaje ha permitido el estudio de la filosofía antigua, los avances científicos, la programación y, por supuesto, enviar mensajes de WhatsApp a amigos y familiares. Y, en la misma medida en que el lenguaje transmite e interviene en la sociedad creando culturas, historias, mitos y formas de arte, entre otros muchos, también la ciberseguridad tiene el suyo propio.

Los eventos de ciberseguridad ocurren todos los días, con amenazas que toman diferentes formas y tamaños y que hablan una gran variedad de idiomas, no sólo geográficos, sino también tecnológicos. Los foros de Internet, los medios y los nuevos canales en todo el mundo se hacen eco de los últimos ataques que, ya sea de forma verbal o escrita, mezclan una serie de acrónimos, jerga y modismos actuando como abreviatura para los que saben, pero que pueden parecer desconcertantes y difíciles de interpretar para personas sin experiencia en el sector.

Los términos "deep web" (web profunda) y "dark web" (web oscura) se usan de forma indistinta y nos evocan una serie de imágenes de pandilleros que se reúnen para comprar números de tarjetas de crédito, drogas, armas, dinero falsificado y cuentas pirateadas.

La realidad es que son cosas diferentes. La "deep web" se refiere a cualquier cosa que no esté indexada en Internet y, por lo tanto, no es accesible a través de buscadores como Google.

La "dark web" es un subapartado de la "deep web" que ha sido "escondido" de forma intencionada y requiere de un navegador especial. Existen razones legítimas para que la gente desee que determinada información no esté disponible y no esté indexada. Por ejemplo, juega un papel importante en el hacktivismo por los derechos humanos, periodistas etc., que pueden hablar libremente cuando no pueden hacerlo en sus países. Sin embargo, esto también se utiliza para actividades ilegales.

Dada la naturaleza esotérica de las transacciones ilegales que se producen, es imposible interpretarlas y entenderlas sin conocer el idioma del cibercrimen. Malware, denegación de servicio, botnets, troyanos, estafas de phishing y registradores de pulsaciones de teclas son términos muy utilizados, pero ¿qué son realmente? ¿Cuánto necesito saber para proteger mi negocio?

Al tiempo que el mundo continúa rediseñando sus prácticas de negocio en medio de la agitación política, medioambiental y económica, la inteligencia sobre las amenazas de ciberseguridad nunca ha sido tan crítica para las empresas. La realidad de un mundo cada vez más digitalizado hace que cada decisión y transacción de negocio implique hoy una dimensión relacionada con la ciberseguridad.

Las prioridades han pasado de los cortafuegos y la gestión de identidades a desafíos estratégicos como la confianza en la marca, la seguridad del producto y la resiliencia.

Kaspersky es una compañía global con expertos en inteligencia de amenazas en todas las regiones. La empresa ha utilizado esta experiencia única para llevar a cabo una exhaustiva investigación sobre cómo los altos directivos que se enfrentan al desafío de proteger sus empresas interpretan la naturaleza evolutiva de las amenazas de ciberseguridad.

¿Se están enfocando y discutiendo las amenazas correctas en los consejos? ¿Han invertido en las herramientas adecuadas para protegerse de esas amenazas? ¿Son conscientes de las amenazas que conllevan mayor peligro?

Nuestros hallazgos revelan que la cúpula directiva es consciente de la frecuencia con la que sus negocios están siendo atacados, pero el lenguaje y la terminología que se utiliza para describir las amenazas de ciberseguridad son simplemente demasiado opacos para que los interpreten. Esto significa que el directivo a menudo se encuentra en una posición en la que tiene que tomar decisiones críticas sin una imagen clara del panorama de amenazas y de los riesgos que representan para su organización.

El siguiente informe destaca tanto avances significativos en la concienciación en materia de ciberseguridad como claras mejoras en otras áreas. Los hallazgos revelan que, si bien no hay escasez de información sobre el tema y la preocupación por parte de la cúpula es evidente, existe una clara falta de inteligencia disponible y procesable.

