La respuesta cibernética de EY al brote de Coronavirus

Fortalecimiento de la resiliencia operativa y de seguridad durante la crisis COVID-19.

EY
Building a better working world

La propagación del coronavirus podría afectar a más de cinco millones de empresas en todo el mundo[1] y los países más afectados representan casi el 40% de la economía mundial[2].

Las empresas de todos los sectores se enfrentan a un panorama en evolución de amenazas cibernéticas resultantes del impacto de la pandemia.

Además, una transición rápida a adaptaciones de trabajo remotos está ejerciendo presión sobre los equipos de seguridad para que comprendan y aborden rápidamente una ola de posibles riesgos de seguridad.

Ciberamenazas y ataques recientes

Phishing, sitios web maliciosos y correos electrónicos comerciales comprometidos

- Los ciberdelincuentes explotan el interés en la epidemia mundial para llevar a cabo actividades maliciosas a través de campañas de spam relacionadas con el brote de coronavirus.

Extorsión, robo de información y daño a la marca

- Puede dirigirse a organizaciones que perciben estar bajo presión relacionada con la pandemia.
- Acciones o declaraciones consideradas inapropiadas como un posible desencadenante de "hacktivismo" y amenazas internas.

Interrupciones comerciales por ataques

- Ransomware con temática de Coronavirus que puede cifrar el disco duro de una computadora y permitir a los piratas informáticos extorsionar los pagos a cambio de desbloquear la computadora.

Dispersión de actividades y procesos realizados anteriormente en la oficina

- Cambio en la línea base de la red:
  - Acciones de alto privilegio realizadas remotamente podrían activar alarmas.
  - Todo el tráfico aparecerá irregular hasta que se establezca la nueva línea de base.
- Mayor carga de trabajo en la mesa de ayuda y TI.

“79% de los miembros de junta admiten que sus organizaciones no están preparadas para enfrentar una crisis.[3]

Dominios con temática de Coronavirus 50% más propensos a ser maliciosos que otros dominios
CheckPoint

Hospital checo golpeado por ciberataque en medio del brote de COVID-19
ZDNet

RedDrip Team
Ataques que contienen documentos de carnada por parte de delincuentes que fingen ser el Ministerio de Salud Pública de Ucrania o el Centro de Salud Pública.

Forbes
Alerta de estafa de coronavirus: Tenga cuidado con estos sitios web y correos electrónicos riesgosos de COVID-19.

Fuente 1: CNBC, 4 Febrero 2020; Fuente 2: McKinsey; Fuente 3: Encuesta Global de Riesgos 2020

Las siguientes acciones se pueden tomar para ayudar a proteger su organización en este entorno que cambia rápidamente a la luz de las recientes amenazas cibernéticas.

Actualizar VPNs, dispositivos de infraestructura de red y los **dispositivos que se utilizan para conectarse de forma remota** a entornos de trabajo con los últimos parches de software y configuraciones de seguridad.

Configure la autenticación multifactor **(MFA) en todas las conexiones VPN** para aumentar la seguridad. Si MFA no está configurado, solicite a los empleados que trabajan de forma remota que usen contraseñas seguras.

Asegúrese de que el personal de seguridad de TI **pruebe las limitaciones de VPN** para prepararse para un uso masivo y, si es posible, realice modificaciones como la limitación de velocidad para dar prioridad a los usuarios que requieren mayores anchos de banda.

Supervise de cerca el acceso privilegiado optimizando las **herramientas de análisis de comportamiento** diseñadas para detectar actividades sospechosas para los administradores y aquellos que tienen acceso a datos críticos.

Los sistemas de información de seguridad y gestión de eventos (SIEM) deben adaptarse para fortalecer las reglas de monitoreo de registros que cubren la activación de alertas. **El Centro de operaciones de seguridad (SOC)** y los equipos de monitoreo deben estar disponibles para administrar el mayor número de alertas, clasificarlas por riesgo en función de un proceso sólido y detectar falsos positivos de eventos reales sospechosos. Considere aumentar el personal para estos fines.

