

Economía

Pandemia aceleró ciberataques y los riesgos para las empresas en el mundo

José A. Barrera | Lunes 14, septiembre 2020 - 12:01 am



El teletrabajo, adoptado por varias firmas, extendió las redes a sitios con poco control. El phishing es una de las principales amenazas.



Los reportes de secuestro de datos (ransomware) han crecido en 200 % durante la pandemia. / DEM

El auge del teletrabajo disparó los riesgos para las empresas. Durante el **confinamiento por la pandemia**, los ataques de denegación de servicio se incrementaron en un 30 %, mientras a las aplicaciones y canales digitales se aumentaron en un 40 %.

Los ataques, sin embargo, son **cada vez más sofisticados** y las empresas –de todo tamaño– urgen la necesidad de aplicar planes robustos para evitar caer en trampas en redes cada vez más dispersas.

PUBLICIDAD

José Vicente Martín, director de clientes corporativos de Movistar Empresas, considera que la **ciberseguridad** es un pilar en una época en la que se aceleró la **transformación digital**.

“La pandemia aceleró de manera vertiginosa la transformación digital en el mundo se, en pocos meses de confinamiento se avanzó digitalmente lo que hubiéramos tardado años en condiciones de normalidad”, dijo.

“Tuvimos que implementar nuestro plan de emergencia en una semana. Ningún plan, en el peor escenario, incluía seis meses de crisis sanitaria”.

Ernesto Gutiérrez,

Vicepresidente Digital de **Ecopetrol** (Colombia).

Enrique Luis Arnaez, comandante de Ciberdefensa Marina de Guerra del Ejército, dijo que en los primeros días del confinamiento los ataques crecieron exponencialmente.

“Muchos hackers lo hacen por ocio y tienen trabajos. En los primeros días del encierro se dispararon los ataques”, dijo Arnaez que reconoció que en la medida que las actividades comenzaron a normalizarse, los ataques también disminuyeron pero alertó que se sofisticaron.

EN CIFRAS

80 %

Es spam

Se estima que el 80 % del tráfico de correos electrónicos en el mundo es contenido malicioso y tiene un gran riesgo de phishing y robo de datos.

DESTACADO: Encuesta ESET: 42 % de las empresas no estaba preparada para aplicar teletrabajo seguro

Ernesto Gutiérrez, vicepresidente Digital de la compañía colombiana **Ecopetrol**, explicó que, aunque ya tenían una estrategia digital, la pandemia aceleró los planes y significó activar un plan de emergencia que involucró a 7,000 colaboradores y 20,000 contratistas.

“**Ningún plan, en el peor escenario, incluía seis meses de crisis sanitaria** y el inicio de ‘una nueva normalidad’”, dijo Gutiérrez durante un foro de ciberseguridad organizado por Movistar Empresas. La compañía, añadió, experimentó un incremento de 2,500 % en los ataques y recibe 30 millones de correos fraudulentos al mes.

“Sabemos que la persona es el eslabón más débil en la cadena, es quien toma la decisión y a veces abrir un correo puede generar grandes riesgos”.

Ramiro de la Rosa,
Global Chief Information Security Officer de CEMEX.

Phishing y ransomware

Desea compartir con un amigo?

Martín explicó que en los seis meses pasados actividades como el **teletrabajo, la educación remota, las compras y las transacciones on line** –incluidas la de pedidos a domicilio– se volvieron actividades cotidianas para millones alrededor del mundo, pero enfatizó que se dispararon los riesgos.

Los casos de **phishing**, correos electrónicos masivos que muchas veces suplantan identidades y ogran robar datos sensibles de los usuarios –cómo números de tarjetas de crédito y cuentas de ahorros–, son parte de los riesgos latentes para las organizaciones, los que pueden derivar en casos de **ransomware**, ataques donde un ciberatacante secuestra información valiosa a cambio de un pago.

