AXA Research Fund

Desarrollo de resiliencia informática

Riesgos, activadores y previsión

Un conjunto de perspectivas del AXA Research Fund

Invierno de 2021

Acerca del AXA Research Fund

AXA Research Fund (fondo para la investigación del Grupo AXA) se creó en 2008 para el estudio de los principales riesgos que enfrenta nuestro planeta. A través de este, AXA ha dedicado un total de 250 M € a la investigación científica con fines filantrópicos y ha financiado 665 proyectos de investigación en áreas clave, como: riesgos para la salud, clima y el medio ambiente y problemas socioeconómicos. La misión filantrópica del AXA Research Fund es financiar y patrocinar investigaciones científicas con potencial transformador y facilitar la toma de decisiones informadas y basadas en la ciencia, tanto en el sector público como el privado, a través de actividades de difusión y divulgación.

www.axa-research.org

@AXAResearchFund

axaresearchfund@axa.com

Contenido

Introducción

Si bien el ciberespacio proporciona importantes oportunidades para la innovación, el progreso económico y el acceso a la información, también entraña nuevas vulnerabilidades. De hecho, el número de ciberataques crece año tras año, con operaciones cada vez más audaces: hemos pasado de la sustracción de datos personales a ataques contra infraestructuras críticas, como redes de distribución, reservas hídricas y hasta sistemas sanitarios. Los costos de los daños producidos por los delitos informáticos crecen a un ritmo vertiginoso. Los puntos vulnerables provienen del propio crecimiento de la interconectividad entre todo lo que nos rodea, lo que facilita ataques con objetivos muy diversos, que los hacen difíciles de combatir. Por ello, la ciberseguridad se ha convertido en un problema para todo el mundo.

El delito informático se ha establecido firmemente como una sofisticada industria oculta, y una evidencia de ello es la oferta de "ransomware-como-servicio".[1] Además, se da la circunstancia de que algunas criptomonedas puedan estar fomentando la circulación furtiva de dinero proveniente del pago de rescates de ataques informáticos. Todo ello es parte de la guerra cibernética librada con el amparo de algunos Estados. Además del anonimato de los perpetradores, la falta de rastro de la cadena de mando, las influencias y la prefinanciación necesaria en algunos casos, plantea la cuestión de si ciertos ataques podrían considerarse como actos de guerra.

Los riesgos informáticos están entre los más acuciantes y más rápidamente cambiantes para la sociedad y las aseguradoras. Plantean retos en materia de seguros por su sistematicidad, que socava los principios de agrupación y diversificación inherentes al negocio de los seguros. Además, como empresas de gran escala a nivel global, las aseguradoras pueden ser en sí mismas un objetivo principal de la ciberdelincuencia.

El Reporte sobre Riesgos Emergentes de AXA en 2021 deja ver que, para los expertos, los riesgos informáticos ocupan el segundo lugar de la lista, inmediatamente detrás del cambio climático.[2] En este contexto, una mejor comprensión y estimación de los riesgos informáticos es crucial para poder elaborar estrategias informadas que consideren la interconectividad de nuestros sistemas y las posibles consecuencias derivadas de un ciberataque. Tales estrategias deberán aunar la prevención con la resiliencia ante los posibles daños.

En el presente informe, el AXA Research Fund reúne conocimientos y experiencia de naturaleza académica, comercial y organizacional para arrojar luz sobre la cambiante dinámica del panorama informático y para contribuir a la comprensión y mitigación de los riesgos asociados, con el objetivo de proteger lo que importa.

Marie Bogataj

Directora de AXA Research Fund y Group Foresight de AXA.

Renaud Guidée

Director de Riesgos de Grupo de AXA.

[1] The Destructive Rise of Ransomware-As-a-Service [El auge destructor del "ransomware-como-servicio"], Barbara Kay, Forbes, 9 de junio de 2021.

[2] 2021 AXA Future Risk Report [AXA 2021: Informe sobre Riesgos Futuros], AXA, septiembre de 2021.

Resumen

Desde el comienzo de la crisis generada por la COVID-19, ha habido un notable incremento de ciberataques, estafas de phishing y actividades maliciosas dirigidas a infraestructuras críticas, gobiernos, organizaciones y hasta usuarios finales. En los primeros meses de 2020, las estadísticas referentes a ciberataques aumentaron drásticamente, registrando una ola de 300 % en la ciberdelincuencia en los Estados Unidos[1], y de 600 %[2] en correos electrónicos maliciosos en todo el mundo, incluido un aumento de 70 %[3] en filtraciones y robos de datos en el sector sanitario, con respecto al año anterior.

La crisis en el sector sanitario ha ocasionado cambios de hábitos en muchos aspectos de nuestras vidas, que persistirán por largo tiempo tras finalizar la pandemia: la adopción del trabajo remoto como un hecho habitual y un aumento de las transacciones online en casi cada ámbito de la vida cotidiana, incluidas las actividades de compras y bancarias, así como de las consultas médicas… Todo esto genera más oportunidades para la gran variedad de posibilidades de ciberataques, en una medida mucho mayor que la existente hasta ahora. Al mismo tiempo, se han sofisticado aún más los ataques digitales al aumentar la complejidad del entorno en que se desarrollan estas amenazas.

Las empresas y organizaciones se ven obligadas a hacer frente simultáneamente a una variedad de situaciones de alerta, detección de vulnerabilidades, aplicación de medidas de seguridad en una diversidad de sistemas y puntos terminales, y a evaluar con la mayor exactitud y en tiempo real los datos referentes a posibles amenazas. Dada la complejidad de estas tareas, empresas y organizaciones están cambiando su posición en materia de seguridad, de una actitud defensiva a un enfoque más realista y resiliente.

La resiliencia informática requiere de una activa monitorización y de la implementación anticipada de sistemas de defensa para poder hacer frente a la variedad de riesgos, amenazas y vulnerabilidades. Una estrategia resiliente en materia informática permite a la organización protegerse contra riesgos informáticos y asegurar su supervivencia y su continuidad ante cualquier ataque. Es un enfoque que se basa en la investigación y en la elaboración de técnicas de defensa novedosas, pero también en la colaboración entre las empresas y organizaciones, e incluso entre los gobiernos, donde la reglamentación desempeña un papel fundamental.

Como uno de los tres riesgos principales a nivel global que señalaba el Reporte sobre Riesgos Emergentes de AXA en 2021,[4] los riesgos informáticos exigen una buena preparación previa para poder combatirlos. Es un terreno plagado de retos, ya que la escasez de datos de naturaleza histórica, el perfil de las amenazas en constante evolución y tanto la interrelación como la complejidad de las situaciones informáticas requieren de nuevas estrategias, técnicas y medidas para mitigar los riesgos.

En esta publicación, el AXA Research Fund ha reunido trabajos de 20 expertos provenientes de medios académicos, gubernamentales y de organizaciones

[1] FBI Official Warns of Increasing Cybercrime Attacks Related to Coronavirus-Relief Efforts [El FBI advierte sobre el incremento de ataques informáticos relacionados con los esfuerzos para combatir el coronavirus], The Washington Times, abril de 2020.

[2] The Latest: UN Warns Cybercrime on Rise During Pandemic [Últimos datos: Las Naciones Unidas advierten sobre el incremento de delitos informáticos durante la pandemia], The Associated Press, ABC News, mayo de 2020.

[3] 2020 Data Breach Investigations Report [Informe de investigación sobre filtraciones de datos en 2020], Verizon, 2020.

[4] 2021 AXA Future Risk Report [AXA 2021: Reporte sobre Riesgos Emergentes], AXA, septiembre de 2021.

internacionales; así como del sector de seguros para proporcionar información sobre la cuestión fundamental del diseño y creación de la resiliencia informática necesaria.

Datos claves

En el mundo digital, la privacidad muchas veces parece estar reñida con la seguridad y la rendición de cuentas, pero no tiene por qué ser así.

Las actividades maliciosas en el ciberespacio se combaten con soluciones de Inteligencia Artificial (IA), que muchas veces son invasivas y arriesgan valores sociales importantes que las tecnologías informáticas deberían respetar. Pero los métodos experimentales para probar la autenticidad personal terminan por desarrollar, a la larga, procedimientos digitales anónimos pero seguros que permiten comprobar sin duda alguna la presencia de personas reales sin necesidad de identificarlas. Tales procedimientos garantizan formas de identificación sólidas y seguras con medios puramente digitales manteniendo el anonimato de la persona física, de modo que se conserven tanto la privacidad como la seguridad.

Si bien el desarrollo de nuevas tecnologías ofrece mayores oportunidades para los ciberataques, por otra parte, surgen nuevas técnicas de gestión de riesgos informáticos, tanto a partir de los sistemas tradicionales como de las propias nuevas tecnologías.

Los riesgos informáticos son más evidentes en el caso de los sistemas de infraestructuras críticas, donde se refleja más claramente el impacto del mundo digital sobre el físico. En esta área, la resiliencia frente a los riesgos informáticos depende de las técnicas de "resiliencia por diseño" que consideran de forma integral, a la vez que la operatividad del sistema, la posibilidad de que suceda algún ataque, frente a lo cual se preparan líneas de defensa, opciones flexibles de recursos o bien la desconexión temporal automática de la red, de modo que esta pueda continuar proporcionando los servicios básicos en caso de un ataque.

Además de las técnicas físicas generadoras de resiliencia, **se están desarrollando los nuevos campos de aprendizaje de máquina y de análisis de riesgos "bajo ataque", para generar sistemas de aprendizaje automático robustos frente a ataques maliciosos**. La creación de mecanismos de defensa más sólidos basados en la anticipación, el conocimiento de la estrategia del atacante y la asimetría en la información asequible al atacante y al defensor están en la base de este enfoque orientado a lograr una mayor resiliencia.

La virtualización de la nube ofrece más oportunidades de ataques en comparación con los sistemas de propiedad privada, ya que se dispone de una mayor "superficie de ataque" que en los sistemas restringidos a la sede del cliente, ya sea en relación con las propias máquinas, el proveedor del servicio o el propio usuario. **Esta situación ha dado pie al desarrollo de estrategias de adaptación como "Zero Trust"**, mediante la creación de espacios separados por barreras de seguridad (como los firewalls) entre el servidor de la aplicación y el servidor de la base de datos, o bien **varios niveles o capas de seguridad digital**, o **principios como el de "privilegio mínimo"** aplicables a los procesos, que proporcionan acceso restringido según reglas o niveles de seguridad precisos.

Respecto a la llegada de la computación cuántica y los problemas de seguridad que podría plantear, tanto la criptografía postcuántica –esto es, el diseño de nuevos

protocolos basados en problemas que sean de difícil resolución, también para un ordenador cuántico– **como la "seguridad física cuántica"** –el diseño de protocolos de criptografía cuántica cuya seguridad esté basada directamente en las leyes de la física cuántica– **proporcionarán formas de asegurar la criptografía: en pocas palabras, se utilizará la tecnología cuántica como protección contra la piratería cuántica**.

El desarrollo de la resiliencia informática implica reevaluar los procesos dentro de las organizaciones para originar un ecosistema informático integral compuesto por las empresas, los organismos reguladores y los gobiernos mismos.

A medida que aumenta la complejidad y la profesionalidad de las empresas, se hace necesario afrontar los problemas de seguridad desde **una estrategia holística basada en las personas, la tecnología y los procesos**. Respecto a las personas, la formación y el conocimiento de los empleados de las empresas son fundamentales en la búsqueda de un equilibrio entre la seguridad y las prioridades del negocio. La tecnología es un requisito básico para los mecanismos de defensa, mediante procedimientos y normas que permitan anticipar tanto el malware "tradicional" como formas de ataque más novedosas, aprovechando las innovaciones como las que aporta la inteligencia artificial. Por último, la aplicación de procedimientos adecuados implica la elaboración de planes que permitan reaccionar y recuperarse de cualquier ataque tan pronto como sea posible.

Más allá de cada organización en particular, se oye el clamor por fortalecer las "colaboraciones en todo el ecosistema" y compartir la información referente a los ciberataques. La confidencialidad, la preocupación por la propia reputación y las diferencias entre niveles de desarrollo informático han impedido muchas veces que las empresas compartieran información esencial sobre ataques informáticos; no obstante, es necesario comunicar información de inteligencia crucial respecto a los modos en que se hace frente a los problemas, así como los éxitos y los fracasos resultantes.

Junto a la anticipación y la colaboración por parte de las empresas, **la reglamentación tiene un papel clave en la resiliencia y la defensa frente a los ciberataques**, y los organismos reguladores están implementando medidas al respecto, especialmente desde la entrada en vigor del Reglamento General de Protección de Datos (RGPD) de la Comunidad Europea. Casi en todas partes, lo que al principio eran incentivos y sugerencias han terminado convirtiéndose en medidas obligatorias, por ejemplo respecto a la notificación de incidentes y en los casos de filtraciones o pérdidas de datos. **Los gobiernos y organismos internacionales están cada vez más de acuerdo en mejorar las estrategias de resiliencia informática a nivel global, y en reconocer que** el cibererspacio debe ser regulado dentro de un marco global vinculante no solo para las administraciones públicas sino también para el sector privado. **La gestión de los riesgos informáticos requiere de la actuación conjunta y coordinada de las organizaciones multinacionales, los organismos regulatorios, las agencias estatales y las empresas y corporaciones**.

Los seguros en materia informática dependen del desarrollo de las partes involucradas y de la capacidad de moldear, de la forma más exacta posible, potenciales situaciones informáticas.

A pesar del progresivo incremento de los riesgos informáticos y del reconocimiento de este problema como asunto de importancia tanto por parte de los expertos como del público en general, el número de gobiernos y de empresas que suscriben seguros en materia informática es todavía relativamente bajo en todo el mundo. Como resultado, **la mayoría de las pérdidas causadas por delitos informáticos no están protegidas hoy en día por ningún seguro. No obstante, la demanda está creciendo, por lo que se hace necesario acelerar la preparación del sector de seguros en cuanto a la cobertura informática con el desarrollo de las transformaciones apropiadas para afrontar los retos que presenta la cobertura de los riesgos informáticos**.

Los riesgos informáticos son un reto para el sector de los seguros en muchos sentidos. Los datos referentes a situaciones informáticas son demasiado escasos como para poder reconocer patrones que permitan asignar precios a los productos, la modelización de acumulaciones en materia informática se halla todavía en una etapa inmadura, y las amenazas informáticas están en constante evolución, con impactos considerables y pérdidas muy serias. Los seguros sobre riesgos informáticos dependen de la capacidad de modelizar los ciberataques de forma tal que sus complejos efectos puedan integrarse respecto a los eventos de los que dependen. Como respuesta a este problema, se han desarrollado recientemente nuevos modelos alternativos capaces de captar los efectos multiplicadores de los eventos informáticos junto con sus interacciones.

Pero para alcanzar un mayor desarrollo, el sector de los seguros necesita superar los escasos conocimientos y la poca experiencia actualmente existente sobre los riesgos informáticos y la correspondiente suscripción de pólizas, incluyendo el innovador terreno de los vehículos autónomos, cuyos datos todavía se basan en modelos no conectados. También debe haber un mayor conocimiento en materia de riesgos informáticos por parte de otros actores claves, como agentes y corredores de seguros.

La previsión estratégica y la ciencia ficción pueden ser una ayuda para una mejor comprensión de las amenazas futuras.

La incertidumbre y la complejidad de los riesgos informáticos revelan las limitaciones de la previsión tradicional y también de los instrumentos de modelización, dado que su forma de proyección del futuro es una simple continuidad lógica del presente. En cambio, la ciencia ficción puede servir como herramienta de previsión estratégica para anticipar amenazas futuras a partir de ideas que no se hallan presentes en los marcos de pensamiento habituales, y ayudar a prepararse ante posibles situaciones futuras con conciencia de las mismas.

Ante la evolución de las necesidades organizacionales y los frecuentes cambios en las amenazas potenciales, podemos definir la resiliencia en materia informática como la anticipación y la preparación, con un refinamiento continuo, mediante la innovación en la modelización, la investigación de estrategias de respuesta ante posibles amenazas, el desarrollo de nuevas capacidades dentro del sector de seguros en materia informática, y el soporte y respaldo mediante técnicas de previsión estratégica.

Capítulo 01

Seguridad y privacidad: ¿conceptos aliados o rivales?

Nuestra creciente dependencia de la tecnología nos hace más vulnerables a las amenazas en materia informática, como la suplantación de identidad o el uso fraudulento del correo electrónico. Las soluciones a estos riesgos generan técnicas que con frecuencia pueden ser invasivas y comprometer nuestra privacidad. ¿Son la seguridad y la privacidad objetivos contrapuestos? ¿Podemos lograr un equilibrio entre esta doble utilización de las tecnologías informáticas? ¿Cómo podemos afrontar el impacto social de las medidas de seguridad en materia informática?

La espada de doble filo de la ciberseguridad

J. Peter Burgess

J. Peter Burgess es profesor de filosofía y ciencias políticas, y director de la cátedra AXA de Geopolítica de Riesgos en la École Normale Supérieure de París. Sus investigaciones tratan de las relaciones entre cultura, política y tecnología, en especial los temas relacionados con el riesgo y la incertidumbre. Es autor de Terror y desengaño: la seguridad tras lo impensable [Terror and Disenchantment: Security after the Unthinkable], de próxima publicación.

> “Las medidas de ciberseguridad, por una parte, suponen un riesgo para los valores sociales más avanzados y, por otra parte, los amenazan directamente.”

En enero de 1961, Dwight D. Eisenhower, presidente de los Estados Unidos, en su alocución al público norteamericano al finalizar su mandato, advirtió de lo que sería un importante interrogante del momento: la apariciónes del "complejo industrial militar". La idea, simple pero impactante, la sugiere la observación de Eisenhower de que la ya poderosa industria armamentística, derivada de la privatización e industrialización de la seguridad, tenía un mayor interés financiero en la guerra que en la paz.

Si bien esta situación sigue vigente hoy día, su conceptualización más reciente es la de la duplicidad inherente a toda tecnología de la capacidad de servir para el bien o para el mal, dependiendo del uso que se haga de ella. Así, por ejemplo, las tecnologías derivadas de la energía nuclear pueden satisfacer las necesidades energéticas de una población o bien aniquilarla, los motores propulsores de los cohetes son útiles para lanzar satélites de comunicación, pero también para esparcir gas nervioso, y el GPS puede guiarnos a un hospital en un momento crítico o conducir una bomba inteligente hasta su objetivo.