Metodología

Se realizaron un total de 1.800 entrevistas con altos directivos en grandes empresas de más de 1.000 empleados en 13 países en septiembre de 2022: Reino Unido (200), Francia (200), DACH (Alemania - 100, Austria - 50, Suiza - 50), Benelux (Países Bajos - 100, Bélgica - 100), España (200), Portugal (200), Italia (200), Rumanía (200) y Grecia (200). Se preguntó a los encuestados sobre la ciberseguridad dentro de su organización, las medidas que toman para protegerse y las barreras que enfrentan como equipo directivo.

Se denominan como "altos directivos" a los directores ejecutivos, los directores de operaciones, los directores de marketing, los directores de riesgos, los directores de inversiones, los directores financieros, los directores de cumplimiento y los directores de información.

Principales hallazgos

Los altos ejecutivos saben que los ciberataques representan la mayor amenaza para su empresas, pero cuanto mayor es la compañía, menos importancia cobran:

- Desde la perspectiva de la alta dirección, el mayor riesgo al que se enfrentan son los ciberataques (49%), seguido de factores económicos -inflación, tasas de interés, etc. - (37%).
- Teniendo esto en cuenta, algo más de la mitad (51%) afirman que la ciberseguridad está ahora en la agenda de la alta dirección, con un 43% que admite que solo "a veces" está en la lista.
- Cuanto más grande es la compañía, menos consciente es de las ciberamenazas, con solo un 35% de las empresas de +5.000 empleados que admiten que conocen estos ataques; comparado con el 52% de las empresas de entre 1.000 y 1.999 empleados.

Aunque la ciberseguridad es una clara preocupación para la cúpula, el lenguaje utilizado para describir amenazas impacta en su habilidad para entenderlas y actuar en consecuencia:

- A pesar de que la ciberseguridad es una clara preocupación, los especialistas en seguridad encuestados (48%) afirman que la **jerga de seguridad y la terminología del sector son la principal barrera para el equipo de dirección a la hora de entender la ciberseguridad y cómo abordarla.**
- El 38% de los ejecutivos encuestados encuentran confusos términos básicos de seguridad como **Malware, Phishing y Ransomware**.
- Las restricciones presupuestarias (47%) y la falta de formación (43%) completan las mayores barreras a las que se enfrentan para entender la ciberseguridad.

Aunque hay algunas diferencias geográficas, los altos ejecutivos todavía confían en las redes sociales, blogs y noticias para recopilar inteligencia:

- En su afán por ampliar conocimientos, casi la mitad (47%) de la alta dirección afirma que depende de las redes sociales, blogs de ciberseguridad y noticias disponibles públicamente para recopilar inteligencia sobre las tendencias de seguridad para su discusión.
- De todos los países, **fue en España donde el 34% admitió que era más probable que recurriera a la dark web para recopilar inteligencia de seguridad**.

Sí, la ciberseguridad es uno de nuestros mayores problemas... sólo que a menudo no es un tema prioritario en la sala de juntas.

Durante los últimos 12 meses, la ciberseguridad ha seguido dominando los titulares, con ataques de alto perfil que resultan en una pérdida de dinero, impacto en la reputación y vulnerabilidades. Por lo tanto, no debería sorprender que nuestra investigación encuentre que **casi todos los altos ejecutivos entrevistados (99%) son ahora conscientes de cuán a menudo sus negocios son atacados.**

De esos encuestados, el 52% de los altos ejecutivos en empresas de 1.000 a 1.999 empleados afirmaron que eran muy conscientes de la frecuencia con la que su empresa era atacada; mientras que solo el 35% en empresas de más de 5.000 admitió lo mismo. Además, casi la mitad (49%) admitió que los ciberataques son ahora la mayor amenaza para su negocio, muy por delante de los factores económicos como el aumento de la inflación (37%), la regulación y las normativas (35%) y competidores (29%).

A pesar de ser plenamente conscientes de la importancia de las ciberamenazas, el 43% afirmó que la ciberseguridad solo a veces era un tema de la agenda durante las juntas.

