CINCO LECCIONES DE CIBERSEGURIDAD EN EL FORO DE DAVOS 2024

FUNDACIÓN ESYS

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL

ANÁLISIS FLASH

ENERO 2024

La ciberseguridad ha sido uno de los grandes temas protagonistas del Foro de Davos 2024. En la misma semana en que el Foro Económico Mundial hospedaba el encuentro, varios sitios web suizos sufrieron una oleada de ataques distribuidos de denegación de servicio (DDoS). Un grupo ruso de hackers con motivaciones políticas conocido como NoName reivindicó la autoría de los ataques. El grupo es conocido por sus ataques DDoS, dirigidos principalmente contra instituciones financieras, sitios web gubernamentales o servicios de transporte en países europeos que apoyan a Ucrania durante su guerra con Rusia. NoName vinculó sus recientes ataques a Suiza con la asistencia del presidente ucraniano Volodymyr Zelensky al Foro Económico Mundial de Davos.

Estas son **cinco grandes ideas** han guiado el debate sobre la ciberseguridad en el Foro de Davos.

1. **Para reconstruir la confianza, necesitamos más y mejor ciberseguridad conectada**

El lema de este año fue 'Reconstruyendo la confianza'. No es casualidad. El secretario general de Naciones Unidas afirmó que "cuando las normas mundiales se derrumban, también lo hace la confianza. Personalmente, estoy conmocionado por el debilitamiento sistemático de principios y normas que solíamos dar por sentados."

Es la primera vez en años que un riesgo tecnológico se coloca como el más importante en el Informe de Riesgos Globales del Foro Económico Mundial. Va por delante de los riegos medioambientales, económicos, sociales y geopolíticos. En 2019 el riesgo tecnológico también apareció en las primeras filas, pero no ha sido hasta este año que se ha hecho palpable en un doble sentido. Primero, la desinformación se considera como el mayor riesgo, con mayor impacto y mayor probabilidad, en el corto período de dos años. La inseguridad cibernética se coloca como el cuarto riesgo global con el mismo criterio.

2. **La ciberseguridad no solo genera riesgos, sino que también lleva a mayores desigualdades (*cyber inequity*)**

Parte de los debates del Foro de Davos fueron marcados por el último *Global Cybersecurity Outlook 2024*. El informe presenta varias cifras.

Primero, crece la desigualdad cibernética entre las organizaciones ciberresilientes y las que no lo son. El número de organizaciones que mantienen una ciberresiliencia mínima viable ha descendido un 30%. Mientras que las grandes organizaciones demostraron notables avances en ciberresiliencia, las PYMES mostraron un descenso significativo. Sin embargo, más del doble de PYME que de grandes organizaciones afirman carecer de ciberresiliencia para cumplir sus requisitos operativos críticos.

Segundo, la mitad de las organizaciones más pequeñas, por ingresos, afirman no tener o no estar seguras de si disponen de las competencias necesarias. Solo el 15% de las organizaciones son optimistas y creen que mejorarán significativamente en los próximos dos años. El 52% de las organizaciones públicas afirma que la falta de recursos y competencias es su mayor reto a la hora de diseñar la ciberresiliencia.

3. **La ciberseguridad debe estar al frente para dar soluciones a la Inteligencia Artificial**

Aunque la IA no amplía necesariamente la superficie de ataque de una organización, hace que la superficie de ataque existente sea más vulnerable y acelera la productividad de los ciberatacantes. Una encuesta reciente entre directores de seguridad de la información y CISOs reveló que el 70% cree que la IA da ventaja a los atacantes sobre los defensores. La IA generativa aumenta los riesgos de ciberseguridad.

Sin embargo, también la IA puede mejorar la propia resiliencia cibernética, aunque todavía es una tendencia creciente y menor. Por ejemplo, un 26% de los CISOs indicó que la IA generativa se está utilizando para analizar las fuentes de

datos y determinar cuáles deben ser optimizados o eliminados; un 23% lo hace para crear estándares de configuración segura; un 25% para hacer análisis de malware; y un 19% para hacer investigaciones forenses y dar respuesta a incidentes.