Setenta años después del discurso de Eisenhower, la relevancia de las tecnologías de seguridad en el seno de la sociedad acentúa e intensifica esta realidad. De hecho, la dualidad de las posibilidades de uso, en el sentido de su potencial para hacer el bien o el mal, destaca en forma especial en el caso de las tecnologías referentes a la seguridad. Las tecnologías informáticas son un ejemplo particularmente importante de este interrogante en materia de seguridad en el seno de la sociedad. Los inmensos beneficios sociales de las tecnologías informáticas en conjunción con la notable vulnerabilidad de los sistemas informáticos, y el elevado rendimiento económico del sector informático y computacional, plantean un dilema especialmente difícil, por la duplicidad de sus posibilidades de uso.

Un buen ejemplo de este dilema en materia de ciberseguridad es el ataque informático que sufrió el gasoducto de la Colonial Pipeline en Norteamérica en mayo de 2021. El ataque efectuado mediante tecnología informática desactivó un sistema regional de distribución de petróleo controlado por ordenadores. Cuando se cerró una de las redes principales de conducción de combustible, el gobierno federal de los Estados Unidos declaró el estado de emergencia, poniendo en operación medidas que entran en conflicto con algunos valores fundamentales de la sociedad norteamericana, como la privacidad, la dignidad, la fiabilidad, el derecho de asistencia y la solidaridad.

El reto principal al tratar el impacto social de las medidas de ciberseguridad es la dualidad del uso de las tecnologías informáticas, en su capacidad tanto de proporcionar beneficios para la sociedad como de representar su peor amenaza. La infraestructura, la pericia, los conocimientos y los métodos, todo ello se origina en el mismo ecosistema. Las únicas defensas que tenemos contra los riesgos informáticos están en las mismas tecnologías informáticas.

Dado que no existe salvaguarda alguna contra la velocidad de actuación de los algoritmos, las únicas opciones posibles son la supervisión mediante los propios recursos informáticos, el rastreo y seguimiento, la elaboración de perfiles, el análisis automático y la toma de decisiones automatizada. Las actividades malintencionadas en el ciberespacio solo pueden ser contrarrestadas inundando de antídotos el propio "cuerpo" del sistema informático, unas medidas invasivas que pueden poner el peligro los mismos valores sociales que las tecnologías informáticas deben preservar, como la privacidad y dignidad de las personas, la confianza y solidaridad, las leyes, los derechos humanos y civiles, la salud y la seguridad, entre otros. Desde un enfoque social de la ciberseguridad, su diseño debe empezar por determinar cuáles son los valores sociales derivados del uso de las tecnologías informáticas, y cuáles de ellos resultan amenazados cuando estas tecnologías son objeto de un ciberataque.

Las sociedades se distinguen, en general, por el grado en que asumen la seguridad de sus integrantes como un asunto colectivo o como un problema personal, que cada quien debe resolver. Mientras que los países escandinavos organizan la seguridad de su sistema social en aras del bien de la colectividad y evitando lo que pueda perjudicarla, las sociedades altamente liberales e individualistas como la norteamericana consideran que dejar al arbitrio de sus ciudadanos el máximo de libertad para decidir lo que ellos consideren bueno y evitar el mal, resulta en el mayor beneficio para todos. Por otra parte, los países de Europa central se sitúan en algún lugar entre estas posiciones.

El desafío actual, como ya lo era para el presidente Eisenhower en 1961, es cómo se desarrollará la tecnología en manos privadas. La seguridad en general, y la ciberseguridad en particular, plantean el mayor riesgo dentro del interrogante originado por la prioridad de los valores financieros frente a los valores sociales. El problema es si las decisiones respecto a cuáles tecnologías informáticas y computarizadas desarrollar, y cómo se van a basar en los balances financieros o en los valores sociales y el bien común.

La privacidad y la determinación de responsabilidades no son principios opuestos

Bryan Ford

El profesor Bryan Ford es director del Laboratorio de Investigación de Sistemas Descentralizados y Distribuidos en la Escuela Politécnica Federal de Lausanne (EPFL), Suiza. Tras la obtención de su doctorado en el MIT, Ford ha ejercido cargos docentes en la Universidad de Yale y la EPFL. Es titular de la cátedra AXA de Seguridad y Privacidad de la Información en la EPFL.

En nuestro mundo digital, la privacidad parece a menudo incompatible con la seguridad y la determinación de responsabilidades.[1] Por ejemplo, cuando necesitamos saber quién está al otro lado de nuestra pantalla ofreciéndonos un servicio, para asegurarnos de que podemos confiar en ese servicio y que su proveedor es una persona responsable; es decir, que cumplirá efectivamente con las reglas del servicio que ofrece.

> “Los nuevos enfoques prometen solidez en materia de seguridad y determinación de responsabilidades, a la vez que preservan el completo anonimato digital y físico.”

En los primeros días de internet, esta prometía ser una plataforma global para la libre expresión, abierta a todo el mundo sin discriminación ni censura. Pero la aparición masiva de comunicaciones fraudulentas (spam) y saboteadores y secuestradores de información (trolls) motivó la necesidad generalizada de medios de identificación de los usuarios, a fin de desenmascarar a los responsables de esos abusos y al menos impedir su nueva ocultación tras identidades falsas una vez que eran bloqueados.

Actualmente, las aplicaciones de Inteligencia Artificial (IA) conocidas como deepfakes pueden usarse para generar millones de identidades falsas e interacciones online, amplificando el poder de la desinformación y el caos en una medida considerable. Tales abusos sociales, que representan una amenaza a los valores democráticos, han suscitado en el público el clamor de que las plataformas mediáticas deberían “hacer algo” al respecto. Pero las respuestas ante esta situación suelen erosionar la privacidad, dado que unos empleados anónimos y un conjunto de algoritmos opacos

[1] Privacy, Security and Accountability: Ethics, Law and Policy [Privacidad, seguridad y determinación de responsabilidades: ética, ley y políticas], edición de Adam D. Moore, Rowman & Littlefield Publishers / Rowman & Littlefield International, 2021.

[2] Aadhaar Failures: A Tragedy of Errors [Fallos del programa Aadhaar: una tragedia de errores], Reetika Khera, Economics & Political Weekly, abril de 2019.

[3] Using “Proof of Personhood” To Tackle Social Media Risks [El uso de la “prueba de individualidad” frente a los riesgos de las redes sociales], Aengus Collins y Bryan Ford, EPFL, marzo de 2021.

[4] Who Watches the Watchmen? A Review of Subjective Approaches for Sybil-resistance in Proof of Personhood Protocols [¿Quién vigila a los vigilantes? Examen de los enfoques subjetivos de resistencia a ataques Sybil en la prueba de protocolos de individualidad], Divya Siddarth, Sergey Ivliev, Santiago Siri y Paula Berman.

al usuario serían los que decidirían sobre la naturaleza "humana" de cada supuesto usuario, mediante criterios que no están consensuados. Además, esos algoritmos requieren la utilización de una gran cantidad de datos de los usuarios, en una forma que invade su privacidad. Y, finalmente, la carrera armamentística que resulta del fraude y la falsificación mediante recursos de Inteligencia Artificial frente a su posterior detección, es una guerra que el ser humano está condenado a perder.

Actualmente, las plataformas digitales de carácter financiero como las creadas para el cambio de criptomonedas prohíben directamente, cada vez en mayor medida, el anonimato, impidiendo la original pretensión de privacidad e "inclusión financiera" de los bitcoins, esto es, su carácter de sistema financiero abierto y democrático que permita la participación global.

En medio de estas tensiones, es natural que la privacidad y la determinación de responsabilidades aparezcan como objetivos contrapuestos respecto a los cuales hay que lograr un equilibrio aceptable. Pero esta dicotomía es falsa, por dos razones. En primer lugar, renunciar a nuestra privacidad —incluso a toda nuestra privacidad— no sería suficiente para garantizar por completo la identificación de un usuario y poder atribuirle con toda seguridad su responsabilidad si nos encontramos sumidos en el círculo de la carrera armamentística IA-versus-IA, ya que las guerras cibernéticas suelen librarse en la práctica con las mismas herramientas de la IA. En segundo lugar, renunciar a nuestra privacidad no solo sería insuficiente, sino también innecesario. Porque los típicos procedimientos para el tratamiento de datos combinan identidad con individualidad, confundiendo el conjunto de la información perteneciente al usuario con el hecho básico de su existencia como individuo único y la capacidad de poder probar este hecho en línea con total seguridad.

Los enfoques basados en grandes conjuntos de datos, o Big Data, asumen que lo importante acerca de las personas es la suma de la información identificativa almacenada en la base de datos: nuestro nombre, dirección, número de identidad, nuestro perfil o perfiles en las redes sociales, etc. Pero toda la información digital es falsificable, y lo está siendo cada vez más. El análisis de esa información como medio de identificar al usuario es lo que compromete nuestra privacidad y, a la vez, lo que nos pone en la carrera armamentística de la inteligencia artificial. El programa Aadhaar, creado en la India,[2] representa un valioso experimento en materia de datos mediante la asignación a cada ciudadano de un número de identificación único basado en sus patrones biométricos. Pero han surgido muchos problemas de fiabilidad, exclusión y corrupción de datos en Aadhaar, que han hecho de este sistema un preocupante caso, que refleja los riesgos involucrados cuando se asume que la información digital representa, de manera fiable, a una persona real.

Por suerte, la obtención y el análisis de información identificativa no es la única forma de determinar y atribuir responsabilidad online. Una alternativa a la identificación personal por métodos invasivos —es decir, un modo de saber quién hace qué en la red— es el uso de métodos de comprobación experimental de la individualidad mediante formas de prueba digitales anónimas pero atribuibles a una persona, que garantizan unívocamente la existencia de esa persona real sin necesidad de identificarla.[3] Se ha investigado una variedad de métodos[4] para comprobar la individualidad manteniendo en gran medida la seguridad y la privacidad.[5] Algunos de ellos prometen una capacidad de seguridad y asignación de responsabilidad fiables dentro de un completo anonimato digital y físico. Por ejemplo, pruebas digitales de "presencia" que demuestran que los asistentes a una conferencia son personas reales y únicas, sin necesidad de aportar información identificativa alguna.

Las criptomonedas y las monedas digitales de los bancos centrales son otro ejemplo de tensión entre la seguridad y la privacidad.[6] El cumplimiento de las normativas financieras requiere la identificación del usuario, lo cual representa un inconveniente para el anonimato, la autonomía y la naturaleza "transfronteriza" tan valorada por muchos usuarios de criptomonedas. De modo similar, la percepción de la moneda digital de los bancos centrales como instrumento de supervisión digital por parte de gobiernos y corporaciones puede terminar por amenazar su adopción. Pero con las tecnologías para la gestión descentralizada de datos personales, por ejemplo, ni las criptomonedas ni las monedas digitales de los bancos centrales tienen que enfrentarse necesariamente con la disyuntiva entre privacidad o determinación de responsabilidad.[7] Las monedas digitales del futuro pueden ser anónimas e incluso en principio similares al efectivo,[8] a la vez que perfectamente susceptibles de rastreo por los investigadores en los casos de fraude o blanqueo de dinero, sin necesidad de saber el nombre o la información de cuenta del destinatario.[9]

Debemos ser prudentes ante la posición purista en materia de seguridad según la cual es necesario sacrificar la privacidad en el altar de la ley y el orden; así como ante la purista posición contraria a favor de la privacidad según la cual para seguir disfrutando de libertad de expresión tenemos que aceptar pagar un alto nivel arbitrario de abuso informático.

Entre ambos extremos existen soluciones que nos permiten vivir tanto con seguridad como con privacidad. Lo que necesitamos es una mejor comunicación e intercambio de conocimientos entre los organismos reguladores y los tecnólogos que desarrollan y manejan estas herramientas.

[5] Identity and Personhood in Digital Democracy: Evaluating Inclusion, Equality, Security, and Privacy in Pseudonym Parties and Other Proofs of Personhood [Identidad e individualidad en la democracia digital: evaluación de la inclusión, igualdad, seguridad y privacidad en la participación mediante pseudónimo y otras pruebas de individualidad], Bryan Ford, noviembre de 2020.

[6] Design Choices for Central Bank Digital Currency [Elección por diseño para la moneda digital de banco central], Sarah Allen et al.: Documento de trabajo 140 para Global Economy & Development, Brookings Institution, 23 de julio de 2020

[7] CALYPSO: Private Data Management for Decentralized Ledgers [CALYPSO: Gestión de datos personales en libros contables descentralizados], Eleftherios Kokoris-Kogias et al., agosto de 2021

[8] How to Issue a Central Bank Digital Currency [Cómo emitir moneda digital de banco central], David Chaum, Christian Grothoff y Thomas Moser, Swiss National Bank, marzo de 2021

[9] Open, Privacy-Preserving Protocols for Lawful Surveillance [Protocolos abiertos que preservan la privacidad para la supervisión legal], Aaron Segal, Joan Feigenbaum y Bryan Ford, julio de 2016

Capítulo 02

Mitigación de riesgos informáticos: de las infraestructuras críticas a la computación cuántica

El futuro de la ciberseguridad se construye a partir de la naturaleza en constante cambio del ciberespacio, en conjunción con la velocidad de procesamiento de la maquinaria actual y la aceleración que proporcionan la inteligencia artificial y la capacidad de aprendizaje automático. Todo lo cual presenta cada vez mayores opciones para los ataques maliciosos. En este entorno, ¿podemos readaptar la resiliencia de las infraestructuras críticas existentes creadas desde una perspectiva tradicional del riesgo? ¿Cómo podemos afrontar los problemas de seguridad relativos a las operaciones en la nube? ¿Podemos proteger nuestros algoritmos de aprendizaje automático de ataques provenientes de la inteligencia artificial? ¿Seguirá siendo segura nuestra información cuando la computación cuántica posea capacidad suficiente para descifrar todas nuestras medidas de protección?

Diseño y readaptación de la resiliencia en infraestructuras críticas

Giovanni Sansavini

Giovanni Sansavini es profesor asociado de Ingeniería de Fiabilidad y Riesgos en la Escuela Politécnica Federal (ETH) de Zurich. Ocupa la cátedra AXA del Centro de Riesgos de la ETH y del Comité Técnico sobre Infraestructuras Críticas de la Asociación Europea para la Seguridad y Fiabilidad. Giovanni Sansavini obtuvo la licenciatura en ciencias en la especialidad de ingeniería de energías y el Master en ingeniería nuclear en el Politécnico de Milán en 2003 y 2005 respectivamente. En 2010 recibió el doctorado en ingeniería mecánica del Tecnológico de Virginia y en ingeniería nuclear del Politécnico de Milán.

> “Hay muchas infraestructuras críticas para el funcionamiento de nuestras sociedades, las cuales pueden ser diseñadas o readaptadas para lograr resiliencia en materia informática.”

Los sistemas y sectores "críticos" son indispensables para mantener el bienestar de la sociedad. La mayoría de esos sectores o industrias son esenciales para el funcionamiento continuo de nuestras sociedades, ya que proporcionan servicios como calefacción o agua potable para satisfacer necesidades vitales básicas, o el suministro eléctrico para las fábricas y el sector financiero.

Los ciberataques a cualquiera de esos sectores o a una parte de sus infraestructuras pueden causar estragos, como ilustra el ataque de ransomware que sufrió en 2021 la Colonial Pipeline, el cual generó escasez en el suministro de gasolina y motivó el pánico en las compras en el sureste de los Estados Unidos.[1] Que una determinada infraestructura sea considerada crítica es un reflejo de nuestras normas y valores sociales. Ciertos sectores se consideran críticos en un país y no en otro, como sucede muchas veces con las instalaciones comerciales o los organismos de defensa. No obstante, todos ellos comparten en la práctica muchas similitudes.

Los enfoques actuales respecto a la protección de las infraestructuras críticas frente a los riesgos informáticos son similares a los de las infraestructuras no críticas, a partir de procesos consolidados y normas internacionales bien establecidas para la evaluación y la gestión de riesgos, como la normativa ISO (International Organization for Standardization), con los que se pretende descartar cualquier problema de importancia en el sector nuclear o en las misiones espaciales, por ejemplo.

No obstante, esta forma de enfocar las situaciones de riesgo tiene serias limitaciones. Los riesgos en materia informática encierran una considerable incertidumbre respecto a la naturaleza y magnitud de las amenazas, así como respecto a su evolución. Además, hay ciertos riesgos de los que simplemente desconocemos sus consecuencias, como pueden ser los efectos para la salud humana o el medio ambiente del derrame de determinada sustancia química. Este tipo de peligros que afectan al mundo físico puede estar relacionado con riesgos informáticos de manera no siempre perceptible a simple vista. Piénsese en el ciberataque que estuvo a punto de tener éxito en una planta de tratamiento de aguas en los Estados Unidos en 2021,[2] cuando unos hackers alteraron los niveles de hidróxido de sodio en un factor de 100, y que podría haber contaminado el agua potable. En esa ocasión, se pudo detener el sabotaje gracias a la intervención humana antes de que llegara a afectarse la calidad del agua, pero disponer de mecanismos de seguridad adicionales representados, por ejemplo, por sensores, podría haber servido de ayuda. Llamamos a tales mecanismos "niveles adicionales de protección".

La idea de los "niveles de protección" es parte de los modernos enfoques basados en diseños resilientes. Actualmente estamos diseñando sistemas capaces de soportar cierto grado de impacto y destrucción, basándonos precisamente en el reconocimiento de nuestra ignorancia respecto a determinados peligros y amenazas. En cierto sentido, debemos ser agnósticos frente al tipo de amenaza que enfrentamos para complementar adecuadamente nuestro tratamiento de la situación de riesgo.

La sociedad moderna depende del funcionamiento de nuestras redes. Estamos interconectados en todo, desde las cadenas de distribución de alimentos y el tratamiento de aguas hasta el suministro de energía. Esas redes nos permiten disfrutar de una variedad de servicios y hacer las cosas de manera eficiente. La red eléctrica, por ejemplo, nos permite compensar el excedente de energía eléctrica producido en algún momento en algún lugar enviándolo a otro que en ese momento disponga de un suministro menor. Estas redes nos hacen interdependientes. En 2015, Ucrania sufrió un ciberataque en su red de suministro que dejó sin energía eléctrica a 225 000 personas.[3] Dada su interconexión con la red eléctrica europea, la inestabilidad pudo haber alcanzado una escala mucho mayor. Afortunadamente, las redes internacionales y tecnológicas de esta clase cuentan con normas que los operadores nacionales cumplen diligentemente.

Para asegurar la disponibilidad de un servicio cuando se presenta un problema en algún punto de la red, como un apagón en un país interconectado, una opción es utilizar estaciones de seguridad intermedias o buffers, como centros de suministro locales. Pero en otro tipo de redes pueden llegar a presentarse drásticos efectos en cascada. El ataque de ransomware de julio de 2021 efectuado contra Kaseya, proveedor norteamericano de software de gestión informática, ocasionó el bloqueo de decenas de miles de ordenadores en todo el mundo, y los hackers pidieron 70 millones de dólares para desbloquear los sistemas afectados[4].