De ellos, 1 de cada 7 (14%) encuestados en empresas con más de 5.000 empleados afirmó que la ciberseguridad rara vez es un tema en sus reuniones con la dirección. Este porcentaje se reduce al 3% en empresas con 1.000-1.999 empleados o 2.000-2.999 empleados.

Estos datos resaltan que cuanto más grande es la organización, mayor es la desconexión potencial entre aquellos con conocimiento técnico y la junta, lo que sugiere un fracaso a la hora de articular los problemas de ciberseguridad en términos comerciales, de una manera que sea significativa para la dirección.

La cúpula directiva considera que la ciberseguridad es la mayor amenaza que enfrentan sus negocios, y casi la mitad lo considera un problema mayor que los factores económicos actuales, como el aumento de la inflación y el impacto que tiene en los costes. Sin embargo, cuanto más grande sea la organización, es menos probable que tengan un conocimiento profundo de los principales problemas de ciberseguridad y el impacto que pueden tener en el negocio, o que incluso se discutan regularmente en las juntas.

	UK	Francia	DACH	Benelux	España	Portugal	Italia	Rumanía	Grecia
Ataques a la ciberseguridad	57.0%	46.0%	61.0%	52.0%	45.5%	51.5%	44.0%	45.0%	43.0%
Factores Económicos	30.5%	37.0%	35.0%	44.0%	40.5%	33.0%	41.0%	45.5%	28.0%
Regulaciones/ Normativa	27.0%	36.0%	35.0%	35.5%	38.5%	35.0%	34.5%	37.0%	34.0%
Desastres naturales	26.0%	36.5%	29.0%	30.0%	40.5%	26.5%	31.0%	32.5%	26.0%
Competidores	30.5%	30.0%	26.5%	30.0%	31.5%	30.5%	28.0%	25.0%	31.0%
Cuestiones ambientales	26.0%	31.5%	25.0%	32.0%	37.0%	20.0%	29.5%	29.0%	28.0%
Reivindicaciones/ Acción social	29.5%	30.0%	29.0%	23.0%	27.5%	29.5%	26.00%	26.0%	34.0%

Fig 1. Mayores riesgos/amenazas a la continuidad del negocio

Es inevitable que cuanto mayor sea la presencia de la empresa en el mundo digital, más numerosos serán los vectores de ataque -por ejemplo, más personas y más sistemas que proteger-, por lo que muchas organizaciones tratan de adecuar el nivel de seguridad a su crecimiento.

Todas las empresas tienen prioridades que compiten entre sí en términos de contratación, captación de clientes, infraestructuras, etc., pero los resultados apuntan a una mayor desconexión dentro de las grandes organizaciones. Una desconexión que complica que la dirección sea consciente de la importancia de la seguridad, convirtiéndose en su mayor reto.

Entender las implicaciones de un ataque exitoso en las operaciones de negocio, el impacto financiero y cómo la reputación puede verse afectada ya no es una opción para los responsables en la toma de decisiones de alto nivel. Es preocupante ver que grandes organizaciones no aprecian la importancia de la ciberseguridad y de la inteligencia de amenazas para su negocio, lo que revela una desconexión entre los expertos TI y los ejecutivos que toman decisiones. Si bien la junta no necesita comprender los complejos entresijos de la ciberseguridad , debe comprender el impacto que las amenazas pueden tener en el negocio.