4. **Eje central para garantizar las elecciones políticas en 2024**

En 2024, más de 70 países y 2.000 millones de personas van a acudir a las urnas. Dos sesiones principales se centraron en este tema: cómo proteger la democracia contra "bots y plots", y hacia dónde está yendo la libertad de expresión.

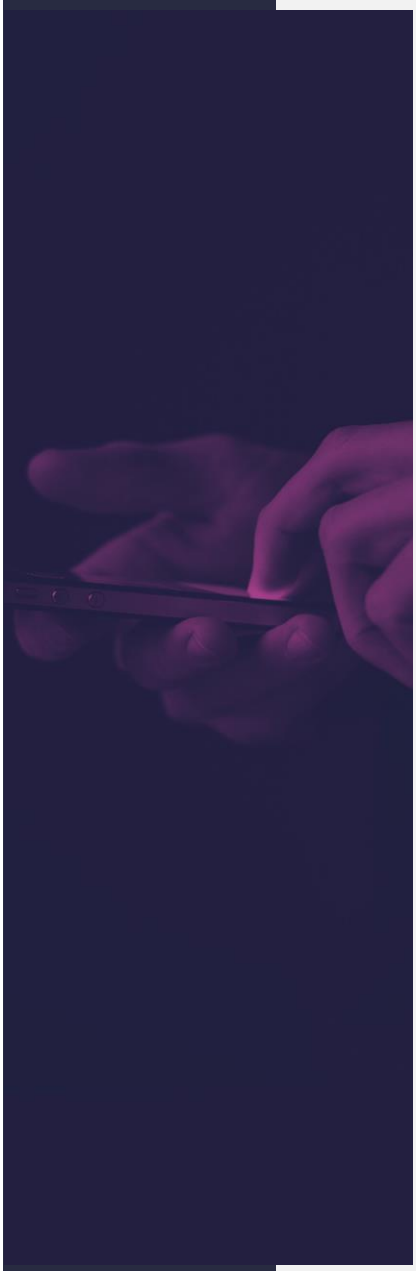
Si bien, la mayoría de los países convocan elecciones para votar única y exclusivamente de manera presencial y física, hay países donde ya se puede realizar la votación de manera online, lo que requiere garantizar que se cumplan con los requisitos de ciberseguridad y el ejercicio del voto libre, secreto y seguro.

Además de este aspecto, otro punto que se enfatizó en las sesiones fue la necesidad de luchar contra la desinformación. Muchos países no constan con una estrategia nacional de desinformación y, cuando la tienen, los recursos y ecosistema de actores disponibles para trabajar en ello son limitados. Sin embargo, es importante mencionar que no hay una responsabilidad única en este tema: la amplitud de actores maliciosos emitiendo mensajes de desinformación se multiplica y diversifica en nuevos espacios y ámbitos, lo que dificulta el trabajo de las personas involucradas en combatirlo.

5. **Una concienciación sobre cómo defenderse ante los ciberriesgos**

Se esperaba que la ciberseguridad fuera un eje mucho más relevante en los conflictos y guerras que se están sucediendo en la actualidad, desde Ucrania y Rusia, pasando por Gaza e Israel, hasta Sudán. Se ha identificado que la ciberseguridad no supone un antes y un después en el desarrollo de un conflicto, sino que genera vulnerabilidades en activos tan estratégicos como las infraestructuras críticas.

De ahí, la necesidad de que las empresas integren las soluciones de ciberseguridad, no solo como un aspecto operativo, sino como un elemento de carácter estratégico en la alta dirección de las corporaciones, así como abordándolo desde un enfoque geopolítico.



RAQUEL JORGE

Directora de Análisis e Investigación de la Fundación ESYS.

ANÁLISIS FLASH

ENERO 2024

CINCO LECCIONES DE CIBERSEGURIDAD EN EL FORO DE DAVOS 2024

FUNDACIÓN ESYS

CALLE FERRAZ, 2, 28010 MADRID - MADRID

TEL.: +34 609 484 940

EMAIL: FUNDACIONESYS@GMAIL.COM

ESYS
EMPRESA SEGURIDAD Y SOCIEDAD DIGITAL