Cuando la infección informática afecta a una parte del sistema, una opción es la desconexión temporal de esa parte de la red. Un diseño resiliente debe asegurar la posibilidad de funcionamiento del sistema en modo aislado, a la manera de "islas" que puedan operar independientemente. Otra forma de adaptación es la flexibilidad en el modo de operación, por ejemplo utilizando fuentes o vías de suministro complementarias, como pueden ser eléctricas o de petróleo, en caso de fallo de la red o la tubería principal.

Tales diseños adaptables pueden incorporarse a infraestructuras existentes, mediante la reelaboración del diseño original o añadiendo niveles de protección. Ello implica un coste, desde luego, pero vale la pena realizar el esfuerzo por mejorar las infraestructuras existentes, ya que la construcción de nuevas infraestructuras tiene un impacto importante, sobre todo en lo que respecta al medio ambiente. Mientras que en el caso de nuevas infraestructuras que aún no existen, por ejemplo, redes para el almacenamiento y distribución de dióxido de carbono, o para la producción y distribución de hidrógeno, su diseño desde cero deberá hacerse siguiendo los principios descritos anteriormente: incluyendo sistemas de aislamiento, buffers, flexibilidad de operación, y otros que proporcionen resiliencia a nuestras infraestructuras interconectadas ya desde la fase de diseño.

[1] DHS to Issue First Cyber Security Regulations for Pipelines After Colonial Hack [El Departamento de Seguridad Nacional promulgará la primera normativa de ciberseguridad para tuberías de distribución tras el ataque a Colonial], Ellen Nakashima y Lori Aratani, The Washington Post, 25 de mayo de 2021

[2] 'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town ["Sustancias peligrosas": Hackers intentan envenenar el suministro de agua de una población de Florida], Frances Robles y Nicole Perlroth, The New York Times, 8 de febrero de 2021

[3] Hackers Behind Ukraine Power Cuts, Says US Report [Hackers tras el apagón de Ucrania, según informe de EE.UU.], BBC, 26 de febrero de 2016

[4] Ransomware Hackers Demand $70 Million to Unlock Computers in Widespread Attack [Los hackers autores del ataque general de ransomware piden 70 millones de dólares para desbloquear los ordenadores], Robert McMillan, The Wall Street Journal, 5 de julio de 2021

Nuevas estrategias para reforzar la ciberseguridad en la nube

Robert Deng

Robert Deng es profesor y catedrático AXA de ciberseguridad, director del Centro de Seguridad Móvil y vicedecano de facultad e investigación de la Escuela de Computación y Sistemas de Información de la Universidad de Gestión de Singapur. Es miembro del IEEE y de la Academia de Ingeniería de Singapur.

En aproximadamente dos décadas, la computación en la nube ha seducido virtualmente a todas las organizaciones de todos los tamaños existentes en la Tierra por sus muchas ventajas, como su rápida implementación, bajos costes iniciales y facilidad de ampliación. En lugar de tener, y tener que mantener, sus propias infraestructuras de software, hardware y almacenamiento de datos, empresas y organizaciones prefieren por lo general realizar sus operaciones en la nube, donde comparten infraestructuras y, a veces, servicios con otros usuarios.

> “En materia de seguridad, el mayor enemigo es la complejidad.”

Este cambio hacia infraestructuras compartidas conlleva nuevos retos en materia de seguridad, como la posibilidad de filtraciones masivas de datos y ataques a recursos informáticos para el robo de criptomonedas. Pero, ¿por qué?

Las dificultades en la seguridad surgen debido a que la computación en la nube es obviamente menos segura que en la propia sede. En los sistemas informáticos tradicionales situados en la sede del cliente, la infraestructura física, el hardware y el software se encuentran todos dentro de la organización. Esta controla todo cuanto sucede, disponiendo de una buena visibilidad de sus propios sistemas y soportes de información.

Debido a la virtualización de los equipos, servidores, etc., en la nube, los distintos componentes se encuentran en lugares diferentes y en las manos de diversos proveedores de servicios, haciendo del entorno algo muy heterogéneo. Ni el propietario de los datos, ni los consumidores, ni tampoco los proveedores de servicios tienen el control completo de la totalidad del entorno virtual. Incluso disponen de poca visibilidad del sistema, por lo que podría producirse una filtración o pérdida de datos sin que nadie lo notara.

Además, lo que llamamos la "superficie de ataque" es mucho más extensa en la nube que en el sistema informático situado en la propia sede: los sistemas se hacen más vulnerables y más expuestos a ciberataques. La vulnerabilidad puede residir en las propias máquinas, o por el lado del proveedor del servicio, y hasta por el lado del usuario, por ejemplo, si recibe un ataque de phishing y el usuario pierde la confidencialidad de sus credenciales.

¿Qué es la estrategia de "confianza cero" (Zero Trust) que predomina actualmente como medida de seguridad en la nube en todo el mundo?

Hasta ahora, habíamos asumido que siempre podíamos confiar en nuestros servidores y sistemas operativos para mantener la confidencialidad de nuestros datos, autenticar correctamente a los usuarios y aplicar las medidas de control de acceso pertinentes. Todo esto había funcionado bien con la tecnología tradicional con base en nuestras sedes. Hoy en día, con la nube, estos supuestos resultan muchos más arriesgados, aunque por desgracia muchos siguen confiando en ellos.

La estrategia de confianza cero, Zero Trust, consiste en no confiar de manera automática en las infraestructuras, dispositivos ni proveedores de servicios sino, por el contrario, estipular en cada caso la confianza necesaria basándonos en una serie de distintos principios. Un ejemplo de ello es la creación de espacios independientes separados por barreras de seguridad. Por ejemplo, el establecimiento de un firewall entre el servidor de la aplicación y el servidor de la base de datos contentiva de la correspondiente información confidencial.

Otro principio es el control de seguridad multinivel, de modo que si un nivel de protección fallara, todavía se mantendría operativo un segundo nivel que protegería la información. Si, por ejemplo, fallara el sistema de acceso al disco duro porque un hacker descubre nuestra contraseña, el cifrado o la encriptación de datos actuaría como un segundo nivel de protección. La autenticación en dos pasos descansa en este principio.

Un tercer principio consiste en seguir las mejores prácticas de seguridad recomendadas, por ejemplo el principio de "privilegio mínimo", el equivalente numérico de la concesión de acceso según la "necesidad de saber".

En la nube, controlar el acceso a cada punto del sistema se convierte pronto en una tarea abrumadora. ¿Cuáles son las estrategias para superar los problemas de la ampliación de entornos distribuidos?

Los modelos de control de acceso diseñados para los sistemas centralizados de información pueden funcionar bien en una variedad de sistemas de información distribuida.

La primera opción es el "control de acceso discrecional": el propietario de los datos decide qué usuario está autorizado para acceder a sus datos, editarlos o utilizarlos. El modelo de control discrecional funciona bien incluso en sistemas altamente distribuidos. Otra opción es el "control de acceso obligatorio", que utilizan los gobiernos y los organismos militares para la información clasificada. Los datos se etiquetan, dependiendo del nivel de seguridad requerido, y cada usuario recibe una autorización de seguridad. Si la etiqueta y el nivel de autorización coinciden, se permite el acceso. Por último, una variante de este sistema es la "autorización según función". Esta es útil cuando, por ejemplo, se realizan muchos cambios en los turnos o en el equipo de trabajo. En vez de conceder acceso privilegiado directamente al usuario, se concede el privilegio dependiendo de la función, de modo que quien ejerza esa función en cada momento dado dispondrá del correspondiente acceso.

El "internet de las cosas" (Internet-of-Things, IoT) es un ejemplo extremo de un entorno informático distribuido. ¿Los problemas de seguridad son aquí distintos de los que se encuentran en la nube?

En la computación en la nube, el centro de datos cumple la función de manejar los datos y suministrar los servicios, por lo que existe todavía una cierta gestión centralizada. Pero el internet de las cosas es un entorno abierto, complejo y enorme, con gran variedad de dispositivos y de usuarios, incluyendo aparatos físicos de poca capacidad computacional y escasa duración de baterías, como cierres de puertas, luces, etc. Aparatos que no admiten encriptación con sólidas medidas de seguridad o soluciones informáticas, y en los que un ejemplo común de ciberataque es la "negación de servicio distribuido", en la cual el hacker envía tantas órdenes a los aparatos que estos se sobrecargan y quedan bloqueados. En otras palabras, la complejidad sistémica del internet de las cosas puede llegar a crecer más allá de la capacidad que pueda tener cualquier persona para manejarlo.

La búsqueda de una solución técnica satisfactoria para el control de acceso al internet de las cosas es hoy día una cuestión abierta. En mi opinión, la "seguridad IoT" requiere de un enfoque diferente: nuevas reglas de seguridad y un mayor conocimiento por parte del usuario acerca de la seguridad general. Esto podría hacerse, por ejemplo, mediante sistemas de certificación: productos como las cámaras de circuito cerrado (CCTV) podrían certificarse para ciertos niveles de seguridad específicos, lo que animaría a los usuarios a conocer mejor estos sistemas, y también promovería la creación de dispositivos más seguros por parte de los fabricantes.

IA y aprendizaje automático: la defensa de los mecanismos defensivos

David Rios Insua

David Ríos Insua es catedrático AXA de análisis de riesgos adversarios en el ICMAT-CSIC y miembro de la Real Academia de Ciencias española. Ha recibido el premio DeGroot del ISBA y fue director del programa de Juegos y Decisiones ante Riesgo y Fiabilidad del SAMSI. Ha desempeñado cargos académicos y de investigación en las universidades de Duke, Purdue, IIASA, Aalto, Paris-Dauphine, Shanghai University for Science and Technology, CNR-IMATI, UCM, UPM y URJC.
Está especializado en análisis bayesiano, análisis para la toma de decisiones y análisis de riesgos, y sus aplicaciones a la seguridad y la ciberseguridad. Es, además, director científico de Aisoy Robotics.

Las máquinas son cada vez más inteligentes. Actualmente, el automóvil nos ayuda a planificar nuestro recorrido y a estacionarnos, detectando los árboles, las aceras y los vehículos cercanos, y activando los frenos cuando es necesario. En un futuro no muy lejano, podrían llevarnos en forma rutinaria de la casa al trabajo sin que tengamos que conducir. Son capaces de reunir y transmitir información, y de aprender durante el proceso, gracias a la inteligencia artificial en un mundo conectado globalmente. Pero, ¿las máquinas inteligentes interconectadas harán nuestro mundo más seguro, o todo lo contrario?

La inteligencia artificial (IA) es utilizada actualmente por gobiernos y empresas de ciberseguridad para detectar vulnerabilidades inesperadas en sus sistemas de información y remediarlas antes de que los hackers puedan aprovecharlas. Por ejemplo, los sistemas automatizados pueden comprobar el estado de cientos de miles de dispositivos conectados y enviar señales de advertencia a los ingenieros en caso de que alguno manifieste anomalías que puedan significar una posible intrusión en el sistema. Los modelos predictivos también pueden anticipar fallos inminentes, y gracias a la IA podemos disponer de un tiempo precioso para reaccionar ante una situación futura.

Además de los sistemas que ejercen una mera función de vigilancia, algunos sistemas inteligentes pueden realizar análisis en profundidad para detectar amenazas en el entorno o en los procedimientos de seguridad de una organización. Pero la avalancha de datos involucrada en estos procesos debe ser agregada en su conjunto de forma coherente para poder obtener indicadores de riesgos que sean útiles y significativos, para lo cual el uso de modelos económicos en combinación con el aprendizaje automático resulta conveniente y eficaz. Los sistemas inteligentes para contrarrestar amenazas también pueden analizar contenidos de la web y las redes sociales para detectar en línea comentarios negativos sobre una empresa, lo que constituye una amenaza a su reputación pero también podría motivar un ciberataque. Estas funciones van más allá de la vigilancia, ya que determinar la naturaleza de un comentario, por ejemplo, requiere del uso de herramientas avanzadas de IA, como el análisis del lenguaje y de las expresiones emotivas.

En todos estos casos, la IA está en la base de la toma de decisiones sobre ciberseguridad en presencia de adversarios. Nuevos enfoques, como el análisis de riesgos adversario, permiten facilitar las decisiones directamente en línea a la vez que mejorar la velocidad y la precisión en la gestión de riesgos informáticos.

No obstante, mientras que la lista de aplicaciones de la IA que requieren de una estricta seguridad es interminable (conducción automatizada, filtros de contenidos, vigilancia y mantenimiento del orden, etc.), la IA en sí misma tampoco es inmune a los ciberataques. Para garantizar la seguridad de las aplicaciones de IA, los algoritmos de aprendizaje automático deben ser robustos y fiables.

De hecho, mientras que los algoritmos de aprendizaje automático más avanzados funcionan extraordinariamente bien en su aplicación a la información estándar, son, sin embargo, vulnerables a los llamados "ataques adversariales". Estos ciberataques utilizan datos diseñados expresamente para engañar a la IA. El primer caso de este tipo de ataque fue dirigido a un dispositivo entrenado para reconocer imágenes de osos panda. El atacante logró que el dispositivo reconociera con toda seguridad un panda cuando la imagen correspondía en realidad a un gibón. Para hacer cosas como esta, el atacante solo tiene que interferir en el proceso de aprendizaje del dispositivo presentándole datos falsamente etiquetados —en este caso, sustituyendo imágenes de pandas por las de un gibón durante la fase de aprendizaje. En la vida real, un equivalente preocupante consistiría en engañar a un automóvil autónomo para que leyera una señal de alto como un límite de velocidad, con lo que no se detendría al llegar a la señal. Un estafador podría representar fraudulentamente una reclamación de seguros, haciendo que el correspondiente algoritmo autorizara una compensación. Muy importante es el hecho de que los hackers reaccionan muy rápidamente a la implementación de sistemas de defensa de los aprendizajes automáticos, lo que puede tener serias implicaciones en ámbitos como los sistemas de conducción automatizada, sistemas de defensa, de aplicación de la ley, o de la atención sanitaria, por nombrar solo unos pocos.

Estos problemas de seguridad cuestionan los métodos estándar del diseño de algoritmos, ante la existencia de adversarios adaptables, dispuestos a intervenir para modificar los datos en los que confiamos.

Frente a estos ataques de adversarios, ha surgido una nueva área de investigación llamada "aprendizaje automático adversario", cuyo objetivo es desarrollar barreras robustas contra los ataques maliciosos a sistemas de aprendizaje automático. Ello implica estudiar los ataques producidos, así como las defensas contra los ataques. Por ejemplo, para la detección de spam se han elaborado sistemas de clasificación capaces de detectar y detener el spam, pero los hackers aprendieron a burlar el sistema de protección cambiando las palabras clave involucradas (en lugar de "viagra", por ejemplo, empezaron a usar VI@GR@) para que el sistema anti spam considerara el mensaje legítimo. Hemos tenido que aprender sobre formas cambiantes de ataque, e incorporar mejores defensas que no afectaran a la entrada de correos legítimos. El campo de investigación del "aprendizaje automático adversario" emplea principalmente teoría de juegos para modelizar la confrontación entre los sistemas de aprendizaje automático y sus adversarios.

Aunque en el "aprendizaje automático adversario" se suele asumir que defensores y atacantes comparten cierta información y conocimientos, esta asunción de una base de conocimiento común es cuestionable en el ámbito de la seguridad, ya que los adversarios siempre tratan, naturalmente, de ocultarse mutuamente la información que poseen. En consecuencia, en los actuales momentos estamos desarrollando otra forma de enfocar el aprendizaje automático adversarial, que denominamos "análisis de riesgo adversarial" y que utiliza pronósticos y previsiones. Lo que hacemos es modelizar la forma en que los hackers realizan sus ataques y cómo reaccionan, y usamos este conocimiento para predecir las formas en que podrían atacar en el futuro, sin partir de la suposición más fuerte de un conocimiento compartido.

La ciberseguridad y la IA van de la mano. Como sucede con muchas herramientas y metodologías, la IA es también una espada de doble filo: hacemos uso de formas modernas de aprendizaje automático y de las herramientas de IA para diseñar sistemas informáticos más seguros, pero necesitamos diseñar formas de aprendizaje automático y de IA que, a su vez, no resulten afectadas por ciberataques. Necesitamos de la ciberseguridad para crecer aún más en inteligencia.

> **"Para poder contar con inteligencia artificial, es necesario estar conectados. Esto abre muchas posibilidades, pero también nos hace vulnerables."**

La computación cuántica: ¿una nueva amenaza?

Antonio Acín

Antonio Acín es profesor de investigación de ICREA en el ICFO-Instituto de Ciencias Fotónicas. Se graduó en Física en la Universidad de Barcelona (UB) y en Ingeniería de Telecomunicaciones en la Universitat Politècnica de Catalunya. Obtuvo su PhD en física teórica en 2001 en la UB y, tras una estancia posdoctoral en Ginebra, se incorporó al ICFO en 2003. En el ICFO, dirige el grupo de Teoría de la Información Cuántica. El profesor Acín es además catedrático AXA en ciencias de la información cuántica desde 2016.

> “Los algoritmos y los ordenadores cuánticos tendrán un impacto sobre la ciberseguridad, pero ya podemos preparar nuestros sistemas para la resiliencia cuántica.”

En la antigua Roma, si se quería compartir un mensaje secreto con un aliado lejano, se utilizaba el código César, una de las técnicas de cifrado de datos más famosas y sencillas. Las letras del mensaje se desplazaban un número fijo de posiciones en el alfabeto: por ejemplo, la A se convierte en I, la B en J, y así sucesivamente. Hoy en día, todos utilizamos la criptografía a diario, por ejemplo en los pagos con tarjeta de débito, los intercambios de correo electrónico o la transmisión de datos críticos. La criptografía es esencial para nuestra ciberseguridad y, por supuesto, las técnicas de encriptación han evolucionado enormemente.

La criptografía es el arte de transmitir información confidencial de forma protegida y segura. Actualmente, este proceso se basa principalmente en la seguridad informática: los protocolos existentes son seguros porque los hackers tienen que resolver un problema para el que no se conoce ningún algoritmo eficiente. Por ejemplo, para entrar en nuestro sitio web favorito o establecer una conexión remota, hacemos uso del protocolo RSA todos los días, el cual se basa en el hecho de que no existe un algoritmo eficiente capaz de factorizar números muy grandes. La seguridad informática es conveniente porque resulta barata: es una solución de software para la que no hace falta comprar ningún dispositivo, basta con ejecutar un programa. A pesar de ello, la seguridad informática encierra sus riesgos.

