22 de diciembre, 2021

Madrid, España

Marta de Zavala Martínez
Consultora de Ciberseguridad

Estrategia De Ciberseguridad Y Responsabilidad Humana

Christian Felber, impulsor del modelo económico de la *Economía del Bien Común* enunció en su día lo siguiente: "la confianza es el mayor bien social y cultural que conocemos. La confianza es aquello que mantiene unida a la sociedad en lo más profundo, no la eficacia."

A menudo la ciberseguridad es percibida como un ente al que solo unos pocos privilegiados, habitualmente ingenieros informáticos o hackers, tienen acceso y conocimiento suficientes para comprender sus entresijos, secretos y claves. Rodeada de lenguajes de programación y el anonimato que puede llegar a brindar la relación hombre-máquina, la ciberseguridad se ha posicionado durante años como la hermana *necesaria* de los equipos de tecnología en las empresas, a menudo sin invitación a los comités de dirección. Es decir, necesaria, pero no suficientemente **estratégica**. Sin embargo, la realidad actual desvela que ese *ente inalcanzable* resulta ser cada día más accesible de lo que podría pensarse.

De lo invisible a lo tangible

En el año 2010, el mundo giraba la mirada hacia Natanz, condado de la provincia de Isfahan, en Irán. Durante una visita de control a la central de enriquecimiento de combustible nuclear, los inspectores de la Agencia Internacional de Energía Atómica detectaron que las centrifugadoras usadas para enriquecer el uranio estaban fallando. Lo que a priori parecía un evento poco usual, se convirtió en un desastre tangible. De hecho, en junio de 2010, 1.000 máquinas de la central que participaban en la producción de materiales nucleares recibieron instrucciones de auto-destruirse. Como si se tratara de una película de ciencia-ficción, *Stuxnet* (nombre con el que se designó a la amenaza persistente o gusano informático) tomó el control de las máquinas resultando en un incremento de la velocidad de centrifugado hasta el punto de provocar su destrucción, y unos daños de gran magnitud en la central. Se trató de una de las primeras veces en las que un ataque *ciber* lograba ejercer el impacto similar al de uno militar tradicional, sin despliegue de efectivos, tanques, ametralladoras o bombas. El ataque de la considerada por los iraníes como *guerra electrónica*, generó gran especulación sobre la supuesta

implicación de Israel y Estados Unidos en su desarrollo y financiación en el la llamada *Operación Juegos Olímpicos*, y removió la caja de pandora hacia una nueva tipología de guerra que se libraba bajo la superficie del mundo físico.

Máquinas de centrifugado en la instalación de enriquecimiento de uranio de Natanz en Irán, 5 de noviembre de 2019 © Organización de Energía Atómica de Irán vía AP

Tal vez ese fuera uno de los ejemplos más extendidos del impacto tangible de las *ciber*-amenazas en el mundo físico, pero no fue el primero ni el último. En mayo de 2019 la ciudad de Baltimore en E.E.U.U. era víctima de un ataque generalizado a sus sistemas e infraestructuras críticas de la mano del ransomware *RobinHood*, dejando el funcionamiento de la ciudad en manos de hackers, durante meses. Los costes de este evento ascendieron a más de 18 millones de dólares entre los costes del propio hackeo y los relativos a la inactividad de la ciudad en el tiempo que duró el *ransom* (secuestro), según recogió Ars Technica ese mismo año. Algo similar había sucedido ya en 2007 en Estonia, en lo que se conoce como la primera cyber-guerra de la historia, cuando una serie de ciberataques coordinados (tipo DDoS) atacaron la infraestructura digital del gobierno durante un período de tres semanas, afectando a servicios financieros, gubernamentales y políticos del país. Las repercusiones económicas del ataque y las consecutivas decisiones que tomaron cuerpos internacionales como la OTAN y la Unión Europea para fortalecer las medidas de seguridad, iniciaron una nueva era para la ciberseguridad nacional, pero ¿Cuál podría haber sido el coste humano de estos ataques masivos a ciudades y estados?

Al conocer las escalofriantes cifras en dólares del caso de la ciudad de Baltimore, uno podría llegar a distraerse y olvidar los daños físicos y humanos potenciales implicados en un ataque *ciber*, además de los sentimientos de inseguridad, descontrol y terror crecientes que genera en la sociedad. El virus que ataca directamente a las infraestructuras críticas de una ciudad, como es el suministro eléctrico, impidiendo que este llegue a los hospitales, conlleva que todos aquellos pacientes dependientes de respiradores, operaciones de urgencia o calefacción, sean víctimas humanas inmediatas (colaterales y no colaterales); de igual modo que lo serían aquellos afectados si el ataque estuviera dirigido hacia los sistemas de control del tráfico aéreo. El código que está programado para *ordenar* a las turbinas de una central como la de Natanz auto-destruirse, conlleva el coste equivalente al de una explosión provocada por armas de destrucción, con los daños correspondientes. Los datos bancarios, direcciones y teléfonos de miles de clientes de diferentes bancos que son expuestos y vendidos a diario en la *darkweb*, conllevan la violación de la privacidad y confidencialidad de todos los clientes implicados.