David Emm
Analista Principal de Seguridad. GReAT. Kaspersky

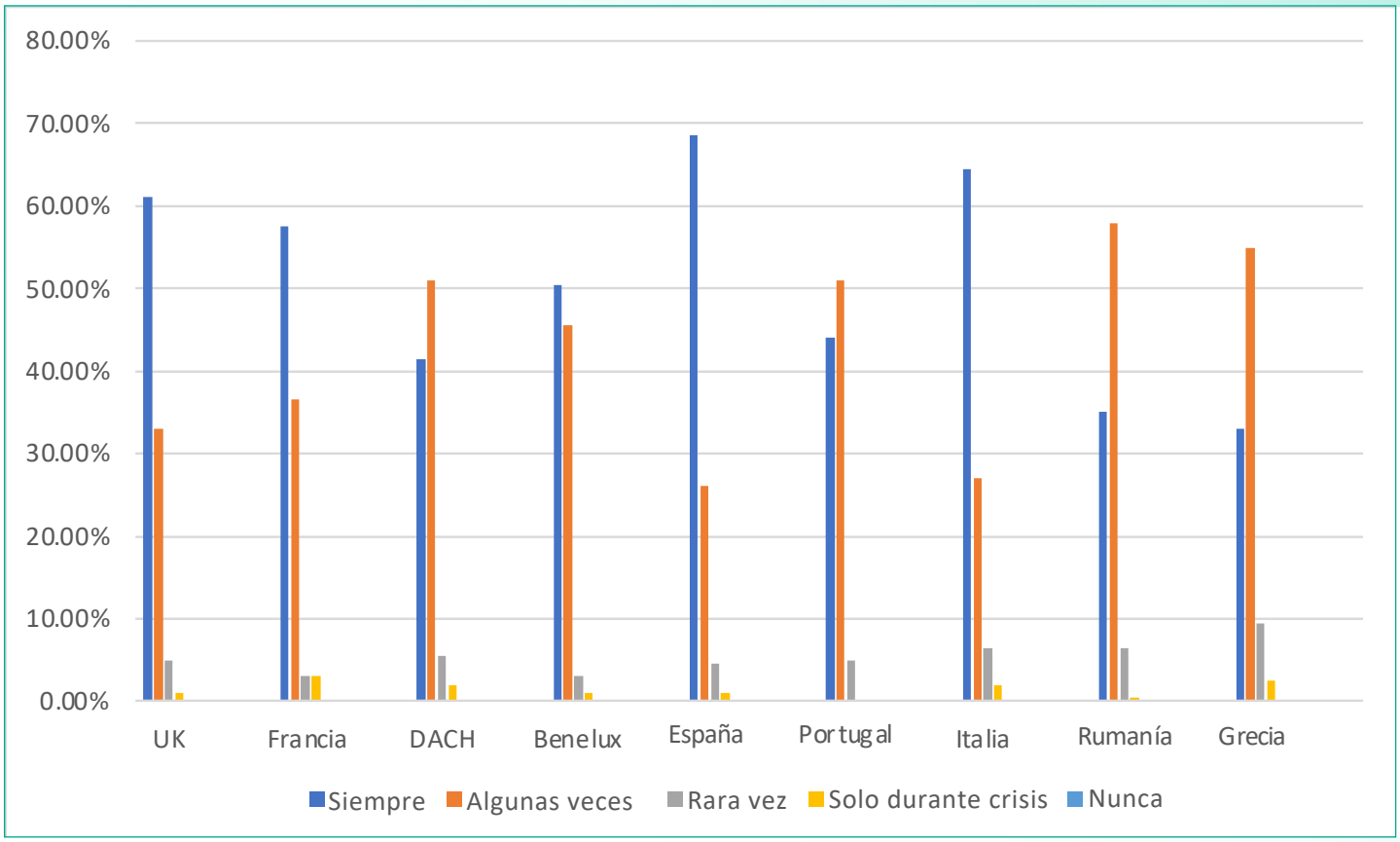

Fig. 2 ¿La ciberseguridad forma parte de la agenda de las reuniones?

El mayor obstáculo: no comprender el significado

A pesar de que la ciberseguridad es una clara preocupación para la alta dirección y sus negocios, casi la mitad (48%) de los especialistas en seguridad, normativa y riesgos cree que la jerga y los confusos términos de la industria representan actualmente la mayor barrera para el equipo de gestión a la hora de entender la ciberseguridad y, lo que es más importante, cómo actuar al respecto.

Esto es particularmente evidente en DACH -Alemania, Austria, Suiza- (47%), Portugal (47%), España (44%) y Reino Unido (42%) con especialistas en seguridad que afirman que la jerga es la principal barrera para que su equipo de gestión comprenda las amenazas de seguridad más apremiantes.