El advenimiento de la computación cuántica, basada en las propiedades colectivas de los estados cuánticos, como la superposición y el entrelazamiento, arroja algunas dudas sobre la aplicabilidad de determinados algoritmos de seguridad, debido a que los fenómenos del mundo cuántico conferirán a los ordenadores cuánticos una enorme potencia computacional. Ya en 1994 el famoso investigador Peter Shor, por entonces en los Laboratorios Bell, diseñó un algoritmo cuántico eficiente para la factorización. Un fisgón provisto de un ordenador cuántico podría estar en condiciones de factorizar grandes números y así hackear el protocolo RSA. Esto no se percibe como un riesgo en estos momentos porque, hasta donde sabemos, nadie posee la tecnología para construir un computador cuántico lo bastante potente para ejecutar el algoritmo de Shor. Pero, ¿podemos estar del todo seguros? Y aunque así fuera, ¿cuánto tiempo transcurrirá antes de que alguien pueda disponer de un computador cuántico de potencia semejante?

Pero, aun sin la computación cuántica, no hay ninguna prueba de que no pueda existir un algoritmo clásico eficiente para resolver las dificultades que actualmente aprovechan los protocolos criptográficos. En el caso del RSA, es posible, en principio, que exista un algoritmo de factorización eficiente de naturaleza no cuántica. Parece improbable que así sea tan solo porque los numerosos intentos efectuados para encontrarlo han fracasado hasta el momento. Pero no podemos excluir que algún día un hacker lo bastante inteligente desarrolle un algoritmo no cuántico capaz de convertir nuestra seguridad informática en mera ilusión.

Frente a este riesgo, hay dos enfoques posibles. El primero es persistir en el paradigma de nuestra seguridad informática y diseñar nuevos protocolos basados en problemas que sean difíciles de resolver también para un ordenador cuántico. Esto se conoce como “criptografía postcuántica”, y ofrece una ventaja importante: sigue siendo una solución de software y, por tanto, barata, y su integración con las infraestructuras existentes es sencilla y directa, ya que solo hay que ejecutar un nuevo programa. Pero conserva, no obstante, algunos de los riesgos anteriores: no hay, y sigue sin haber, prueba alguna de la no existencia de un algoritmo eficiente para descifrarla. Por tanto, no podemos excluir la posibilidad de que un hacker lo bastante inteligente y equipado con un algoritmo tal pueda descodificar el protocolo.

El segundo enfoque es la “seguridad basada en la física cuántica”, un cambio de paradigma en las aplicaciones de seguridad. A partir de los fenómenos cuánticos, es posible diseñar protocolos de criptografía cuántica cuya seguridad se fundamenta en las leyes de la física del quantum. De este modo, un fisgón que intentara hackear el protocolo no tendría que resolver un complejo problema computacional, sino hackear la propia implementación cuántica. La gran ventaja de los protocolos basados en la criptografía cuántica es que tienen una seguridad demostrable. Pero su gran desventaja, por otra parte, es que se trata de una solución de hardware: habría que adquirir un dispositivo aparte, que además sería costoso. Debido a ello, la seguridad dependería de la implementación, y su integración con las infraestructuras existentes sería también más compleja.

El mejor enfoque que se ha pensado hasta la fecha es combinar la seguridad informática basada en las propiedades de la física cuántica con una criptografía difícil de descodificar por medios cuánticos. Se trataría, por una parte, de diseñar protocolos postcuánticos que ofrezcan, hasta donde podamos comprobar, la mayor resistencia posible frente a los ordenadores cuánticos y, por otra parte, desarrollar protocolos de criptografía cuántica más baratos y a la vez más integrables con las infraestructuras existentes. De este modo, reforzaríamos nuestras técnicas de encriptación añadiendo un nivel de seguridad proveniente de la física cuántica cuanto antes lo permita el desarrollo de la técnica. La seguridad en la comunicación tiene muchas vertientes, y hay que considerar la variedad de niveles confidencialidad, riesgos y presupuestos, entre otras cosas. Mientras más herramientas tengamos para enfrentar todos esos retos, mayor será nuestra fortaleza ante los mismos, y ya resulta claro que la física cuántica nos aporta nuevos recursos para mantener la confidencialidad que deseamos. La combinación de ambos enfoques harán las cosas mucho más difíciles para los hackers, que tendrán que enfrentarse al mismo tiempo a complejos problemas computacionales y a los fenómenos de la física cuántica.

[1] How Does a Quantum Computer Work? [¿Cómo funciona un ordenador cuántico?], Michael Tabb, Andrea Gawrylewski y Jeffery DelViscio, Scientific American, 7 de julio de 2021

Capítulo 03

Resiliencia informática de organizaciones y estados

El desarrollo de la resiliencia informática reclama la participación de todos los agentes económicos: el sector privado, los estados y los organismos internacionales. ¿Qué implicaciones tiene esto para la empresa privada? ¿Cómo puede el sector privado colaborar para una mayor resiliencia colectiva? ¿Y qué regulaciones existen, si las hay, sobre el uso del ciberespacio? ¿Cuáles son los factores de éxito que nos permitirán avanzar colectivamente en el área de la seguridad informática? ¿Cuál es la posición de los estados y cuál su papel?

Creación de resiliencia informática en las organizaciones

Arnaud Tanguy

Arnaud Tanguy es director de seguridad del Grupo AXA, responsable de la seguridad de la información, la seguridad física, el sector de salud y seguridad, y la resiliencia operacional del Grupo. Anteriormente fue director de seguridad de la información (CISO) de la Gestora de Inversiones AXA, y estuvo a cargo del programa global de seguridad de la información en todas las líneas de negocios. Antes de su incorporación a AXA, Arnaud fue gerente sénior de PwC y de EY, especializado en seguridad de la información y estrategia de TI. Inició su carrera como oficial de la Marina francesa, donde dirigió el departamento de TI, telecomunicaciones y seguridad de la información en la base naval de Brest.

Con las vulnerabilidades del software, las amenazas de infiltración en el sistema y la desatención de las medidas de seguridad por parte del personal, las empresas se enfrentan a riesgos informáticos provenientes tanto de su propio personal como de amenazas exteriores.

> “La “seguridad por diseño” es la forma en que debemos abordar cada proyecto de la empresa.”

¿Qué significa la resiliencia informática para una organización?

Conseguir resiliencia en materia de informática requiere capacidad de anticipación, así como un riguroso enfoque sistemático que nos permita estar preparados para hacer frente a cualquier situación inesperada. La resiliencia no significa solamente la capacidad de evitar incidentes, sino también estar en posición de recuperarse incluso de la peor situación que pudiera presentarse. La resiliencia informática es todo un reto en el espacio cibernético, donde las cosas cambian a un ritmo vertiginoso. En el futuro, todas las organizaciones deben estar en capacidad de responder adecuadamente a sus clientes, empleados e inversionistas, independientemente de los problemas que puedan presentársele en el terreno informático.

¿Cuáles son las repercusiones concretas que puede tener un ciberataque para una empresa? ¿Por ejemplo, un robo de información?

Una sustracción de información se produce cuando un individuo logra acceder a datos que puede difundir, vender o utilizar para suplantar la identidad de otra persona; por lo que el primer riesgo lo sufre la persona a la que pertenecen los datos. El segundo riesgo es para la empresa, que podría fallar en el cumplimiento de reglamentaciones que normalmente incluyen, entre otras cosas, la obligación de informar a las

personas cuyos datos hayan resultado comprometidos por la sustracción o filtración. La reputación es otro punto por considerar: la empresa es una víctima, pero es su nombre el que aparece en los medios, lo que puede ocasionar falta de confianza por parte de sus clientes y pérdidas de oportunidades comerciales.

Desde el punto de vista legal también existen riesgos porque muchos contratos no contemplan todavía cláusulas que especifiquen las medidas de seguridad que debe asumir el cliente, lo que crea lagunas legales. Por último, son muchos los impactos financieros que genera un ciberataque, ya que hay que implementar una pronta solución a las vulnerabilidades detectadas, emitir comunicados a los medios y a los clientes, que pueden ser millones de ellos, compensar a los clientes afectados y a veces incluso pagar multas, todo lo cual puede generar costes importantes.

¿Qué medidas toman las organizaciones privadas para limitar los riesgos informáticos?

Los riesgos son cada vez más complejos y los ataques más profesionales, por lo que las medidas de seguridad deben adoptarse de forma holística y estratégica. Estas empiezan por las personas: hay que proporcionar conocimiento y preparación a través de comunicaciones internas, formaciones obligatorias dentro de la empresa y hasta campañas de prevención mediante ataques de phishing simulados. Capacitamos a nuestros empleados como ciudadanos de un entorno informático, y estimulamos la difusión de esa capacitación entre sus familiares y amistades, de modo que, a través de nuestro personal, contribuimos indirectamente a la capacitación de todo el entorno social.

El equilibrio adecuado entre las prioridades de la empresa y la seguridad es un tema complejo, pero actualmente existe mucha conciencia al respecto en las juntas directivas, lo que facilita las decisiones correctas en materia de seguridad a la vez que se atiende a los objetivos del negocio.

Los equipos dedicados a la seguridad tienen la tarea de asignar el nivel de seguridad apropiado a cada proyecto desde sus inicios, un principio que llamamos “seguridad por diseño”. Además, cualquier agente relacionado con la empresa puede también ser víctima de un ataque informático, por lo que se deben incluir cláusulas referentes a la seguridad en los contratos con los proveedores. La parte técnica de los equipos implementa las normas, medidas y procedimientos desde el punto de vista técnico para anticipar tanto la posibilidad de malware “tradicional” como de ciberataques de naturaleza más novedosa, aplicando innovaciones provenientes de la inteligencia artificial, entre otras, y debe también monitorizar las actividades para garantizar que las medidas de seguridad sean las adecuadas. Adicionalmente, se elaboran planes de reacción y recuperación de ciberataques que permitan normalizar la situación lo antes posible.

Los mismos principios son de aplicación en todas partes. Ya sea que la empresa disponga o no de un equipo interno especializado, siempre debe haber alguien encargado y responsable de la seguridad.

¿En qué forma ayudan los reguladores a tener una mayor seguridad en las empresas?

Los organismos reguladores están al tanto de los problemas en materia de informática, especialmente desde la promulgación en Europa del Reglamento General de Protección de Datos (RGPD). Casi en todas partes se pasó de meros incentivos a medidas obligatorias, por ejemplo en lo que respecta a la notificación de incidentes y de filtraciones o pérdida de datos.

Para una empresa tiene mucha ventaja relacionarse desde el principio con los organismos reguladores, practicar la transparencia y generar confianza, ya que ello ayuda a resolver rápidamente los problemas. Desde luego, esto puede representar un reto en sí para las multinacionales: AXA, por ejemplo, trabaja en 64 países diferentes, y tiene que ver con 64 organismos reguladores, cada uno de los cuales trabaja de forma distinta.

Algunas empresas se especializan en servicios de ciberseguridad para sus clientes, por ejemplo, mediante auditorías y el suministro de herramientas de seguridad. ¿Qué papel desempeñan en la creación de un mundo más resiliente en materia informática?

Para una empresa privada, cuya actividad principal no se relacione con la informática, por ejemplo una empresa de una cadena de suministro, la colaboración con los proveedores de ciberseguridad es clave. Porque existe actualmente una auténtica carrera armamentística en este terreno, y el alcance y la velocidad de los ciberataques van rápidamente en aumento, mientras que, como sociedad, aún no contamos con suficiente personal capacitado en materia informática, y el mercado de la ciberseguridad es muy competitivo. Las empresas de servicios de ciberseguridad están en condiciones de reunir y aprovechar esos talentos y de desarrollar recursos avanzados para la ciberdefensa, como la automatización. En pocas palabras, los proveedores de ciberseguridad están contribuyendo a organizar eficazmente el ecosistema informático.

Los proveedores están aportando conocimiento frente a los ciberataques, datos e información, e inteligencia de defensa, además de innovaciones en los servicios que prestan; y por otra parte, los equipos internos de las empresas son buenos conocedores de su negocio, del sector y de la historia de la empresa. Esos equipos internos, además, tienen características híbridas, ya que están conformados por expertos de TI y por personal corporativo, que establece la relación entre los recursos que necesitan proteger y las medidas de protección a utilizar por la empresa. Este trabajo conjunto a nivel directivo es una necesidad.

La resiliencia informática en el mundo tras la pandemia: la urgente necesidad de la cooperación y la comunicación de datos

Heyrick Bond Gunning

Heyrick Bond Gunning es director general (CEO) de S-RM, consultora global de inteligencia e informática. Anteriormente, fue director gerente de Kroll, y antes había sido consultor de DHL en Iraq en 2003 y 2004, tras finalizar la guerra de Iraq. De 2000 a 2003, fue director de captación de clientes para Mergermarket (Acuris). Empezó su carrera trabajando durante 5 años en el ejército británico. Heyrick es licenciado en geografía y arqueología por la Universidad de Manchester y antiguo alumno del Instituto Europeo de Administración de Negocios, INSEAD.

Desde la irrupción de la crisis de la Covid-19 ha habido ataques de phishing dirigidos a los trabajadores remotos, han aumentado los ataques de ransomware a los hospitales, y hasta un mercado de valores tuvo que cerrar por un clásico ataque de negación de servicio.

Aparte del hecho de que el número de ciberataques parece haber aumentado en frecuencia y en magnitud, ¿ha cambiado también el tipo de ataques?

Con la COVID-19, entre marzo de 2020 y marzo de 2021, el número de ataques de ransomware se multiplicó por 4. En estos momentos, esta modalidad de ataque informático constituye aproximadamente el 50 % de todas las formas de sustracción de información, y es una modalidad de ciberataque dinámica y que cambia muy rápidamente. Anteriormente, consistía en que alguien encriptaba la información perteneciente a otra persona y pedía el pago de un rescate para desencriptarla. Hoy, lo que hacen es que acceden a la información, la encriptan y, conociendo el perjuicio a la reputación y los problemas que la situación acarrea en materia reglamentaria, amenazan además con difundir públicamente el ataque. Es, de hecho, una "doble extorsión", y así precisamente se le llama, porque actúa en dos niveles.

¿La pandemia ha generado cambios en cuanto a las prioridades en materia de ciberseguridad?

A un nivel puramente práctico, el uso de dispositivos personales para el trabajo, como ordenadores y teléfonos móviles, constituye un problema. Las políticas y procedimientos al respecto siempre han sido importantes, pero ahora van a estar al frente de los problemas de resiliencia informática, dado que en todo el mundo se están adoptando prácticas flexibles de trabajo remoto, y es una tendencia creciente. Este modelo de trabajo híbrido plantea cuestiones muy difíciles sobre cómo lograr un equilibrio adecuado entre la privacidad del empleado y la aplicación de medidas de protección apropiadas para la información referente al trabajo.

Otra cuestión que va a cambiar en el futuro es la forma en que se asegurarán los riesgos en materia informática. En el sector de los seguros se habla mucho acerca de qué servicios utilizar para reducir los riesgos, incluyendo avisos y ofertas de formación a los clientes, como informes detallados sobre su situación de riesgo, y el establecimiento de planes de contingencia en caso de una filtración o secuestro de información. Si la situación no se maneja bien desde el principio, las primeras 72 horas pueden significar un aumento de más del doble del costo de recuperación.

¿Debería cambiar la forma en que evaluamos los riesgos y la resiliencia informática en una organización?

Ya antes de la COVID-19 se planteaban dudas acerca del valor y la utilidad de las "métricas de preparación" en materia de seguridad informática; y la pandemia ha traído aún más incertidumbre, que ha hecho que disminuya la confianza de los equipos dedicados a la seguridad y de las directivas de las empresas acerca de su capacidad para manejar y hacer frente a la mayoría de los problemas informáticos más importantes.

No obstante, los tres aspectos principales del problema siguen siendo los mismos: las personas, la tecnología y los procesos. Necesitamos garantizar que todo el mundo esté preparado y sepa qué hacer en caso de presentarse una

situación sospechosa. Luego, a pesar de lo útil que pueda ser la tecnología, no podemos depender de ella en exceso, en especial cuando la gente no la entiende bien. Las personas y la tecnología van a la par; y lo que las une son los procesos. Concretamente, disponer de un plan cuando las cosas salen mal. Tenemos que pensar en la peor situación posible antes de que se presenten los problemas, porque resulta muy difícil pensar con claridad en medio de un ataque de ransomware.

Para evaluar nuestro nivel de preparación en ciberseguridad debemos hacernos cuatro preguntas claves: ¿Conocemos a nuestros adversarios? ¿Nos estamos concentrando en los riesgos correctos? ¿Nuestros planes de reacción responden a las situaciones de riesgo más probables, y han sido comprobados? ¿Contamos con un mapa de ruta de recuperación en caso de un incidente? En otras palabras, ¿cómo vamos a volver a poner los sistemas en funcionamiento?

Esto último es lo que resulta más importante ahora, dado que es muy probable que en algún momento la información en manos de la empresa resulte comprometida, ya sea por un ciberataque, un error de algún empleado o incluso por una acción maliciosa por parte de un empleado descontento.

¿Cuáles son las dificultades a superar para poder contar con un ecosistema informático más resiliente?

En primer lugar, el mayor reto reside, obviamente, en la escasa información que poseemos. El sector de la informática es reciente, y los ciberataques muy dinámicos y difíciles de modelizar. La mejor estrategia, en este caso, es diagramar el mapa de decisiones que nos gustaría tener, identificar la información que necesitamos para tomar esas decisiones y elaborar un plan para recolectar esa información.

La escasez de datos proviene en parte de la falta de comunicación de la información existente. Las empresas poseen la inteligencia necesaria: la forma en que afrontan los problemas, así como los éxitos y fracasos que han tenido. Pero todo el mundo es reacio a compartir sus datos de inteligencia, incluso dentro de la empresa misma. Y externamente, evitan hacerlo debido a preocupaciones en torno a su reputación y también respecto a las reglamentaciones existentes, ya que ciertos ataques pueden poner en evidencia posibles fallos en los requisitos reglamentarios.

Construir un ecosistema informático empieza por establecer relaciones y cultivar la confianza. Veo diferentes áreas en las que podemos trabajar, por ejemplo en la libre discusión sobre las mejores prácticas entre expertos de nivel similar provenientes de distintos departamentos de TI. Las empresas podrían acordar planes para compartir ciertos tipos de información entre ellas. Y otro punto importante sería la comunicación regular con los organismos reguladores, que suelen mostrarse más abiertos cuando se establece esta relación.

¿Los estados y organismos internacionales están estableciendo algún tipo de coordinación para mejorar las estrategias de resiliencia informática a nivel global en un mundo posterior a la pandemia?