Oficina de Departamento de Finanzas de Baltimore en 2019, notificando: *los sistemas están inactivos hasta nuevo aviso.* © Baltimore Sun

Así pues, tanto por su integración en planes de Estrategia de Seguridad Nacional de numerosos países como España, Rusia o Emiratos Árabes Unidos, como por el crecimiento del comercio electrónico, la digitalización de productos y servicios, las redes sociales, y la viralización de tendencias tecnológicas y entornos *cloud* en el ámbito global, se ha producido un cambio de paradigma radical para el sector de la ciberseguridad. Es habitual observar en el ámbito corporativo que la inversión *ciber* viene motivada al menos, por uno o varios de los siguientes factores: (i) la empresa ha sufrido un ataque informático que ha impactado en su actividad; (ii) la empresa debe cumplir con normativas vigentes (p.ej. RGPD – Reglamento General de Protección de Datos); (iii) la empresa de forma *proactiva* busca mitigar el riesgo de sufrir un ataque informático. Lo cierto es que independientemente de la causa que motive la inversión, es relevante abrir el debate de la responsabilidad humana y la importancia de la seguridad física vinculada a la seguridad *ciber*, en un planeta cuya curva de dependencia de digitalización y conectividad crece exponencialmente.

Cuestión de derechos

Uno de los temas que se encuentran en boga en los últimos tiempos, es el derecho a la privacidad. No debe ignorarse que este derecho es uno de los que están recogidos en la Declaración Universal de los Derechos Humanos de la ONU y se considera un derecho fundamental, inherente al ser humano, independiente, intransferible e irrenunciable. Al trasponerse este derecho al mundo digital, es posible analizar normativas como el Reglamento General de Protección de Datos de la Unión Europea (RGPD – Reglamento (UE) 2016/679) cuya misión es precisamente la de reforzar la protección de la privacidad en el ámbito digital. Por ello, cuando las empresas o instituciones hacen uso de los datos personales, la trascendencia de todo lo que suceda con ellos a partir del momento en el que ciudadanos y clientes dan el consentimiento para su uso en contratos, páginas web o plataformas sociales, es mucho mayor de lo que se conoce a pie de calle, siendo este un tema lo suficientemente amplio y complejo como para abordarse en otro artículo dedicado.

Eleanor Roosevelt y la Declaración Universal de Derechos Humanos de las Naciones Unidas, noviembre de 1949 © Wikimedia Common

Por otro lado, relacionado con el impacto físico y el coste humano potencial de un ciberataque, está la responsabilidad de cuidar y preservar la vida humana. Esta responsabilidad está comprendida en el derecho a la vida, también recogido en la Declaración de Derechos Humanos y que dicta que "Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona". La pregunta que los ciudadanos deben hacerse, se relaciona con entender si el gobierno y las empresas son capaces de garantizar esa seguridad y compromiso junto a las medidas implantadas para ello, en el escenario de un ataque como los enunciados anteriormente. También podría encontrarse el quid en identificar quién debe garantizar ese derecho en un mercado de economía

mixta, en el que las empresas deben cumplir con normativas de seguridad por imperativo legal, y paralelamente se buscan atajos a la rentabilidad económica sin considerar el impacto de unos riesgos no calculados.

Estrategia de ciberseguridad y humanización

Si se dividieran los componentes que conforman el término *estrategia*, el desglose podría parecerse a esto: un escenario dado con un porcentaje de incertidumbre, acompañado de un análisis profundo de las acciones que pueden controlarse, y un objetivo claro a alcanzar en un horizonte, más o menos cercano. El concepto de *estrategia de ciberseguridad* comprende todo lo anterior, e integra dos aspectos diferenciadores e indispensables: por un lado, la seguridad física y por otro, la preservación de la tríada de ciberseguridad - confidencialidad, disponibilidad e integridad de la información.

En el año 2014 se comenzó a hablar de la Responsabilidad Social Estratégica (RSE), la cual suponía "integrar la responsabilidad social dentro de la orientación estratégica y la misión de las organizaciones con una implicación decidida de la alta dirección." (Fundación Factor Humà). Este movimiento se centraba fundamentalmente en los ámbitos del impacto medioambiental, la cadena de suministro o el apoyo a la diversidad, y todos aquellos ya defendidos por la Responsabilidad Social Corporativa de mitad del siglo XX, que busca el equilibro entre las dimensiones social, económico y medioambiental de las empresas. En este sentido, si la ciberseguridad fuera considerada un factor más del impacto positivo social, como rama necesaria para el buen funcionamiento de la sociedad, el escenario de la RSE de la inversión empresarial en ciberseguridad se presentaría como un candidato viable del movimiento RSE.

Sin embargo, independientemente de encontrar una pertenencia a un movimiento o a otro, hoy es crucial entender las implicaciones de introducir la ciberseguridad en la estrategia empresarial e institucional, junto a sus ventajas e inconvenientes. El impacto de una buena o mala estrategia de ciberseguridad podría adivinarse siempre a posteriori, con una adecuada evaluación de daños, y los detalles de cuándo, dónde y cómo sucedió todo. Es fácil hablar *a toro pasado*, pero lo cierto es que la prevención y proactividad son necesarias para minimizar los costes, no solo desde un punto de vista económico o reputacional, sino los derivados de una insuficiente responsabilidad humana. Para ello, es necesario influir en el comportamiento en las corporaciones, en un ejercicio que vas más allá de la concienciación y el cumplimiento normativo.

La confianza de clientes y ciudadanos en las empresas e instituciones es, como ya enunciaba Christian Felber, aquello que mantiene la sociedad unida en lo más profundo. Tal vez por ello, la ciberseguridad deba pasar a ser la piedra angular de la estrategia digital, que ponga en el centro de la estrategia, al ser humano.