Tanto es así que **el 38% de todos los encuestados afirmaron que les resultan confusos los términos básicos de ciberseguridad como Malware, Phishing y Ransomware.** El lenguaje un poco más técnico, como 'Zero Day Exploits' y 'Reglas Suricata' generó niveles similares de confusión con el 39% de los encuestados que afirmaron no comprender completamente estos términos.

Entre todos los países, los ejecutivos encuestados en Italia tienen más probabilidades de encontrar confusos los términos Malware, Phishing y Ransomware (50%), confesando que estos términos no se entendían por completo. Los encuestados en Francia tenían más probabilidades (47%) de encontrar confuso el término “ataque al Estado-Nación”.

Globalmente, las restricciones presupuestarias (47%) y la falta de capacitación (43%) del equipo de gestión completan las tres principales barreras. De los países encuestados, fueron los ejecutivos en el Reino Unido (56%) y Francia (52%) quienes afirmaron que lo que más los frenaba era el presupuesto. Mientras que en Italia y DACH, el 42% afirmó que la razón era una formación insuficiente.

En pocas palabras, la investigación de Kaspersky revela que existen obstáculos significativos para que la alta dirección desarrolle una comprensión y concienciación más completas de los problemas de ciberseguridad más importantes que enfrentan sus negocios. Y es el lenguaje que se está utilizando para transmitir y mediar en estos problemas lo que actualmente limita la capacidad de una organización para desarrollar una cultura de ciberseguridad, compartir conocimientos y, en última instancia, incorporar inteligencia de amenazas.

Nuestros datos sugieren que la ciberseguridad, aunque puede diferir según la geografía, es una industria que tiene su propio lenguaje, un lenguaje que puede ser impenetrable para quienes no tienen experiencia en seguridad especializada. La concienciación y la comprensión llegarán, pero para que esto suceda se requiere un puente que una el léxico y los términos utilizados en ciberseguridad con la junta directiva.

De un vistazo

Malware	Término genérico para programas informáticos diseñados para instalarse en el ordenador de una persona e infligir daño de múltiples maneras. Es una contracción de "software malicioso". El malware común incluye virus, gusanos, troyanos, spyware, adware y ransomware.
Ataques de Phishing	El phishing es una forma de ingeniería social empleada tanto en la ciberdelincuencia como en ataques APT. Los objetivos son contactados por correo electrónico, teléfono o mensajería por alguien que se hace pasar por una institución legítima para comprometer un dispositivo y obtener acceso a datos sensibles. Estos datos también pueden utilizarse para el robo de identidad con fines fraudulentos.
Ataques Estado-Nación (APTs)	Ataques de gran envergadura dirigidos contra infraestructuras nacionales, con el fin de debilitar la esfera económica, militar o política de un país determinado.
Ransomware	Software malicioso que cifra los datos o bloquea su acceso, exigiendo al usuario que pague para desbloquearlos o descifrarlos.
Ataques a la cadena de suministro	Su objetivo son elementos de la cadena de suministro antes de la venta al usuario final. Un ejemplo es la modificación de una actualización de producto para que el malware llegue a todos clientes de ese producto.
Zero Day Exploit	Este término se utiliza para describir el código de explotación que se ha escrito para aprovechar una vulnerabilidad antes de que el proveedor de software la conozca y haya tenido la oportunidad de publicar un parche. El resultado es que los posibles atacantes son libres de explotar la vulnerabilidad, a menos que se hayan implementado tecnologías proactivas de prevención de exploits para defender el sistema/dispositivo objetivo del atacante.
Indicador de Compromiso (IoC)	Objeto o actividad detectada en una red o en un dispositivo que indica una alta probabilidad de acceso no autorizado al sistema; en otras palabras, que el sistema está comprometido. Estos indicadores se utilizan para detectar actividades maliciosas en sus primeras fases, así como para prevenir amenazas conocidas.
TTP	TTP son las siglas de tácticas, técnicas y procedimientos. Es el término utilizado por los profesionales de la ciberseguridad para describir los comportamientos, procesos, acciones y estrategias utilizados por un actor de amenazas para desarrollar amenazas y participar en ciberataques.
Mitre ATT&CK	Se trata de una base de conocimientos que describe las tácticas y técnicas de los ciberdelincuentes basándose en observaciones del mundo real. La MITRE Corporation creó la base de conocimientos en 2013 y el propósito del proyecto es desarrollar una matriz estructurada de técnicas cibercriminales para facilitar la respuesta a ciberincidentes.
Reglas Suricata	Las reglas Suricata son el método de facto para compartir y cotejar la información sobre amenazas con el tráfico de la red.
MD5	Este algoritmo convierte un conjunto de datos de tamaño arbitrario en un hash: una secuencia pseudoaleatoria de caracteres de longitud fija. El resultado es una especie de identificador del conjunto de datos cifrados. MD5 se utiliza para verificar la autenticidad, integridad e inmutabilidad de cualquier conjunto de caracteres (por ejemplo, código informático). Si las sumas de comprobación coinciden, significa que el archivo no ha sido modificado. Algunos sistemas operativos utilizan MD5 para almacenar contraseñas.
Yara	Herramienta utilizada principalmente en la investigación y detección de malware que proporciona un enfoque basado en reglas para crear descripciones de familias de malware basadas en patrones textuales o binarios