Uno de los grandes retos que plantea la informática es que traspasa las fronteras, es un tema de proyección global. En muchos sentidos, es como la pandemia, y requiere de la acción conjunta de organizaciones multinacionales, organismos reguladores y agencias estatales.

> **“Nos estamos concentrando en los riesgos correctos? ¿Nuestros planes de reacción responden a las situaciones de riesgo más probables, y ha sido verificada su eficacia? ¿Contamos con un mapa de ruta de recuperación en caso de incidentes? En otras palabras, ¿cómo vamos a volver a poner los sistemas en funcionamiento?”**

Un importante punto de inflexión que hizo que las empresas empezaran a pensar seriamente en la protección de datos dentro de la informática fue la promulgación del RGPD, que se publicó originalmente en 2016: un buen ejemplo del impacto real de las regulaciones internacionales.

Los acuerdos internacionales son muy difíciles de lograr porque cada quien tiene sus propios intereses, pero actualmente parece haber cierta coincidencia de opiniones en torno al pago de rescates a las organizaciones terroristas, a diferencia de las organizaciones criminales, y sobre la relación entre la financiación del terrorismo y la ciberseguridad. Creo que en torno a esto veremos grandes cambios en los próximos años. Por ejemplo, la Oficina de Control de Activos Extranjeros de los Estados Unidos tiene una lista de personas que debe ser examinada para prevenir actividades de financiación del terrorismo. En tal sentido, las empresas deben ser extremadamente cuidadosas a la hora de pagar un rescate, a fin de estar seguros de que el receptor es “solo” una organización criminal y no terrorista. Esto es algo muy difícil de aclarar, pero a veces hay ciertas claves ocultas, como la cartera de bitcoins utilizada, o la forma en que la organización se comunica con la víctima.

Ecosistemas informáticos contra el ciberdelito

Nicolas Arpagian

Nicolas Arpagian es director de estrategias de ciberseguridad de Trend Micro. Además, es asesor del Sr. Michel Van Den Berghe, designado por el Primer Ministro francés para la construcción del Cyber Campus, un centro de ciberseguridad que reunirá a los principales agentes nacionales e internacionales del sector para unificar el desarrollo de sinergias en la comunidad de la ciberseguridad.

> “Aunque parezca algo contra el sentido común hablar sobre nuestras debilidades, el intercambio de información referente a los ciberataques resulta absolutamente esencial.”

El ecosistema informático es extremadamente extenso. En el mundo digital desaparecen las barreras físicas, y cualquiera con conexión a internet puede realizar actividades informáticas, ya sean legales o ilegales. Una parte de la población usa medios ilegales para ver canales de video o juegos de futbol, por ejemplo, sin que por eso se consideren a sí mismos hackers.

Las organizaciones internacionales han empezado a hablar de "ecosistemas informáticos" contra la industria del ciberdelito. El Foro Económico Internacional, entre otros organismos, ofrece orientaciones para mejorar la resiliencia en materia de informática, entre ellas el fortalecimiento de la "colaboración en todo el ecosistema informático", y el intercambio de información sobre ciberataques entre grupos de confianza pertenecientes a un mismo sector o una cierta cadena de la economía. Recomendaciones como esta ya se han dado con anterioridad, pero cuestiones referentes a la confidencialidad, la preocupación acerca de la propia reputación y las disparidades entre niveles de desarrollo informático han impedido el flujo de información sobre ataques informáticos. Hablar sobre sus propias debilidades no es algo que les guste hacer a las empresas, en especial cuando los nuevos compañeros del ecosistema de la seguridad informática pueden ser competidores en el ámbito comercial, como proveedores o clientes. A pesar de ello, intercambiar información sobre los ciberataques resulta absolutamente esencial en estos momentos.

Al entrar en dicho ecosistema, hay dos cosas que las empresas deben tener en cuenta. Primero, que es imposible evitar los riesgos en materia informática: la cuestión no es si se puede producir un ataque, sino cuándo se producirá. Segundo, siempre existe un "paciente cero", la primera entidad que resultará infectada. Los participantes en el ecosistema deben superar el estigma de quién es la primera víctima de un ciberataque. La creación de un entorno en el que los participantes de confianza compartan información sobre los ataques informáticos que reciban llevará a un mejor conocimiento de las perspectivas y posiciones de los ciberdelincuentes. Uno de los miembros del grupo quizás descubra que el software comercial que utiliza tiene alguna vulnerabilidad, o que esa vulnerabilidad le representa un riesgo, y seguramente sabrá que muchas otras empresas de su sector usan el mismo software, por lo que están expuestas al mismo riesgo, o quizás ya están teniendo un ataque informático.

En la práctica, hay varios factores importantes para la creación de un ecosistema informático resiliente ante los ciberataques. Antes de producirse este, las partes deben conocerse y confiar unos en otros, habrán acordado una estrategia, así como el empleo de determinados canales de comunicación confidenciales. También necesitan acordar cómo documentar el ataque de modo que la información sea útil para los demás. Para ello, lo mejor es imaginar que la víctima es otra organización, que será la que nos proporcione la inteligencia que necesitamos: quiere decir que tenemos que conocer el contexto, exactamente qué sucedió, cuáles fueron los síntomas detectados y cómo se manejó el ataque.

Un ecosistema informático va mucho más allá del mero interés económico. Requiere ver las cosas desde una perspectiva transversal, ya que algunas de nuestras herramientas informáticas son compartidas con otros sectores. Es una forma nueva de hacer las cosas.

Aunque los gobiernos no pueden implantar la creación de ecosistemas informáticos para combatir el ciberdelito, pueden incentivarla. Pueden divulgar sus beneficios, señalar las prácticas de utilidad comprobada en los distintos sectores, por ejemplo organizando grupos de confianza en los que las empresas puedan compartir información sobre las amenazas informáticas más recientes, o promover programas de formación profesional de TI en las universidades, para que todos los estudiantes puedan conocer los principales aspectos técnicos y legales de la ciberseguridad.

El ecosistema informático necesita reunir el talento humano proveniente de empresas, organismos reguladores y cuerpos estatales. La ciberseguridad necesita personal. Las administraciones civiles, los cuerpos militares, las empresas grandes y medianas, los proveedores de servicios y los cuerpos que combaten el delito, todos necesitan expertos sobre el tema. Muchos países en desarrollo enfrentan escasez de candidatos, porque no logran incorporar suficiente gente en sus programas de formación. Creo que una solución podría ser la cooptación, que refuerza los valores compartidos, en especial los valores éticos. Otra opción para las grandes empresas sería transferir a sus departamentos de ciberseguridad su propio personal de confianza que posea conocimientos y experiencia técnica. También es importante dar a conocer la variedad de funciones que existen en ciberseguridad, desde formación hasta gestión de crisis, pasando por auditoría informática, consultoría o desarrollo técnico, entre otras.

Organización y regulación del ciberespacio

Guillaume Poupard

El Dr. Guillaume Poupard es director general de la Agencia Nacional de Ciberseguridad francesa (ANSSI) desde marzo de 2014. Tras graduarse en la École Polytechnique, obtuvo su PhD en criptografía en la École Normale Supérieure en el año 2000. Fue director del Laboratorio de Criptografía del Directorio de Seguridad de la Información y la Red Central, que en 2009 fue el fundamento de la ANSSI. Se incorporó al Ministerio de Defensa en 2006, y fue nombrado director de la División de Ciberseguridad de la Sección Técnica de la Agencia de Procuraduría de la Defensa Nacional (DGA) en 2009. (©Patrick Gaillardin)

Juhan Lepassaar

Juhan Lepassaar es director ejecutivo de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) desde octubre de 2019. Antes de incorporarse a la ENISA, desempeñó diversos cargos en la Comisión Europea, entre ellos director de gabinete del vicepresidente Andrus Ansip, responsable del Mercado Único Digital. En este cargo, dirigió y coordinó los preparativos y las negociaciones de la Ley de Seguridad Informática. Juhan Lepassaar inició su carrera en relaciones de la Unión Europea en la Oficina del Gobierno de Estonia, liderando el sistema de coordinación nacional de la Unión Europea como director de relaciones y asesor del Primer Ministro para la Unión Europea.

> “Las regulaciones pueden ser parte de la solución, si se hacen de la forma correcta.”
>
> G. Poupard

Desde el espionaje al ransomware, pasando por la interferencia de infraestructuras críticas, los ataques informáticos perturban la tranquilidad de personas y empresas, así comola seguridad de Estados y las democracias.

¿Puede compararse la actual guerra informática con anteriores formas de enfrentamiento? ¿La guerra cibernética está generando un nuevo equilibrio de poderes?

Guillaume Poupard: El término "guerra" es adecuado para los conflictos informáticos, pero difiere de las guerras que conocemos del pasado. El ciberdelito incluye una variedad de formas de ataque, atacantes y víctimas. Algunos gobiernos intentan espiarse unos a otros, mientras que otros están buscando iniciar una auténtica guerra, si bien en el espacio digital. Emprender una guerra informática hoy en día es relativamente barato, dado que un ejército de atacantes puede estar compuesto de solo unos centenares de individuos. No obstante, potencias como los Estados Unidos, Rusia o China, están invirtiendo masivamente en sus arsenales de esta guerra informática, tanto en plan ofensivo como defensivo, con el objetivo principal, para cada quien, de asegurarse de ser la fuerza dominante. Y el inmenso campo de posibilidades de los ciberataques se nutre tanto de los nuevos tipos de ataque actuales como de las renovadas estrategias del pasado.

Juhan Lepassaar: En la guerra cibernética, si los diversos participantes —entre los que hay Estados soberanos, corporaciones e individuos— no cambian su actitud actual, el número de ciberataques crecerá indefinidamente. El problema de la existencia de nuevas vulnerabilidades y su impacto aparece con frecuencia cuando hablamos del cambio climático, y lo mismo sucede respecto al ciberespacio, donde todavía no hemos evaluado por completo el impacto de todas las vulnerabilidades existentes. La actitud de las personas y el funcionamiento de los procesos, los sistemas legales y los marcos de acción política que hemos construido en materia informática tienen una tremenda importancia. Todo el mundo está en capacidad de hacer algo, que puede parecer poco, pero es absolutamente necesario para resolver este problema global.

¿Cómo podemos elaborar un marco global para evitar las guerras cibernéticas?

GP: Los mecanismos existentes para controlar la apariciónde conflictos tradicionales no se aplican al mundo cibernético. Por ejemplo, un programa informático puede ser enviado por correo electrónico con fines perfectamente legales o bien como una forma de ciberataque, por lo que nuestros acuerdos y convenciones sobre la exportación de armamentos serían en este caso irrelevantes.

Actualmente se realizan esfuerzos a nivel internacional para resolver la nueva situación. Por ejemplo, el Grupo de Expertos Gubernamentales de las Naciones Unidas y el Grupo de Trabajo de Composición Abierta están discutiendo leyes y reglamentos sobre el uso del ciberespacio. Hay desacuerdos

> "La maquinaria utilizada en el ámbito informático pertenece en su mayor parte al sector privado, fuera del control estatal, por lo que tenemos que buscar marcos de naturaleza vinculante no solo para los gobiernos sino también para el sector privado."
>
> J. Lepassaar

> “La ciberseguridad es problema de todos. Desde cada persona hasta los estados, alianzas industriales y grupos de consumidores, necesitamos sembrar conciencia y establecer regulaciones.”
>
> G. Poupard

sobre muchas cosas entre los distintos países, pero existe consenso general sobre la necesidad de la discusión sobre el ciberespacio, y en que este nuevo medio no puede permanecer sin reglamentación. Como sucede con frecuencia, se trata de armonizar diferentes enfoques culturales y políticos. En Francia, por ejemplo, se habla de la “seguridad de los sistemas de información”, nunca usamos la expresión “seguridad de la información” porque para nosotros suena demasiado parecido a “control de la información”, y preferimos poner el enfoque en la infraestructura en lugar del contenido. Sin embargo, otros países establecen relaciones directas entre la seguridad de los sistemas de información, la seguridad de la información y el control de la información. Esta ha sido una de las razones principales que han limitado las discusiones internacionales hasta ahora.

JL: La maquinaria utilizada en el ámbito informático pertenece en su mayor parte al sector privado, fuera del control estatal, por lo que tenemos que buscar marcos de naturaleza vinculante no solo para los Estados sino también para el sector privado. Con todo, son los Estados, y alianzas como Unión Europea, los responsables de garantizar la aplicación en la vida real de los marcos regulatorios que se diseñen.

Es importante entender que el ciberespacio no es operado y controlado por un número pequeño y bien definido de actores, sino por una inmensa multitud, que debemos considerar en forma holística. También necesitamos entender mejor la llamada “obligación de diligencia” o el “deber de cuidado” en el ciberespacio, es decir, cuáles son las responsabilidades de cada uno de los actores involucrados.

¿Cuál es la posición de Europa para lograr una mayor seguridad en el ciberespacio?

JL: Nuestra posición es de prudencia basada en el análisis de riesgos para poder construir un ciberespacio más resiliente. Hasta ahora, nuestro trabajo se ha dirigido a los mínimos requisitos en los sectores críticos, que todo el mundo debería seguir. Pero, tal como sucede con el calentamiento global, esas medidas podrían no ser suficientes. Así que empezamos a pensar en los productos y servicios del ciberespacio, en el intercambio de información en Europa, y en el establecimiento de normativas comunes para todos los actores involucrados: qué es lo que se espera de ellos, y cómo asegurar la tranquilidad de la sociedad. Otro aspecto importante es la seguridad de los suministros: en algunas áreas deberíamos disponer de una mayor autonomía digital, mejores capacidades industriales y de investigación, y realizar mayores inversiones para asegurar que podamos construir un entorno informático con la resiliencia necesaria.

GP: La ciberseguridad es problema de todos. Desde cada persona hasta los Estados, alianzas industriales y grupos de consumidores, necesitamos sembrar conciencia y establecer regulaciones. Las regulaciones pueden ser parte de la solución, si se hacen de la forma correcta.

En la práctica, ¿cómo organizan los distintos Estados y alianzas sus capacidades de ataque y defensa en materia informática?

JL: El objetivo principal de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) es garantizar que el mercado interno se mantenga funcional, sin que resulte afectado por ciberataques. Esto requiere, entre otras cosas, la creación de capacidad informática, de modo que los participantes posean el desarrollo necesario para poder responder adecuadamente, y el establecimiento de sinergias entre los diferentes actores involucrados con la ciberseguridad a nivel de la Unión. En junio de 2021 se creó el “Centro de Competencia de Ciberseguridad para la Industria y la Investigación”, en vista del papel fundamental que tienen la investigación, la innovación y la inversión para el adecuado funcionamiento del sector.

GP: La mejor forma de organizar las capacidades informáticas difiere de un país a otro, dependiendo de su organización política, de su historia y de

muchos otros factores. En Francia, se creó la Agencia Nacional de Ciberseguridad (ANSSI) hace 12 años para contar con un organismo a nivel nacional a cargo del ciberespacio, que no fuera un servicio de inteligencia ni un cuerpo para la aplicación de la ley. En tal sentido, trabajamos con una variedad de agencias y ministerios: de justicia, militares, servicios de inteligencia, la policía, relaciones exteriores, el sector económico, el educativo… Tanto el Primer Ministro, en su función de jefe del gobierno, como el presidente, jefe de la defensa nacional, están directamente involucrados en la ciberseguridad y los asuntos relacionados con la defensa informática del país, estableciendo las prioridades y asignando los recursos necesarios. Otros países han designado "controladores del ciberespacio" a la manera de un "zar", para coordinar y representar las acciones en materia de seguridad informática. Pero en Francia, con la ANSSI como organismo interministerial, no creo que la figura de un "zar" plenipotenciario funcionara de modo eficiente.

¿Hay un buen equilibrio entre las capacidades de defensa y ataque en materia informática?

GP: En cierto sentido, la mejor defensa es la defensa misma: para protegernos, necesitamos que todas las entidades estén conectadas en el ciberespacio, ya que cualquiera puede ser el punto de entrada de un ciberataque. Pero si solo nos dedicamos a detectar y reaccionar al ciberataque, siempre estaremos un paso por detrás.

Actualmente estamos trabajando a nivel europeo para desarrollar un marco de certificación de productos y servicios desde una perspectiva de ciberseguridad. El ámbito europeo, que ofrece un mercado atractivo a los proveedores, es el más relevante en materia de protección de los consumidores.

Por otra parte, a nivel nacional es necesario desarrollar tanto inteligencia informática como capacidades ofensivas. En Francia existe una estricta separación entre ataque y defensa, porque son conceptos muy diferentes, y uno no debe ser priorizado sobre el otro. En lo que respecta a la defensa, necesitamos una industria informática capaz de proporcionar productos y servicios eficientes y avanzados. En cuanto a la capacidad ofensiva, el sector público es el único encargado de desarrollar armas informáticas, con la participación de las empresas privadas solo en la elaboración de ciertos componentes. Pero, por el momento, el desarrollo de la capacidad ofensiva pertenece exclusivamente al Estado, tanto a nivel nacional como europeo: somos totalmente opuestos a contraataques por parte de empresas privadas.

Más allá de las regulaciones y los marcos de referencia internacionales, y de las estrategias de defensa y ataque, ¿cómo podemos hacer que el mundo sea más resiliente a los ciberataques?

JL: Cuando vamos por la calle, estamos adaptando constantemente nuestro comportamiento: prestamos atención a nuestro alrededor, miramos a izquierda y derecha, no nos arriesgamos innecesariamente cuando conducimos un vehículo o salimos a dar un paseo. Lo mismo debemos hacer en el ciberespacio. Una buena defensa empieza asegurando nuestra resiliencia ante una situación disruptiva. Innegablemente, debemos partir de los principios de "seguridad por diseño" y "seguridad por omisión", no solo en lo que respecta a las infraestructuras críticas, sino también en lo referente a los nuevos productos y servicios para nuestro propio uso, y en lo que respecta a nuestro propio comportamiento.

> **"En cierto sentido, la mejor defensa es la defensa misma: para protegernos, necesitamos que todas las entidades estén conectadas en el ciberespacio, ya que cualquiera puede ser el punto de entrada de un ciberataque. Pero si solo nos dedicamos a detectar y reaccionar al ciberataque, siempre estaremos un paso por detrás."**
>
> G. Poupard

Capítulo 04

El seguro contra riesgos informáticos: un cambio de paradigma

El sector de los seguros es un factor clave en la gestión de riesgos informáticos y el objetivo de la resiliencia frente a los ciberataques. ¿Cuál es el estado actual del mercado de la seguridad informática? ¿Qué nuevos retos representan para el negocio de los seguros las nuevas tecnologías, como los vehículos conectados y los vehículos autónomos? ¿Cuáles son los problemas principales que afrontan las aseguradoras y cuáles los límites actuales que hay que superar para alcanzar el éxito?