LEA TAMBIÉN: [Crecen las estafas en línea que usan como gancho al covid-19](#)

Temas como **“vacunas” o “coronavirus”** son parte de los ganchos que usan redes criminales para generar una nueva ola de ataques que antes estaban casi limitados solo a la suplantación de cuentas de banco, por lo que ahora los riesgos son mayores y ante los que una infraestructura reforzada desde los departamentos de tecnologías de la información solo pueden filtrar hasta el 80 %, el resto debe ser bloqueado por el usuario.

“Necesitamos crear un **‘firewall humano’** como estrategia para protegernos, podemos filtrar ataques, pero habrá un porcentaje que la tecnología no es capaz de ver”, puntualizó Global Chief Information Security Officer.

Riesgos de ciberseguridad en crecimiento por la pandemia

- ✓ **Señuelos:** De acuerdo con un reporte de ESET, el tema de covid-19 se convirtió en un señuelo para correos maliciosos. Aunque también otros que suplantarón a DHL por el incremento de su operación en la pandemia.
- ✓ **Equipos lentos:** ESET también descubrió el auge del botnet VictoryGate utilizado principalmente para minar criptomonedas, programa que ralentiza los equipos mientras procesa bitcoins sin que el usuario se percate de la actividad.
- ✓ **Secuestro de datos:** El ransomware (código malicioso usado para extorsionar a sus víctimas) fue una de las áreas de más rápido desarrollo en el segundo trimestre del año, de acuerdo con el reporte del primer semestre de 2020 de ESET.

Conclusiones

Temas como **“vacunas” o “coronavirus”** son parte de los ganchos que usan redes criminales para generar una nueva ola de ataques que antes estaban casi limitados solo a la suplantación de cuentas de banco. Los ataques, sin embargo, son **cada vez más sofisticados** y las empresas –de todo tamaño– urgen la necesidad de aplicar planes robustos para evitar caer en trampas en redes cada vez más dispersas.

MUNDOMEDIA +

Educación presenta prueba que sustituirá la PAES y así se hará

Veterinarios en El Salvador trasplantan plumas a gavián para que pueda volar

El humo de los incendios en el oeste de EEUU llega hasta Nueva York

Trump advierte de que respondería a un ataque de Irán con uno “mil veces mayor”

RECOMENDACIÓN DE LA REDACCIÓN

OPINE Y COMENTE

Diario El Mundo abre este espacio de opiniones para que se pueda debatir, construir ideas y fomentar la reflexión. Por eso, pedimos que se evite hacer uso de ataques ofensivos, que incluyan malas palabras, de lo contrario no reservamos el derecho de publicación.

Recuerde que este es un medio que está para generar opinión constructiva.

0 Comentarios | [elmundo.sv](#) | [Política de privacidad de Disqus](#) | [Acceder](#)

[Recomendar](#) | [Tweet](#) | [Compartir](#) | Ordenar por los mejores

INICIAR SESIÓN CON

O REGISTRARSE CON DISQUS ?



Sé el primero en comentar.

[Suscríbete](#) | [Añade Disqus a tu sitio web](#) | [Do Not Sell My Data](#) | **DISQUS**

SOBRE NOSOTROS

- Catálogo de Impresos
- Tarifario Diario El Mundo
- Historia
- Términos y condiciones

GRUPO BORJA

- Grupo Borja
- Fundación Borja
- Vida Sana
- DeVacaciones
- El Migueleño

SOCIAL MEDIA



EDICIONES ANTERIORES

Archivos [Ver más]



VERSIÓN E-PAPER



CONTÁCTENOS

- PBX General: +503 2234-8000
- Ventas: +503 2234-8014
- Redacción: +503 2234-8020
- redaccionweb@elmundo.sv
- ventas.digital@elmundo.sv
- esquelas@elmundo.sv

15^o Calle Poniente y 7^a Avenida Norte, N° 521, Centro de Gobierno, San Salvador.