Glosario completo disponible en **https://encyclopedia.kaspersky.es/glossary/**

La comunicación no debería representar un obstáculo para la ciberseguridad. Lo que destaca nuestro estudio es la importancia de la planificación estratégica, la elaboración de presupuestos y la contratación de personal capacitado; pero también la necesidad de canalizar los incidentes relevantes de abajo hacia arriba de una manera comprensible y clara, sin la necesidad de recurrir a un lenguaje confuso o jerga compleja. Una comunicación bidireccional que funcione es esencial para una operación funcional a largo plazo.

Christian Funk
Director GReAT. Región DACH. Kaspersky

	UK	Francia	DACH	Benelux	España	Portugal	Italia	Rumanía	Grecia
Restricciones presupuestarias	56.5%	52.0%	46.5%	47.0%	47.5%	42.5%	42.5%	43.5%	45.5%
Falta de formación	43.0%	51.5%	42.0%	40.5%	55.0%	39.5%	42.0%	42.5%	31.5%
Jerga/ terminología confusa	42.0%	40.0%	46.5%	43.0%	44.0%	46.5%	41.0%	45.0%	31.5%
Falta de herramientas	35.0%	37.5%	40.5%	49.5%	45.5%	35.0%	44.5%	37.5%	47.0%
Falta de tiempo	37.5%	35.5%	28.0%	41.0%	42.0%	30.0%	40.0%	35.0%	46.0%
Ninguna barrera	0.5%	2.5%	2.0%	0.5%	1.5%	1.0%	8.0%	0.0%	0.0%

Fig 3. ¿Qué obstáculos encuentra, si es que encuentra alguno, para que su equipo directivo tenga un conocimiento completo y amplio de la ciberseguridad?

Entonces, ¿qué es un Malware?

Primero, es importante entender a qué se enfrentan las organizaciones.

Concebidas originalmente como un proyecto del Departamento de Defensa de EE. UU. a principios de la década de 1990 para desarrollar una red anónima y encriptada que protegería las comunicaciones confidenciales de los espías del país, las "dark webs" (webs oscuras) han seguido su propio camino desde entonces. Aunque presenta diferentes variaciones según su implementación técnica y sus respectivos "objetivos", se puede definir como una red altamente sofisticada y compleja de foros, salas de chat, servidores de archivos e imágenes y mercados.

Para personas que viven bajo regímenes opresivos que bloquean gran parte de Internet o castigan la disidencia política, es importante tener en cuenta que las "dark webs" son un salvavidas que brinda acceso a la información y protección contra la persecución.

Pero para la gran mayoría se utiliza para actividades despreciables. Su sofisticación y complejidad proporciona el entorno ideal para que los delincuentes prosperen, lejos de las miradas de las autoridades.