El reto de los seguros contra riesgos informáticos

Libby Benet

Libby Benet, JD, es la directora global de suscripción de seguros de las Líneas Financieras de AXA XL. Libby es miembro de la Junta Supervisora de S-RM, consultora de inteligencia e informática global y miembro de la Junta Directiva Mutual de Abogados de Minnesota. Libby es licenciada en ciencias políticas por la Towson University y posee el título Juris Doctor de la Escuela de Leyes de la Universidad de Baltimore.

La transformación digital de nuestras economías genera una variedad de oportunidades, pero también riesgos informáticos por todas partes. Ya en 2017, la OECD calificó al sector de los seguros como un actor clave en la mejora de la resiliencia informática y la gestión de riesgos informáticos a nivel global.[1] Por otra parte, la conciencia acerca de los riesgos informáticos ha aumentado considerablemente en la población en general, que ha sido testigo de un número creciente de ciberataques durante la crisis de la COVID-19, dirigidos incluso a infraestructuras críticas como los hospitales.

> “El desequilibrio entre la oferta y la demanda está impidiendo el desarrollo del sector de los seguros.”

¿Cuáles son los retos que se presentan en el ámbito de los seguros contra riesgos informáticos?

Las tecnologías de conexión a internet no siempre han tenido la seguridad como prioridad principal, sino la innovación, que ha estado en la primera línea de las actividades comerciales. De ahí que en las empresas y en los gobiernos existan muchas vulnerabilidades que todavía carecen de una cobertura total de seguro. Si bien esto está cambiando, el número de gobiernos y de empresas que suscriben pólizas de seguros informáticos es todavía relativamente bajo en todo el mundo. En definitiva, la mayoría de las pérdidas en el área de actividades informáticas carecen actualmente de cobertura de seguros.

Por otra parte, el área de la seguridad informática está plagada de retos. Para empezar, el sector de los seguros se basa en el reconocimiento de determinados patrones de información para establecer los precios de los productos. Ante un riesgo natural, por ejemplo, disponemos de datos históricos de los patrones climáticos que nos permiten predecir las consecuencias de un huracán o un tsunami; en cambio, la información referente a la seguridad informática se remonta apenas a 10 o 12 años de antigüedad. Y el análisis de riesgos resulta aún más complejo por el hecho de que en este campo la amenaza es producida por el hombre, y está en constante evolución. Además, las conexiones e interconexiones técnicas se realizan a muy diversos niveles, cada uno con sus propias especificidades, ya sea de software, hardware, internet de las cosas, monitorización remota, y muchas cosas más.

Los modelos de acumulación en el terreno informático son todavía muy inmaduros. Tenemos un par de escenarios y modelos de siniestros realistas, pero solo se remontan a

[1] Enhancing the Role of Insurance in Cyber Risk Management [Mejorando el papel de los seguros en la gestión de riesgos informáticos], OECD, diciembre de 2017.

> **“Lo que aumenta la complejidad del análisis de riesgos desde la perspectiva de los seguros es que la amenaza cambia constantemente, además de los muchos niveles de conexión e interconexión tecnológica, cada uno de ellos con sus propias especificidades y vulnerabilidades pertenecientes al software, el hardware, el internet de las cosas, la monitorización remota y muchas cosas más.”**

unos pocos años, y no incluyen la totalidad de los posibles cambios en cuanto al comportamiento del agente y a la amenaza misma. Por otra parte, los modelos tradicionales de riesgos, como de incendio o explosión, y otros tipos de daños a la propiedad que podrían ser consecuencia de un desastre informático, todavía no han sido modelizados del todo. Estamos tan solo en los primeros días de la elaboración de modelos de acumulación.

La falta de datos y las dificultades de modelización son una fuente de incertidumbre. Estamos ante una oportunidad para el sector de los seguros, pero tenemos una seria necesidad de que los expertos en seguros y en ciberseguridad se reúnan para evaluar conjuntamente los temas y analizar el nivel de desarrollo informático de la empresa que pide la cobertura de seguro.

¿Cuáles son las tendencias principales en materia de seguridad informática?

Lo que ha sido realmente nuevo en 2021 es el desmesurado impacto de los casos de ransomware, que ocasionaron graves pérdidas el año pasado. Eso está cambiando la tolerancia al riesgo en el sector de los seguros, que este momento se encuentra en modo de reacción.

Otra tendencia muy importante es el paso de una política de “silencio” a una política de “afirmación”, es decir, de hacer explícito lo que está incluido y lo que no está incluido en la póliza. El sector de los reaseguros empezó a explorar todo esto en torno a 2015 o 2016. AXA XL hizo ese cambio de política en 2019; posteriormente Lloyd’s ordenó a sus aseguradoras utilizar pólizas explícitas, y les dio 24 meses para incorporar los cambios en los formularios. Como consecuencia, algunas reaseguradoras les preguntan ahora a sus clientes si sus pólizas son del tipo de “silencio” o “afirmativas”. Creo que esta será la corriente de actuación del sector en todas las líneas de negocios durante uno o dos años. Esto no solo afectará directamente a los propios productos informáticos sino también a aquellos que involucren riesgos informáticos en otras líneas de negocios, como los seguros de responsabilidad o de bienes inmuebles.

Por último, está creciendo a nivel global la conciencia respecto a los riesgos y las pérdidas en materia informática. Las pequeñas empresas empezarán a suscribir pólizas independientes para la cobertura de riesgos informáticos con límites más elevados, en lugar de los paquetes de seguros con riesgos informáticos incluidos.

No obstante, el desequilibrio entre la oferta y la demanda está dificultando el desarrollo del sector. En conjunto, todavía no hay capacidad suficiente, o número de compañías de seguros, para cubrir la totalidad de los riesgos en materia informática. Y por parte de las aseguradoras existe además el temor ante la posibilidad de cambios imprevistos por parte de los delincuentes informáticos…, aparte de la poca experiencia existente en cuanto a riesgos y pólizas en esta área. También se aprecia falta de experiencia en la materia por parte de actores claves, como los agentes y corredores que asesoran a las empresas. A pesar de todo esto, hay un serio compromiso por parte del sector informático para mejorar los conocimientos y la capacitación de los intermediarios.

¿Qué cosas deben saber las juntas directivas acerca de los riesgos en materia informática?

Otra limitación para el desarrollo del sector de seguros de riesgos informáticos es el conocimiento y la conciencia en cuanto al riesgo que pueda tener la dirección de la organización, y su capacidad de decidir si hacen una inversión en ciberseguridad, si adoptan una política combinada haciéndose cargo directamente de los riesgos, o si prefieren transferir esa función a una. Las direcciones de las empresas públicas suelen tener las ideas más claras que las del sector privado pero, como sucede generalmente en el ámbito informático, en este respecto son también relativamente inmaduras.

Hay varias cosas que la dirección de una empresa pública debería saber razonablemente, en materia de riesgos informáticos. Se trata de un banquillo de tres patas: por una parte están los marcos normativos, por la otra la gobernanza de la organización, y por último la evaluación del daño financiero de tener algún riesgo no controlado. La investigación sin fines de lucro realizada por el Grupo Crossroads subraya la necesidad de identificar las circunstancias que contribuyen a los riesgos informáticos de la organización, primeramente a escala local dentro de la misma, y determinar su tolerancia general a ese tipo de riesgo.[2] Ello lleva a la implementación de un plan de respuesta a riesgos informáticos con las medidas necesarias para gestionarlos, incluyendo, por supuesto, los correspondientes mecanismos de supervisión.

[2] Cybersecurity is at a Crossroads [La ciberseguridad en la encrucijada], Cyber Crossroads, mayo de 2021.

Cambio en las técnicas de modelización de riesgos para vehículos conectados y autónomos

David Williams

David Williams es director gerente de Servicios Técnicos y de Suscripción de AXA Insurance en el Reino Unido. Ha ejercido los cargos de director de Pólizas Comerciales, gerente de Reaseguros, gerente de Seguros de Accidentes, director gerente de Reclamaciones y director gerente de Pólizas. David dirige las operaciones de AXA sobre Vehículos Conectados y Autónomos, lo que incluye las operaciones con cinco consorcios de apoyo gubernamental (entre ellos Venturer, UK Autodrive y Flourish). Es presidente del Grupo de Seguros de Conducción Autónoma ABI y del Comité del Motor ABI, y presidente de RiskAuthority.

> “Para una mejor gestión de los riesgos informáticos en el sector del automóvil, necesitamos entender la forma en que el ser humano se relaciona con los vehículos autónomos y cómo interactúan estos con otros dispositivos conectados a internet.”

Todos los vehículos modernos incluyen actualmente asistencia a la conducción, unidades de control, sensores y conexión permanente a internet. Pero necesitamos anticiparnos al futuro ahora, y será un futuro de vehículos totalmente autónomos, interconectados entre sí, a los servicios de carretera y a la infraestructura.

A medida que los vehículos se vayan conectando cada vez más a su entorno exterior, aumentarán considerablemente las vulnerabilidades y, con ellas, las oportunidades de ciberataques, incluyendo, por ejemplo, amenazas a los controles del motor, los sistemas de presión de los neumáticos o las llaves de control remoto. Por ejemplo, en 2015 se produjo un ataque remoto a un Jeep Cherokee a través de su canal de conexión de controles, y el hacker se apoderó del control del sistema de frenos, entre otras cosas.[1]

El sector de los seguros está trabajando en el estudio de esta nueva clase de riesgos informáticos que afrontan los vehículos autónomos y conectados. Se trata de un reto de envergadura, ya que las compañías de seguros se han basado tradicionalmente en la información existente sobre los productos para establecer sus precios y proporcionar el servicio apropiado a sus clientes. La mayor parte de esa información son datos históricos basados en millones de casos de pólizas y de clientes anteriores, lo que les permite anticipar con bastante precisión el rendimiento general de las pólizas. Pero hoy en día, en el sector de seguros de vehículos, los datos existentes provienen de vehículos de operación manual, con poca o ninguna conectividad. Para poder incluir los vehículos autónomos en nuestras pólizas, necesitamos un cambio en la estrategia y los modelos de riesgos, que esté basado en conocimientos y sistemas de modelización científicos, más que en información proveniente de la experiencia previa.

Necesitamos saber la forma en que los vehículos estarán conectados y cómo se interrelacionarán, ya que esa es la vía de entrada para un hacker, y conocer en detalle los sistemas autónomos y la tecnología que utilizarán, ya que ello nos permitirá estar al tanto de los posibles riesgos. Porque, por ejemplo, un ciberataque a un sistema de frenos automatizado no solo afecta a los pasajeros del vehículo sino también, muy probablemente, a otros usuarios de la vía; y un sistema de navegación hackeado podría llevarnos, quizás con seguridad… a un destino no deseado.

Ahora bien, debido a la gran cantidad de módulos de control y microprocesadores que utilizarán, los nuevos vehículos podrán tener unos 100 millones de líneas de codificación repartidas en unas 50 unidades de control del motor, o quizás más. En la práctica, es muy probable que algunas vulnerabilidades pasen inadvertidas, porque revisar detalladamente todos los códigos y realizar todas las evaluaciones de seguridad sería impracticable; y esas vulnerabilidades pueden terminar por poner en peligro alguno de los mecanismos de control del vehículo. Por ejemplo, un ataque a la red de sensores del vehículo podría falsear los datos de un sensor, o afectar directamente a los módulos de control. Evaluar adecuadamente los puntos vulnerables para gestionar y para asegurar los correspondientes riesgos informáticos, implica conocer el diseño del vehículo, las funciones de cada componente en particular y las interacciones entre los componentes.

Los futuros vehículos inteligentes estarán cada vez más conectados a internet, adaptados para aceptar actualizaciones automáticas, además de que actuarán como puntos de conexión wifi y se comunicarán a través de la red con otros dispositivos, como vehículos e infraestructuras. En otras palabras, los mayores riesgos están aún por llegar.

Pero, además, los vehículos serán también el punto de entrada a muchos otros vehículos y a la infraestructura en su conjunto, lo que significa que un hacker que logre acceso físico o remoto a un vehículo podría utilizarlo como punto de partida para causar perturbaciones aún mayores. Y, dado que existe la posibilidad de acceso físico, retirar la conexión a internet o privar de acceso remoto a un vehículo no elimina el riesgo por completo mientras los vehículos sigan interconectados. Por eso, los sistemas de seguridad clave para proteger contra ciberataques los vehículos conectados y autónomos serán probablemente una combinación de criptografía, detección estadística de anomalías y soluciones integrales de software.

Con mucha de esta tecnología todavía en fase de prueba, las aseguradoras se esfuerzan por reunir datos que puedan incorporar a sus modelos habituales de precios basados en los riesgos. Para subsanar la falta de información, las compañías de seguros se están involucrando directamente en las tareas de desarrollo, a fin de lograr una mejor comprensión del tema. Por ejemplo, la Asociación Británica de empresas de seguros ha creado el “Grupo de Seguros de Conducción Autónoma”, para establecer enlaces con los fabricantes de motores a fin de recibir información sobre nuevas tecnologías y realizar pruebas en el terreno. La información y los datos obtenidos del trabajo en estas áreas nos permitirá elaborar modelos analíticos, con el auxilio de la IA y el aprendizaje automático. De este modo esperamos estar preparados para cuando estos vehículos sean más comunes en el mercado. Los vehículos conectados y autónomos son un fenómeno global, y el intercambio de información a nivel internacional facilitará el proceso, por ejemplo, mediante el uso de recursos como la Base de Datos Nacional de Vulnerabilidades de los Estados Unidos. Por otra parte, organismos como el Instituto de Investigaciones Thatcham sobre Vehículos de Motor, en el Reino Unido, o el Centro de Pruebas de Colisiones de AXA, en Suiza, pueden facilitar la experiencia práctica necesaria.

Para finalizar, y a pesar del importante enfoque en tecnología, muchos expertos piensan que el eslabón más débil en lo que respecta a los ciberataques de vehículos conectados y autónomos sigue siendo el elemento humano. La actitud del usuario es clave ante situaciones que pueden ir desde un fallo en un sistema operativo hasta una interferencia en las comunicaciones externas, pasando por la manipulación de equipos o el retraso en la instalación de actualizaciones de seguridad. La actitud y la atención del usuario, junto con un mejor equilibrio entre el conocimiento de los últimos avances en tecnología y la forma en que los aplicamos, son requisitos necesarios para que podamos asegurar los vehículos autónomos y conectados.

[1] Hackers Remotely Kill A Jeep on The Highway [Hackers desactivan un jeep a distancia en la autopista], Wired, julio de 2015.

Acumulación, dependencia y construcción de escenarios extremos: precondiciones del seguro contra riesgos informáticos

Caroline Hillairet

Caroline Hillairet es profesora en el ENSAE de París, donde está a cargo del programa actuarial. Es miembro del Centro de Investigaciones Económicas y Estadísticas (CREST) y del Laboratorio de Finanzas y Ciencias Actuariales (LFA). Además, es miembro del Comité del Instituto de Actuarios de Francia y codirectora de la Iniciativa de Investigación Conjunta de AXA para la modelización actuarial de riesgos informáticos.

Olivier Lopez

Olivier López es profesor en la Universidad de la Sorbona y director de su Instituto de Estadística (ISUP). Es miembro de pleno derecho de la Asociación Actuarial Francesa (Institut des Actuaires), miembro de su Comité Científico, y miembro representante del Comité de Educación de la Asociación Actuarial Europea. También es codirector de la Iniciativa de Investigación Conjunta de AXA para la modelización actuarial de riesgos informáticos.

> **“Los seguros se basan en la anticipación de eventos futuros. En el caso de riesgos en los que el comportamiento de los actores involucrados es tan importante y los cambios tan rápidos, solo un cuidadoso análisis de los eventos informáticos puede permitirnos anticiparnos a los hechos en lugar de tener que soportar las consecuencias.”**

Los ciberataques aumentaron en forma considerable en 2020 y 2021, en particular los ataques de ransomware, y no parece que esto vaya a detenerse en un futuro inmediato. Actualmente, la mayoría de los sistemas de información están interconectados y presentan deficiencias similares, lo que intensifica la condición sistémica de los riesgos informáticos.

En este contexto, la asegurabilidad del riesgo informático depende de nuestra capacidad de modelizar los ciberataques de modo que podamos integrar sus complejos efectos dependientes. Mientras que los modelos de seguros tradicionales asumen que los reclamos se presentarán en forma independiente, esta asunción resulta inadecuada para representar los eventos informáticos, que tienden a aparecer en grupo e interrelacionados. Por el contrario, los modelos alternativos más recientes[1] permiten representar el efecto multiplicador de estos eventos así como sus interacciones. Estos modelos también permiten parametrizar las características de los eventos, por lo que pueden modelarse y compararse una variedad de eventos junto con su frecuencia, y representar asimismo su impacto y la posterior perturbación remanente que constituye el "contagio del ataque".

Otra preocupación de importancia, aparte de la frecuencia de los ciberataques, es el potencial sistémico de una "tormenta informática". En 2017, el ataque del ransomware Wannacry[2] contagió a más de 300 000 ordenadores en más de 150 países. Tales ataques masivos pueden ocasionar un diluvio de reclamaciones y generar altos costes, aun cuando cada reclamación en particular no sea muy elevada, lo que tiende a socavar el principio de mutualización que sostiene el sector de los seguros. De hecho, en un escenario "acumulativo" de tal naturaleza, muchos asegurados son víctimas del ataque al mismo tiempo, lo que podría llevar a una saturación de la capacidad de respuesta de las aseguradoras, dado que los contratos de seguridad informática contemplan por lo general la rápida intervención de equipos de expertos para asistir al titular del seguro durante la crisis. La incapacidad de la compañía de seguros de responder apropiadamente en un tiempo breve produce pérdidas adicionales (sanciones financieras, pérdida de reputación, además de que incrementa los daños para el asegurado). No obstante, existen metodologías generales[3] para el diseño de situaciones de acumulación, la medición de la capacidad de respuesta de la aseguradora y la elaboración de estrategias de seguros que permitan lidiar con una tormenta informática.

Además, cada reclamación en concreto podría tener consecuencias desastrosas. Debido a la fuerte dependencia del sector económico respecto a los sistemas informáticos, un ataque malicioso puede causar muy graves daños. Tendría una alta probabilidad de ocurrir lo que los estadísticos llaman una "reclamación extrema", como muestran los casos de sustracción de datos.[4] En una situación así, la mutualización puede fallar, dado que incluso podría no ser posible, matemáticamente hablando, definir el valor medio de una reclamación, un concepto que sustenta el principio de determinación de precios del seguro.