Preste más atención a las siguientes **tareas de ciberseguridad de acceso remoto**: revisión de logs, detección de ataques, respuesta a incidentes y recuperación.

Lista blanca y marcado de correos electrónicos externos. Además**, informe a los empleados** sobre un aumento anticipado en los intentos de phishing con temas relacionados con el coronavirus y pídales que se abstengan de hacer clic en enlaces sospechosos de fuentes desconocidas.

Protección web y de correo a través de tecnologías de filtrado web destinadas a evitar que los empleados visiten sitios web maliciosos. Establezca reglas de filtrado de correo para bloquear correos no deseados y de phishing. Los hospitales y otras instituciones con infraestructuras críticas deben observar estas pautas de manera más estricta y deben considerar la inclusión de lista blanca.

Limite el acceso del administrador y las actividades a aquellas que sean absolutamente necesarias. Las actividades administrativas también deben ser monitoreadas y verificadas de manera más efectiva (aplicando el principio de control dual, etc.).

Aumentar las **capacidades de gestión de emergencias** reasignando recursos. Compruebe si su copia de seguridad funciona y pruebe sus capacidades de conmutación por error. La mesa de ayuda también debe estar preparada para manejar un mayor número de eventos y debe poder aplicar el procedimiento para clasificar esos eventos.

Aumente su protección de monitoreo **Endpoint**.

Prepárese para lo peor, **revise la gestión interna de crisis y las capacidades de respuesta a incidentes**, así como la disponibilidad de sus proveedores. Considerando expandir su panorama de proveedores.

¿Qué mensajes deben comunicarse a sus empleados?

1. **Adherirse constantemente a las políticas de la compañía.**
   - Observe todas las políticas, pautas y reglas relativas al acceso a la red de la empresa fuera de la oficina. Asegúrese de informar cualquier comportamiento sospechoso a la función de soporte y observe los estándares básicos, como mantener actualizados los sistemas operativos, el software antivirus y antimalware y garantizar el análisis periódico de virus, etc.
2. **No permita que miembros de la familia usen sus dispositivos de trabajo.**
   - Trate su computadora portátil, dispositivo móvil y datos confidenciales como si estuviera en la oficina.
3. **Use una solución de almacenamiento aprobada por la compañía.**
   - Asegúrese de almacenar todos los datos de su trabajo en una ubicación segura aprobada y accesible para su empresa.
4. **Utilice únicamente dispositivos aprobados por la empresa y consulte a su departamento de TI si desea utilizar un dispositivo personal para conectarse a redes corporativas.**
   - Si se conecta a través del Wi-Fi de su hogar, asegúrese de que la red Wi-Fi tenga una contraseña segura. Evite el uso de redes públicas o no seguras.
   - Si se requiere el uso de un dispositivo personal en un caso excepcional, tome todas las precauciones posibles, como actualizar los sistemas operativos, el software antivirus, el enrutador Wi-Fi, etc.
5. **Tenga en cuenta su higiene en línea.**
   - Tenga cuidado de hacer clic en enlaces sospechosos, especialmente si están relacionados con el coronavirus, teniendo en cuenta que los atacantes están explotando este miedo para atraer más fácilmente a las víctimas al hacer clic en enlaces que de otro modo se considerarían sospechosos.

Su equipo EY

Geovanni Nacimba
EY Forensics - Associate Partner
+593 2 2555 553
geovanni.nacimba@ec.ey.com

Krystel Zamora
EY Forensics - Manager
+593 2 2555 553
krystel.zamora@ec.ey.com

Gabriel Cuestas
EY Forensics - Manager
+593 2 2555 553
gabriel.e.cuestas.flores@ec.ey.com

Todd J. Marlin
Global Forensic Technology Leader
todd.marlin@ey.com