Las "redes oscuras" no tienen una indexación estándar de páginas por parte de los motores de búsqueda web, lo que significa que Google y otras herramientas de búsqueda no pueden descubrir ni mostrar resultados para esas páginas. Según el tipo de dark web, se pueden usar túneles de tráfico virtuales a través de una infraestructura de red aleatoria que hace que sea inaccesible por medios tradicionales. Para el usuario inexperto es una fortaleza impenetrable.

Con el fin de educarse y formarse contra las amenazas de la web oscura, la encuesta revela que casi la mitad (47%) de los altos ejecutivos depende principalmente de las noticias, los blogs de la industria y las redes sociales para recopilar información sobre temas de ciberseguridad. Este método es una forma importante de comprender las amenazas a las que se enfrentan las empresas; sin embargo, debe ser parte de un plan de educación y concienciación.

La información pública en blogs y en medios es una forma de mantenerse al día sobre las últimas problemáticas, pero la excesiva confianza en las informaciones o noticias más "populares" puede impedir una comprensión holística de las amenazas que se les presentan y cómo detenerlas.

Apenas el 40% de los encuestados afirmó que recurren a proveedores/expertos externos para recopilar información sobre las últimas amenazas que surgen de la dark web, y que prefieren desarrollar y ampliar sus conocimientos utilizando la información disponible públicamente. Si bien 2 de cada 5 (46%) altos ejecutivos encuestados utilizan fuentes privadas para recopilar inteligencia, y las analizan durante las reuniones de las juntas; otro 40% confía en los recursos internos para descifrar las amenazas emergentes y, posteriormente, presentar los hallazgos durante las reuniones.

De todos los países encuestados, los ejecutivos españoles admitieron en un 50% que es más probable que utilicen la inteligencia de amenazas de la web oscura. En el polo opuesto, los encuestados en el Reino Unido son los que menos utilizarían la dark web (34%).