En consecuencia, para hacer viable la contratación de seguros informáticos, el único recurso es rediseñar el perímetro del contrato de seguro. La especificación de límites y condiciones de las reparaciones financieras reduce la incertidumbre para la empresa aseguradora, y permite realizar la gestión del riesgo. Ahora bien, a medida que prevalecen escenarios más extremos, se incluirán más restricciones, con lo que disminuirá la calidad de la cobertura, lo que, desde luego, va en detrimento del asegurado, y el contrato ya no será tan atractivo, lo que perjudica a la aseguradora, que podría no conseguir clientes suficientes para asegurar su mutualización. Pero mediante técnicas científicas de tratamiento de la información y herramientas estadísticas avanzadas provenientes de la teoría del valor,[5] será posible comprender los factores que desembocan en la incidencia de tales reclamaciones "extremas" en materia informática, incluyendo, entre otras cosas, el comportamiento de la víctima o su sector de actividad, así como el tipo de ataque. Se trata de herramientas adaptables que permiten trazar una línea entre lo que puede o no puede figurar en un contrato de seguro, y de este modo mejorar la cobertura adaptándola al perfil particular del cliente.

Pero las metodologías, por eficientes que sean, deben alimentarse de la información adecuada. Una de las principales dificultades actuales de la modelización de riesgos informáticos y la asegurabilidad es la carencia fundamental de bases de datos consistentes. Resolver este problema es una tarea colectiva que requiere atención por parte de las compañías de seguros, los gobiernos, el sector privado y, de manera general, todos los actores económicos. Desde esta perspectiva, el reciente estudio "Lucy"[6] es una iniciativa prometedora, un primer intento de realizar un estudio estadístico riguroso basado en la recolección de datos de los corredores de seguros en Francia.

Los seguros se basan en la anticipación de eventos futuros. En el caso de riesgos en los que el comportamiento de los actores involucrados es tan importante y los cambios tan rápidos, solo un cuidadoso análisis de los eventos informáticos puede permitirnos anticiparnos a los hechos en lugar de tener que soportar las consecuencias.

[1] Multivariate Hawkes Process for Cyber Insurance [Procesos de Hawkes multivariantes para seguros informáticos], Y. Bessy-Roland, A. Boumezoued, C. Hillairet, Annals of Actuarial Science, 2020.

[2] What Is Wannacry Ransomware and Why Is It Attacking Global Computers? [¿Qué es el ransomware Wannacry y por qué está atacando ordenadores en todo el mundo?], Alex Hern y Samuel Gibbs, The Guardian, 12 de mayo de 2017.

[3] Propagation of Cyber Incidents in An Insurance Portfolio: Counting Processes Combined with Compartmental Epidemiological Models [Propagación de incidentes informáticos en la cartera de seguros: procesos de conteo en combinación con modelos epidemiológicos compartimentales], C. Hillairet, O. López, Scandinavian Actuarial Journal, 2021.

[4] Heavy-Tailed Distribution of Cyber Risks [Distribución de cola pesada de los riesgos informáticos], T. Maillart, D. Sornette, The European Physical Journal B, 2010.

[5] Cyber Claim Analysis Through Generalized Pareto Regression Trees with Applications to Insurance Pricing and Reserving [Análisis de riesgos informáticos mediante árboles de regresión generalizada de Pareto con aplicaciones a los precios y reservas de seguros], S. Farkas, O. López, M. Thomas, Insurance: Mathematics and Economics, 2021.

[6] LUCY: LUmière sur la CYberassurance [LUCY: Luz sobre los seguros informáticos], AMRAE, 2021.

Capítulo 05

Escenarios y tendencias futuras

¿Cuáles serán las amenazas informáticas de la próxima década? ¿Cómo pueden la ciencia ficción y la previsión estratégica ayudarnos a prever cómo será la resiliencia informática del mañana? ¿Y cuáles dicen los expertos que serán las tendencias regionales futuras en materia de informática?

Previsión estratégica y ciencia ficción para una mejor comprensión de las amenazas futuras

Olivier Desbiey

Olivier Desbiey es economista de profesión y explorador por vocación de las intersecciones entre la tecnología, los cambios sociales y las políticas públicas. Como analista sénior de previsión de AXA, explora el horizonte de las tendencias emergentes así como los indicios más tenues para fundamentar de manera segura las iniciativas inmediatas dentro de perspectivas a largo plazo.

> “La ciencia ficción crea una visión de los futuros problemas cibernéticos de manera complementaria a la de los instrumentos de predicción tradicionales.”

Las principales tendencias actuales sugieren que las tecnologías digitales van a seguir jugando un papel destacado en nuestras vidas. ¿Significa esto que la sociedad se verá expuesta necesariamente a amenazas informáticas cada vez mayores?

Dentro de la previsión estratégica, se estima que la capacidad de contrarrestar un ataque informático futuro dependerá de tres aspectos, los cuales reflejan la situación de las tendencias emergentes y las áreas de incertidumbre. En primer lugar, las tendencias actuales más marcadas, como las tensiones geopolíticas o la rivalidad entre los estados y entre las empresas tecnológicas. Segundo, las situaciones o actitudes generadoras de cambios, como por ejemplo los enfoques de seguridad y privacidad por diseño, y el conocimiento cada vez mayor de las distintas formas de ciberataques. En tercer lugar, ciertas tensiones de importancia sobre el doble sentido del uso de la tecnología y la forma en que el ser humano se relaciona con las herramientas tecnológicas.

Esta diversidad de fuerzas puede dar lugar a una variedad de situaciones. Un suceso tipo “cisne negro”, de baja probabilidad de aparición pero de importantes consecuencias, podría desencadenar una mayor y súbita toma de conciencia de estos problemas. Por ejemplo, un “bloqueo digital” originado por un incidente informático a nivel global podría cambiar nuestra actual manera de pensar sobre el futuro. No obstante, para muchos especialistas, el elefante informático ya está en la habitación, y algunas

> **“El género cyberpunk de la ciencia ficción, como la llamada literatura de clima ficción, emplea todo el poder persuasivo de la narración para sembrar conciencia sobre cosas que verdaderamente están en juego.”**

de sus principales consecuencias por venir ya se revelan claramente… en la ciencia ficción.

La ciencia ficción nos ayuda a construir una visión de los futuros problemas cibernéticos. En la literatura y en el cine, el género cyberpunk[1] ya nos está mostrando lo que las tecnologías informáticas y cibernéticas nos pueden traer en las próximas décadas.

Lo que está sucediendo en el ciberespacio torna borrosos los límites entre la realidad y el mundo virtual. Una ruptura típica de esa frontera es la conexión directa del cerebro humano con un sistema informático como el que aparece en la película Matrix, en la que el héroe, Neo, intenta liberar a los humanos atrapados en una realidad virtual a través de cables que conectan sus cerebros a máquinas inteligentes; por otra parte, la fusión del cuerpo humano con diversos dispositivos tecnológicos da origen a la figura del cyborg, organismo cibernético del que el célebre T-800 es un ejemplo en la película Terminator. Hay ficciones cyberpunk que se desarrollan en mundos distópicos en los que la conectividad de la internet a través de gigantescas computadoras da paso a la corrupción o la guerra entre organizaciones, empresas y estados, y donde grandes corporaciones multinacionales tienen el poder de cambiar gobiernos y centros de poder político, económico o militar. En estos mundos distópicos, la figura del hacker aparece muchas veces como el salvador, contrariamente a la imagen negativa del oscuro ciberdelincuente que acecha en la oscuridad de la web, como se revela en el mundo de hoy.

La corriente cyberpunk nos plantea una visión extrema de los problemas que enfrentamos actualmente: el mundo dominado por programas informáticos, la guerra cibernética como más barata y fácil de hacer que la guerra física, y el ser humano sobrepasado por las máquinas que él mismo ha creado. La ciencia ficción también desarrolla y destaca otros problemas muy serios como la contaminación, el cambio climático, la superpoblación o los desequilibrios originados por el dominio de las máquinas.

Desde la irrupción de la COVID-19, la mayoría de los expertos en previsión describen un “mundo pospandemia” caracterizado por una serie de crisis complejas y recurrentes,[2] que plantea la cuestión de cómo debemos pensar en el futuro y sus riesgos emergentes. El problema de los riesgos informáticos ilustra esta incertidumbre y complejidad, a la vez que revela las limitaciones de las herramientas de predicción tradicionales cuando el futuro se proyecta como una continuación lógica del presente. En cambio, la ciencia ficción como instrumento de previsión estratégica nos permite anticipar futuros riesgos informáticos mediante ideas que no tendrían cabida dentro de los marcos de pensamiento habituales, y nos ayuda a tomar conciencia y prepararnos ante situaciones futuras.

Las investigaciones revelan que los escenarios planteados por las obras de clima ficción pueden ejercer un notable efecto positivo sobre el conocimiento y la actitud del lector frente al cambio climático, incluido el hecho de que el calentamiento global causará más desastres naturales y pobreza en el mundo, y pueden modificar el grado de preocupación del lector, la importancia que atribuye al hecho, y su percepción de que el calentamiento global le afectará personalmente, así como a las generaciones futuras.[3] Muchos de esos efectos pueden plantearse mediante mecanismos de persuasión narrativos, que sumergen al lector en el mundo de la historia y estimulan su identificación con los personajes.

A veces se recurre a los autores de ciencia ficción por su capacidad de imaginar y describir peligros futuros que pueden amenazar a la sociedad, como ejemplifica el proyecto “Red Team”[4] del ejército francés, conformado por autores de ciencia ficción cuya misión es aportar ideas novedosas que ayuden a prevenir situaciones disruptivas y anticipar, por ejemplo, la forma en que grupos terroristas o potencias hostiles podrían utilizar en el futuro tecnologías informáticas y cibernéticas avanzadas.

El recurso del relato y la representación de escenarios disruptivos pueden ayudar a cambiar creencias y actitudes respecto a la ciencia y los problemas ambientales, despertar la conciencia y anticipar amenazas futuras para las que tenemos que empezar a prepararnos ahora mismo. El siguiente artículo hace precisamente eso.

[1] Science Fiction in the Eighties [La ciencia ficción de los años ochenta], Gardner R. Dozois, The Washington Post, 30 de diciembre de 1984

[2] 2020 Strategic Foresight Report, Charting the Course Towards A More Resilient Europe [Informe de previsión estratégica 2020: Orientando el rumbo hacia una Europa más resiliente], Comisión Europea, 2020.

[3] Reading Environmental Literature Can Persuade on Climate [La literatura sobre problemas ambientales puede persuadir sobre el cambio climático], Gustavson et al., Programa de la Universidad de Yale para la comunicación sobre el cambio climático, 2020.

[4] The French Army is Hiring Science Fiction Writers to Imagine Future Threats [El Ejército francés recluta autores de ciencia ficción para imaginar amenazas futuras], Andrew Liptak, The Verge, 24 de julio de 2019.

Anticipando el futuro de los ciberataques: relatos futuristas y precauciones para la vida real

Cécile Wendling

La Dra. Cécile Wendling es directora del Grupo de Conciencia y Seguridad Estratégica de AXA. Antes de ocupar este cargo, dirigió el Grupo de Previsión de AXA y fue investigadora asociada del Centro de Sociología de las Organizaciones (CNRS — Ciencias, Institut d'Études Politiques de París) en el área de sociología de riesgos y catástrofes. Posee un PhD en gestión de crisis en la UE por el Instituto Universitario Europeo, y es profesora de métodos de predicción y de gestión de riesgos y crisis, entre otras materias.

Mathieu Cousin

Mathieu Cousin dirige las actividades de Previsión de Amenazas del Grupo de Seguridad de AXA desde el 1° de enero de 2020. Antes de incorporarse al Grupo de Seguridad de AXA en agosto de 2016 como investigador de seguridad dentro del equipo de Estrategia, Arquitectura e Investigación, Mathieu ejerció cuatro años como analista de investigaciones e investigador de seguridad.

Lou-Anne Ducos

Lou-Anne Ducos es estudiante del máster en ciencias en el Institut d'Études Politiques de Saint-Germain-en-Laye, donde cursa relaciones internacionales, y es pasante como analista de seguridad en el equipo de anticipación de amenazas del Grupo de Seguridad de AXA desde marzo de 2021.

“La información falsa sobre ciberataques pone en peligro a las redes sociales multinacionales, actualmente acusadas de estar bajo control gubernamental”

4 de diciembre de 2023

Estás sentada en tu espacio al aire libre, tratando de finalizar tu cometido lo antes posible para ir a recoger a tus niños al colegio. Pero te es imposible concentrarte. Los teléfonos zumban constantemente, todo el mundo murmura a tu alrededor, y te sientes como si estuvieras en un patio de recreo. Molesta, decides irte a casa a terminar tu tarea. Por el camino te encuentras con un compañero de trabajo: “¿Has oído la noticia?”, te pregunta. Tú no tienes ni idea de lo que habla, pero echas una mirada a tu teléfono y, súbitamente, todo cobra sentido: Facebook, Instagram, Twitter, TikTok… Las redes no paran de hablar de tu empresa.

Un conocido grupo de ciberdelincuentes ha anunciado que ha hackeado tu sistema y que tiene acceso a toda la información de tus clientes. Y presenta pruebas de ello en las redes sociales. Los hackers te están dando 24 horas para pagar el rescate antes de que hagan pública toda la información que poseen. Es una auténtica pesadilla: has pasado los últimos seis meses trabajando en esta gigantesca fusión empresarial y ahora, con la luz verde de los reguladores, tienes casi a punto la importante operación que cambiará la economía del país. La empresa conoce el tema de los ciberataques y debería estar preparada, en especial en estos momentos tan importantes. Irritada, decides buscar más información. Compruebas que tu liderazgo sigue siendo unánime: la empresa no ha sido víctima de ningún ciberataque. La noticia, simplemente, es falsa. Aliviada, piensas que el departamento de relaciones públicas se encargará de desmentirlo.

Pero es demasiado tarde, y las acciones de la compañía ya están cayendo en la bolsa. La primera respuesta oficial declarando que “La empresa está investigando cualquier posible filtración de datos”, y la segunda, señalando que las supuestas “pruebas” esgrimidas por los hackers eran falsas, han pasado desapercibidas. Nadie está prestando atención, y el miedo prevalece sobre la razón. Finalmente, cuando se cumple la hora límite para el pago del rescate y los hackers no toman ninguna represalia, la gente se da cuenta de que todo era mentira. Pero la situación ha representado un alto costo para la compañía, y ahora tu negocio de fusión está en peligro.

El gobierno, que te había dado su apoyo en esta fusión empresarial, decide que no pueden volver a pasar cosas como esta y, como primer paso, impone medidas restrictivas a todas las redes sociales para evitar que pueda producirse una serie de eventos semejantes. Como resultado, muchos usuarios se encuentran, sin previo aviso, con que sus cuentas han sido cerradas. Y, a pesar de que comprendes las razones que motivan la imposición de estas nuevas medidas más estrictas que las existentes hasta ahora, en la noche te acuestas pensando en qué va a pasar ahora con tu apreciada libertad de expresión.

[1] EU Terrorism Situation & Trend Report (Te-Sat) [Informe de la UE sobre la situación del terrorismo y sus tendencias (Te-Sat)], 2021.
[2] Russia Used Social Media for Widespread Meddling in U.S. Politics: Reports [Rusia utilizó las redes sociales para una intervención masiva en la política norteamericana: Informes], Mark Hosenball, Reuters, 17 de diciembre de 2018.
[3] Calculating the Reputational Cost of Cyber Security Breaches [Cálculo de los costos sobre la reputación ocasionados por la sustracción de datos informáticos], Barclay Simpson, 26 de abril de 2018.

En la vida real…

Una situación como esta podría darse actualmente, en cualquier momento, y no nos extrañe que suceda algo así en los próximos años, o incluso solo meses. De hecho, la desinformación se está convirtiendo en una seria preocupación tanto para los gobiernos como para el sector privado.

Europol ha señalado que en las redes sociales está aumentando “la proliferación de desinformación y de teorías conspirativas”.[1] Como ejemplo, baste recordar los recientes ciberataques provenientes de Rusia que utilizaron las redes sociales para influir en las elecciones norteamericanas[2], lo que pone de relieve la creciente influencia que pueden tener estas plataformas en las opiniones y el comportamiento de la gente. Por otra parte, los ciberataques producen importantes costos indirectos, también llamados blandos, además de los costos directos que ocasionan (como perjuicios a determinadas marcas, y pérdidas de confianza por parte de los clientes, asociados e inversores). Desde 2016, la encuesta global del Instituto Ponemon sobre filtraciones de datos señala que el coste promedio de los daños a la reputación representa más del 40 por ciento de todos los costes ocasionados.[3]

Para limitar el impacto de las noticias falsas, los riesgos a la reputación han empezado a formar parte de la estrategia y la planificación, incluyendo, por ejemplo, la monitorización de las redes sociales para detectar prontamente cualquier intento de desinformación, la elaboración de planes de comunicación, que pueden contemplar un control centralizado de todos los canales de comunicación del usuario, y la disposición de medios al alcance del público y de la prensa para que puedan ser verificados los mensajes y declaraciones oficiales.

Las noticias falsas afectan también a las personas particulares, con diversas y variadas consecuencias. En estos momentos, la toma de conciencia al respecto es una de las herramientas clave para combatirlas.

"Por motivo del cambio climático, se cierra el sistema de asistencia sanitaria en todo el país"

15 de septiembre de 2022

Han pasado 45 minutos desde que llegaste a la sala de espera del médico. Ya has leído todas las revistas que hay allí, y decides echar un vistazo a tu teléfono móvil para ver las últimas noticias. Protestas contra la reforma laboral… Bajo crecimiento económico… Por último, te pones a leer un artículo sobre desastres naturales. Extensos incendios destruyen edificios enteros en la zona del oeste, inundaciones seguidas por un huracán devastador en el este… Nada para sorprenderse demasiado, piensas, ya que el cambio climático está ocasionando desastres en todas partes.

Finalmente llega el médico, y poco después entras al consultorio. Enseguida notas que no está de buen humor. El médico te comenta que desde esa mañana no consigue acceso a ninguno de sus registros, y que todo el sistema de salud está colapsado. "¿Cómo es posible?", le preguntas. Y él empieza a hablar de los desastres naturales y los centros de datos. En un momento dado lo interrumpes porque no consigues ver la relación entre los desastres naturales y la desaparición de tu información médica. Tu doctor te pregunta si te has enterado de los incendios en el sector suroeste y del reciente huracán que destrozó la costa este, y le respondes con cierta presunción que acabas de leer un artículo que habla de las infraestructuras afectadas en todo el país. Pero, claro, no esperabas que una de esas infraestructuras, precisamente la que alberga un importante centro de datos, hubiera quedado destruida, impidiendo que toda una región del país pudiera acceder a su información médica; y por primera vez te das cuenta de cómo depende nuestro mundo digital de nuestras estructuras físicas.