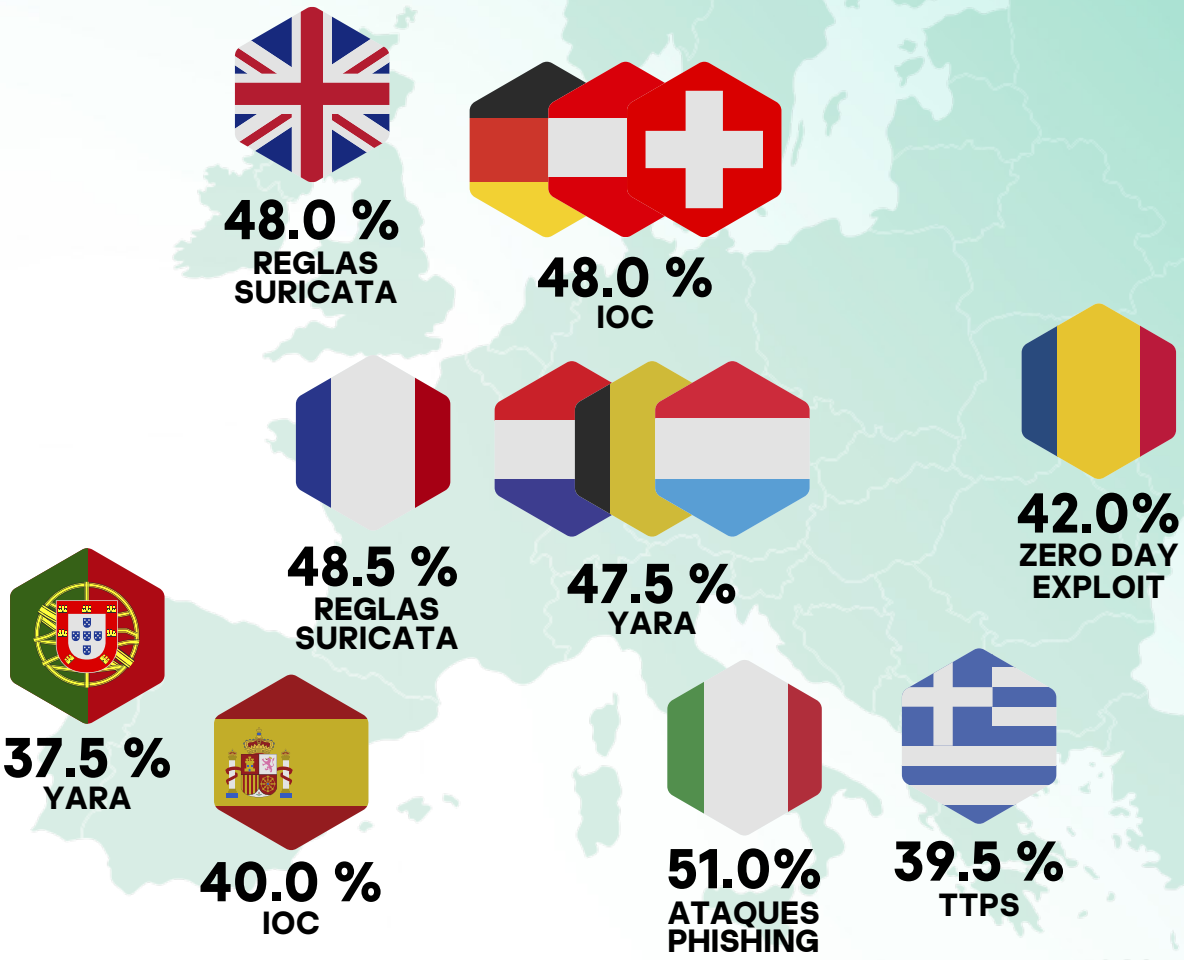

Fig 4. Porcentaje de términos que a los altos directivos les cuesta más entender

Ciberseguridad: ¿a quién vas a llamar?

La investigación revela que la alta dirección necesita ayuda para comprender las amenazas de seguridad que enfrentan sus negocios todos los días. El panorama de ciberamenazas es complejo y en constante evolución, con algunos de los criminales más motivados y tecnológicamente más sofisticados del planeta. Una cosa es estar al tanto de las ciberamenazas que existen y otra completamente distinta es comprenderlas.

A medida que ha evolucionado el panorama de las amenazas, también lo ha hecho el lenguaje que se utiliza. Como hemos visto en el estudio, esta evolución supera en muchos casos la capacidad de las empresas para mantenerse al día. Prioridades de negocio, competitividad, entornos económicos y sociales que cambian rápidamente no han eclipsado la realidad de la amenaza que representan los ciberataques. Pero, la incapacidad de comprender su naturaleza y, por ello, de actuar en consecuencia han hecho que la ciberseguridad no esté presente en la agenda de la alta dirección.

El consumo de recursos disponibles públicamente y la disponibilidad de más presupuesto para capacitación ayudarían a desarrollar esta conciencia. La realidad, sin embargo, es que sin una experiencia sólida para identificar, analizar y correlacionar ciberamenazas, las organizaciones solo se están preparando a medias. En el centro de este enfoque es necesario un partner que no solo pueda hablar el idioma de las amenazas, sino que también comprenda cómo la privacidad y el anonimato del que gozan los delincuentes se pueden usar en su contra para extraer inteligencia crítica.

Para obtener más información sobre cómo las empresas pueden protegerse contra las ciberamenazas, póngase en contacto con el equipo de **Kaspersky Threat Intelligence**.

Otros factores que afectan a la concienciación

- El 41% cree que la falta de herramientas disponibles es una barrera importante para tener una comprensión completa y amplia de la ciberseguridad y las amenazas.
- Según la cúpula directiva, los directores de TI son los más propensos a presentar información de inteligencia sobre amenazas durante sus reuniones (51%), seguidos de los CISO (45%), los proveedores externos de ciberseguridad (44%), los resúmenes ejecutivos escritos no técnicos (31%) y, por último, los partners (25%).
- Los encuestados que utilizan fuentes públicas de inteligencia (fuente abierta, redes sociales, blogs) son más propensos a afirmar que lo hacen más para evitar la interrupción del negocio (56%), que para eludir cuestiones de costes (53%) o porque es la fuente más fiable (22%).