En realidad, el hecho representa un incidente menor para ti, pero no puedes dejar de pensar en la gente que estará necesitando asistencia médica urgente, y en las terribles consecuencias que puede tener ese incendio para ellos y para los equipos médicos. ¿Qué vamos a hacer en caso de que todas nuestras actividades más importantes queden sin conexión en cualquier momento debido a un problema físico?

"Hackers se apoderan de millones de dólares mediante ciberataque a banco con Inteligencia Artificial de creación casera"

21 de junio de 2028

Nada te destinaba a hacerlo, pero la crisis económica, el desengaño y la necesidad de mantener a tu familia pusieron ante ti una oportunidad que no podías dejar pasar. Al principio, cuando tu amigo te mencionó la posibilidad la rechazaste, pensando que no tenías ninguna de las cualidades requeridas en materia de informática para esa clase de trabajo, pero él te aseguró que sería fácil, y tenía razón. Ahora estás ganando más de lo que jamás habías imaginado, mediante ciberataques a las empresas donde está el dinero.

Gracias a la inteligencia artificial, los ciberataques se realizan de forma automatizada, y el nivel de habilidades necesarias para lanzar un ataque es muy elemental. Algunos individuos que encontraste en la dark web te dieron las herramientas apropiadas. Ahora formas parte de un equipo de treinta, cada uno especializado en una cosa, y apenas notas la diferencia con tu anterior trabajo. Hoy, tu objetivo es usar una potente herramienta de IA contra una empresa bancaria. Sabes que te vas a encontrar con su sistema de "detección y respuesta de puntos terminales" que, en teoría, detecta directamente las amenazas al sistema informático, pero no te preocupa porque tu herramienta tiene la capacidad para eludir esa barrera, ya que puede detectar rápidamente cualquiera de las muchas debilidades del sistema del seguridad que habrán pasado desapercibidas para el fabricante del software y el proveedor del servicio, las llamadas "zero days", que tú podrás aprovechar para inutilizar el sistema de protección bancario. La IA de que dispones,

En la vida real…

Una situación como esta puede haberse producido realmente, y podría volver a pasar en los próximos años, o incluso tan solo meses. Nuestras infraestructuras críticas están bajo la amenaza de ataques maliciosos, como el ataque de ransomware que tuvo lugar en mayo de 2021 contra una de las principales tuberías de distribución de petróleo de los Estados Unidos[4], o el dirigido a los servicios de salud en Irlanda,[5] además de que ya están bajo la amenaza física de los efectos del cambio climático. El número creciente de desastres naturales ha llevado al Foro de Seguridad de la Información (ISF) a señalar como una de las mayores amenazas para 2022 la posibilidad de "interrupciones y daños de importancia en los sistemas y dispositivos de TI como consecuencia de un desastre natural".[6] En tal sentido, los casos de desconexiones y ataques contra infraestructuras críticas, interconectadas e informáticas, se harán más frecuentes, y deben ser atentamente mitigados.

Aparte de las necesarias medidas proactivas a nivel global para combatir el cambio climático, la adecuada gestión de las infraestructuras críticas y los mismos usuarios pueden reducir el impacto de los riesgos naturales e informáticos mediante medidas de seguridad para los accesos remotos, utilizando, por ejemplo, sistemas de protección en los puntos terminales, buenas prácticas de seguridad y del empleo de contraseñas, teniendo un inventario preciso y actualizado de los dispositivos, y monitorizando por si surgen anomalías. La información puede reproducirse para almacenarla en diferentes ubicaciones y así evitar la pérdida de datos, como puso de relieve el incendio que en marzo de 2021 afectó a las instalaciones de servicios en la nube de OVHcloud, en Francia.[7]

En la vida real…

Una situación como esta podría producirse realmente en los próximos años, o incluso solo meses. La IA permite formas de ataque muy diversas, desde el diseño mismo del ciberataque, pasando por procedimientos extremadamente rápidos de extracción de información, hasta la simulación de comunicaciones programadas y el enmascaramiento del propio ataque durante su realización.

Pero la IA también ofrece herramientas de vigilancia contra ciberataques, desde procedimientos de escaneo y análisis a respuestas automatizadas para contener el ataque inmediatamente. La mejora continua de los sistemas de seguridad informática y el escaneo en busca de posibles vulnerabilidades contribuyen también a limitar el impacto de un ciberataque de IA. Actualmente se están implementando ecosistemas informáticos en diversos sectores y cadenas de la economía para facilitar el intercambio de información sobre ciberataques.

además, acelerará tu ataque gracias a sus procesos automatizados, por lo que normalmente sueles terminar temprano tu jornada de trabajo.

Todo lo que tienes que hacer es lanzar el ataque, y la inteligencia artificial hará el resto. Es un enfrentamiento entre dos sistemas de IA. Finalmente, tu ataque tiene éxito. Encontraste cinco puntos vulnerables, que aprovechaste para apoderarte de la información, que ahora podrás vender, o utilizar para lanzar nuevos ciberataques. Nunca pensaste que el manejo de datos te haría rico, pero ha resultado ser toda una mina…

"Ciberataque cuántico destruye las pretensiones de empresa automovilística de dominar el mercado – "Había muy mala preparación", sentencian los expertos"

5 de noviembre de 2031

Mañana es el gran día para tu equipo de trabajo: es el día en que la compañía lanzará su nueva serie de automóviles equipados con tecnología punta, adelantándose a toda la competencia. Después de años de trabajo técnico, ha llegado la hora de celebrar el resultado, y bromeas con tus compañeros del equipo técnico sobre los millones que vas a ganar. Hoy es un gran día para todos, y nada puede estropearlo.

Uno de tus compañeros se te acerca apresuradamente. El director quiere hablar contigo lo antes posible: tu principal competidor acaba de anunciar su nuevo modelo de automóvil, en todo similar al que acabas de desarrollar. Te parece imposible de creer. Has estado trabajando con el mayor secreto durante los últimos 15 años para desarrollar la nueva tecnología. ¿Cómo han podido desarrollar otros exactamente el mismo modelo de automóvil, y lanzarlo al mercado justo un día antes de que lanzaras la nueva serie? Las llamadas urgentes del departamento técnico se acumulan en tu teléfono, y finalmente no tienes otro remedio que aceptar la realidad. Furioso, convocas a todo tu equipo: "¡Nos han estado espiando! ¿Cómo ha podido pasar?"

Desconcertado, uno de tus empleados responde que toda la información confidencial estaba encriptada, siguiendo los procedimientos de seguridad. Al fondo, un joven pasante del departamento de TI se muestra visiblemente incómodo. Le preguntas qué opina de todo eso, y él expone la forma en que los técnicos de la competencia pudieron haber descifrado los protocolos criptográficos y los algoritmos utilizados mediante computación cuántica. Y termina diciendo que al principio de su pasantía le sorprendió mucho ver que no empleaban ningún procedimiento de codificación de datos resistente a la tecnología cuántica.

Entonces recuerdas que, por supuesto, unos meses atrás habías oído hablar de algoritmos de encriptación a prueba de descodificación cuántica, pero era algo muy costoso y, de todos modos, pasarían por lo menos unas dos décadas antes de que la tecnología cuántica pudiera llegar a ser una amenaza. Hace un par de años, el centro de datos de tu proveedor de TI fue víctima de un robo, y algunos de tus servidores estuvieron entre los muchos dispositivos físicos que fueron sustraídos. Pero gracias a que habías tenido la precaución de guardar duplicados de tus archivos en centros de respaldo en otros lugares, tus operaciones no resultaron afectadas, y en ese momento tus investigadores y asesores te aseguraron que cualquiera que intentara descifrar la información encriptada en esos archivos tardaría por lo menos unos 100 años en conseguirlo. Creer en esa afirmación fue un error, que ahora te está costando 15 años de trabajo y perder la ventaja que habías logrado sobre la competencia.

[4] Pipeline Attack Yields Urgent Lessons About U.S. Cyber Security [Ataque a red de distribución arroja inesperada lección sobre ciberseguridad en los Estados Unidos], The New York Times, 14 de mayo de 2021.

[5] Irish Cyber-Attack: Hackers Bail Out Irish Health Service for Free [Ciberataque en Irlanda: Hackers liberan el Servicio de Salud irlandés sin cobrar el rescate], BBC, 21 de mayo de 2021.

[6] ISF, Threat Horizon 2022: Digital and Physical Worlds Collide [ISF – Panorama de riesgos informáticos 2022: El choque entre los mundos físico y digital], ISF.

[7] Millions of Websites Offline After Fire at French Cloud Services Firm [Millones de sitios web desconectados por incendio en centro francés de servicios en la nube], Reuters, 10 de marzo de 2021.

En la vida real…

Los expertos no están de acuerdo en cuándo se resolverán los diversos problemas que plantea la computación cuántica de modo que pueda estar disponible para uso público, pero la tecnología cuántica podría empezar a dar sus frutos quizás dentro de unos 10 años.

Las importantes consecuencias que tendrá la computación cuántica para la ciberseguridad nos obliga a prepararnos para ello ahora mismo, ya que en estos momentos ciertos algoritmos y dispositivos cuánticos de seguridad podrían descifrar los protocolos criptográficos dentro de un tiempo y esfuerzo razonables. Lo que es más, probablemente muchas organizaciones, desde gobiernos a grupos delictivos, estén ya reservando información encriptada que hayan podido interceptar con la intención de descifrarla en el momento que sea posible hacerlo.

Lo cierto es que la tecnología cuántica también promete progresos en ciberseguridad mediante la criptografía postcuántica y la seguridad que ofrece la propia tecnología cuántica. Por otra parte, la transición hacia formas de codificación más resilientes frente a técnicas cuánticas y la monitorización de cualquier posible pérdida de información que pudiera utilizarse contra la organización en caso de ser descifrada, ayudarán a mitigar los riesgos de la computación cuántica.

Cibertendencias futuras alrededor del mundo

... en Asia

Dale Johnstone, director de Seguridad de AXA China Region Insurance Company Limited y AXA General Insurance Hong Kong Limited

"Durante los próximos años, debemos esperar ver agentes maliciosos organizando nuevos ataques a organizaciones establecidas en Asia. La cultura asiática tiende a ser más del tipo de respuesta –y responden de manera muy eficiente ante cualquier incidente– que de estar enfocados en estrategias y en planes generales de gestión de seguridad de la información para anticipar y evitar, con suerte, cualquier ataque o pérdida de información. Aunque actualmente esa diferencia está desapareciendo".

Cifras: Desde 2019, la ciberdelincuencia ha pasado de efectuar ataques oportunistas e indiscriminados, a objetivos más específicos. Es la "caza de grandes presas", esto es, empresas grandes, con información y activos de gran valor, con la intención de obtener rescates más elevados. Esta tendencia es global. En Singapur, aunque la mayoría de los casos denunciados provenían de PYMES, entre mayo y agosto de 2020 se observaron ataques de ransomware a empresas más grandes, de los sectores de fabricación, distribución y servicios sanitarios".
(Fuente: Tendencias globales y locales del ransomware en 2020, T1-T3, Equipo de Respuesta de Emergencia Informática de Singapur, 17 de noviembre de 2020)

... en los Estados Unidos

Libby Benet, directora global de suscripción de seguros de las Líneas Financieras de AXA XL

"La administración de Biden promulgó una orden ejecutiva a principios de mayo de 2021, que es especialmente útil para que la industria de software actúe más diligentemente en la seguridad de sus productos. Espero que en el futuro cercano veamos más decisiones al respecto en esta administración y en los gobiernos de todo el mundo. Creo que los gobiernos deberían primero exigir a los proveedores de software que incorporen medidas de seguridad en sus programas y, si no son capaces de demostrar que pueden ser sus propios regidores, entonces establecer normativas que garanticen esa seguridad. Y lo mismo en lo que respecta al hardware".

"El clamor general por la seguridad está llegando a las instancias del poder y a los gobiernos de todo el mundo. El sector de los seguros es el principal indicador a tener en cuenta, ya que nosotros podemos cuantificar los costos de las pérdidas, lo que tiene sentido real para todo el mundo. Y ahora hemos entrado en el terreno geopolítico, y necesitamos una respuesta global y unánime ante las pandillas de ciberdelincuentes, mediante una colectiva aplicación de las leyes".

Cifras: "En la primera mitad de 2020, las investigaciones revelan un marcado incremento en el número de ataques de ransomware, que se multiplicó por siete en todo el mundo, y el ransomware representó casi la mitad de todas las reclamaciones de seguros por motivos informáticos presentadas en Norteamérica". (Fuente: Tendencias globales y locales del ransomware en 2020, T1-T3, Equipo de Respuesta de Emergencia Informática de Singapur, 17 de noviembre de 2020)

... en Francia

Guillaume Poupard, director general de la Agencia Nacional de Ciberseguridad francesa (ANSSI)

"Un tema de gran interés durante los próximos meses y años será la soberanía informática, un asunto de connotaciones políticas muy complejo. ¿Mantendrá Europa su posición de aplicar exclusivamente reglas europeas a nuestros sistemas clave y nuestra información crítica, de que podremos contar con socios y aliados exteriores sin aceptar sus propias leyes y reglamentos? Si podemos hacerlo al tiempo que mantenemos una posición abierta, dado que soberanía no significa proteccionismo, será un tema muy interesante".

Laurence Lemerle, director de Ingeniería y Riesgos Informáticos, AXA Francia

"Las empresas evolucionan ahora muy rápidamente: han cobrado conciencia de los riesgos, y buscan soluciones. Están entendiendo que el primer paso es equiparse con soluciones defensivas en materia de informática, y luego adquirir un seguro. Hay todavía cosas que explicar, principalmente a las PYMES, pero las cosas están avanzando rápido, y eso es alentador".

Cifras: El 57 % de las empresas francesas fueron objeto por lo menos de un ciberataque en 2020 (Fuente: 6ª edición del barómetro anual del CESIN, CESIN, 9 de febrero de 2021); la Agencia francesa para la Seguridad de los Sistemas de Información (ANSSI) recibió 255 % más denuncias de ataques de ransomware en 2020 que en 2019 (Fuente: Informe de amenazas e incidentes del CERT-FR, ANSSI, 5 de febrero de 2021

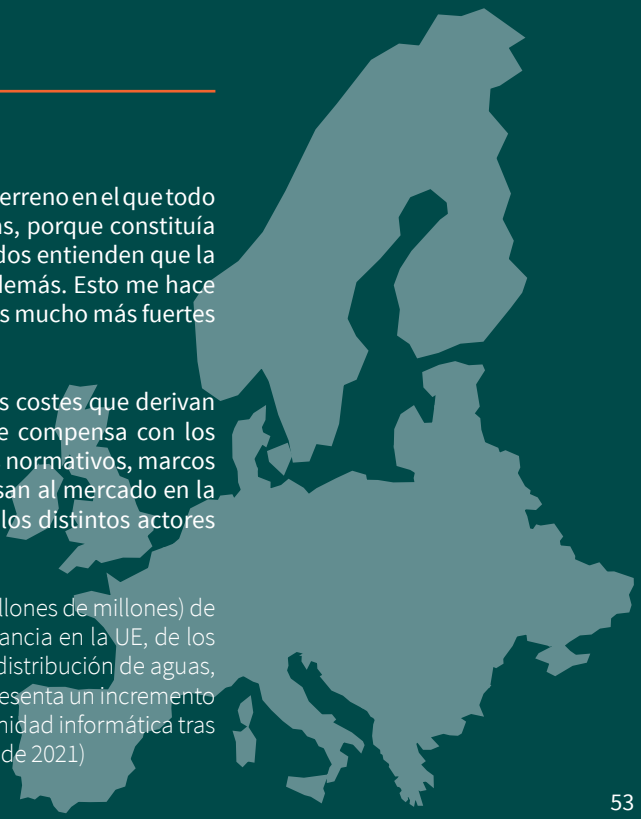
... en el Reino Unido

Heyrick Bond Gunning, director (CEO) de S-RM

"La falta de talento, las sanciones por incumplimiento del RGPD y la probable eliminación del seguro contra secuestros informáticos se compensan por las innovaciones de los servicios de respuesta ante ciberataques y la aparición de un nuevo banco de talentos de una variedad de orígenes fuera de la TI tradicional, que aportan diversidad y complementariedad a la fuerza de trabajo".

Cifras: "A pesar de la COVID-19, la ciberseguridad sigue siendo una prioridad para los organismos de gestión de las empresas. […] El 77 % de las empresas declara que la ciberseguridad es una alta prioridad para su directiva y ejecutivos sénior" (frente al 69 % de 2016). "Pero la COVID-19 ha hecho que la ciberseguridad sea más difícil […] Con la estrechez de recursos, hay menos negocios […] cuya protección contra el malware esté actualizada (83 % frente al 88 % de 2020) y que cuenten con firewalls operativos en su red (78 % frente al 83 % de 2020)". (Fuente: Encuesta sobre fallos de seguridad informática 2021, GOV.UK, 24 de marzo de 2021)

... en Europa



Heyrick Bond Gunning, director (CEO) de S-RM

"Ha sucedido algo verdaderamente nuevo: la informática solía ser un terreno en el que todo el mundo se mantenía en su esquina evitando hablar con los demás, porque constituía un riesgo de seguridad. Eso ha cambiado drásticamente, y ahora todos entienden que la única manera de tener éxito en este campo es con la ayuda de los demás. Esto me hace sentir optimista porque como grupos, de personas y de países, somos mucho más fuertes que antes frente a las amenazas informáticas".

"La imagen sombría del inevitable incremento de ciberataques y los costes que derivan de ello —porque, definitivamente, la situación va a empeorar— se compensa con los distintos pasos que ha dado Europa en materia de políticas y marcos normativos, marcos de inversión, desarrollo de capacidades y de estándares que impulsan al mercado en la dirección correcta, y en la creación de redes de colaboración entre los distintos actores involucrados".

Cifras: "El coste anual del ciberdelito a nivel global fue de 5,5 billones (millones de millones) de dólares en 2021". […] "En 2020 hubo 949 ataques maliciosos de importancia en la UE, de los cuales 742 estuvieron dirigidos a sectores críticos (energía, transportes, distribución de aguas, sistema sanitario, infraestructuras digitales y sector financiero). Esto representa un incremento del 72 por ciento en comparación con 2019". (Fuente: La UE crea nueva unidad informática tras la ola de ataques online, Elena Sánchez Nicolás, euobserver, 24 de junio de 2021)