Resiliencia en tiempos de **Ransomware** (I)

Por **Isabel María Gomez, Global CISO** de Atento

ATENTO

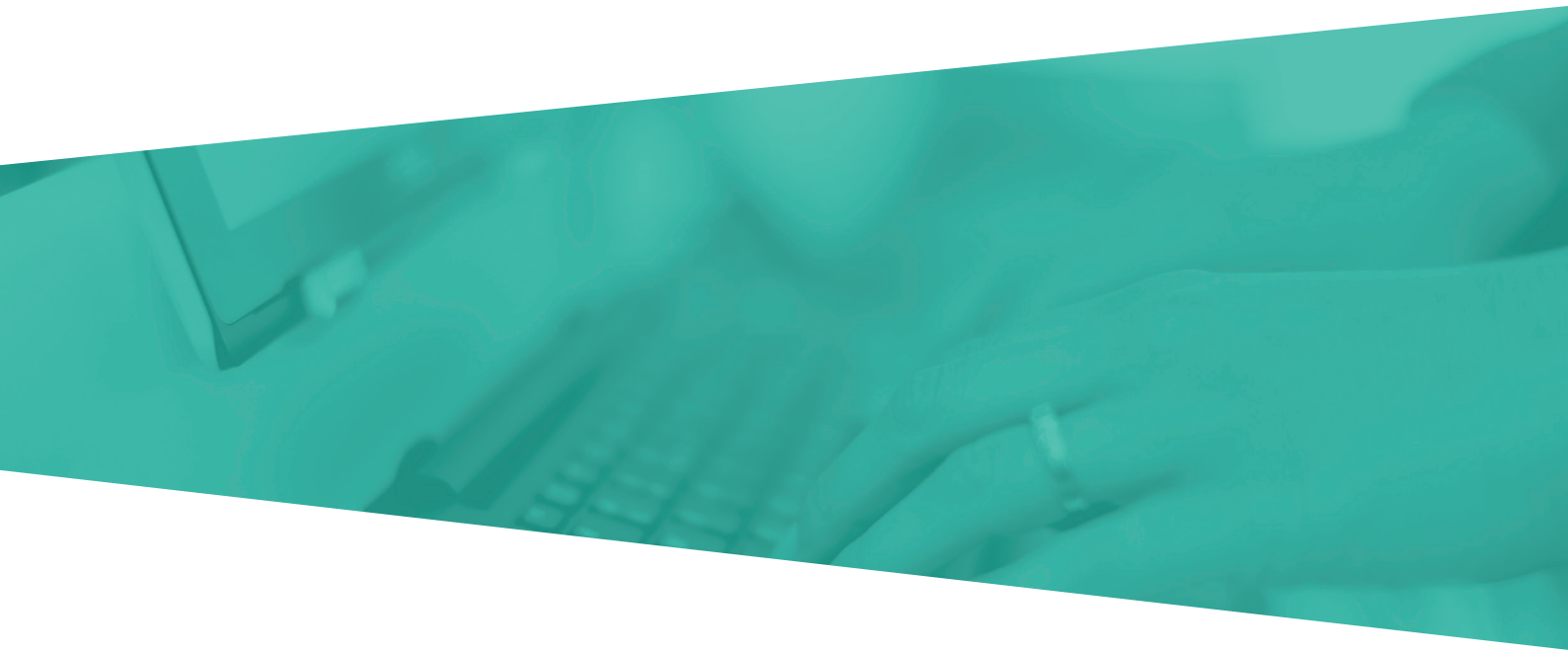
WHITE PAPER

CONTENIDO

01 Resiliencia en tiempos de **Ransomware**

Una infección de ransomware es uno de los escenarios más difíciles a los que las empresas se enfrentan hoy en día. No solo porque **pone a prueba los procesos de continuidad de negocio de la organización,** sino porque genera un escenario de estrés que va más allá de la ciberseguridad y la tecnología, generando unas líneas de actuación y toma de decisión que en pocas ocasiones han sido testadas con tanta fortaleza.

Todas las áreas de la compañía, sin excepción, se ven envueltas en un ejercicio que ha dejado de ser la prueba teórica aburrida en la que todos participan para garantizar la recuperación en un escenario de desastre, bajo control y supervisión de un reloj, que suele finalizar en los plazos esperados sin mayores contratiempos dada su cuidadosa planificación. **Se convierte en una situación real, que pondrá a prueba la resiliencia real de los líderes de la seguridad y la tecnología** responsables de dar soporte y guiar el sobreesfuerzo de todo el equipo: ***No existe viento favorable para quien no sabe a dónde se dirige.***



02 El momento que lo **cambia todo**

Como todo escenario de desastre siempre hay una chispa, una pieza de dominó que cae e inexorablemente arrastra a las demás que la acompañan: ***El comienzo del cifrado de un equipo***. Es ese momento, en el que el **CISO** (Chief Information Security Officer) recibe la llamada que activa el comité de crisis, en el que de verdad se activa la resiliencia de la ciberseguridad. Porque de ese rol depende el tomar las primeras decisiones adecuadas para contener y remediar mientras que a su vez da soporte y da su mejor consejo al resto de la compañía para ayudar a priorizar cada línea de acción y dar más viento a las alas de la tecnología: ***Lo que se decida en esos primeros momentos será lo que marque el tiempo de recuperación de la compañía.***

A estas alturas es más que conocida la metodología que utiliza un ransomware para funcionar, no obstante, es importante hacer un breve recordatorio simplificando la secuencia de los pasos de los escenarios que van a generar que un cibercriminal acceda a la red, los sistemas y los dispositivos conectados.

Hay tres etapas en un incidente de ransomware que se pueden simplificar en **3 grandes actividades:**

- El cibercriminal gana la entrada a su red, sistemas o dispositivos.
- El cibercriminal toma el control y despliega el ransomware.
- El cibercriminal activa el cifrado los datos, destruye las copias de seguridad y roba los datos de la organización y/o de sus clientes, y luego exige el pago de un rescate.

03 El **origen**

Un cibercriminal malicioso de la amenaza suele encontrar su **punto de entrada a su red** a través de:

- Ataques de fuerza bruta.
- Explotando vulnerabilidades no corregidas.
- Mediante ataques de phishing en los que el cibercriminal intenta solicitar información confidencial a un individuo, grupo u organización imitando o suplantando a una marca específica, en general conocida, para obtener un beneficio económico. El cibercriminal intentará engañar a los usuarios para que revelen datos personales, como números de tarjetas de crédito, credenciales bancarias en línea y otra información sensible, que luego pueden utilizar para cometer actos fraudulentos.

04 El despliegue

Una vez que el cibercriminal ha obtenido **acceso a la red:**

- Tomará el control de sus sistemas y dispositivos conectados escalando permisos si no los hubiera conseguido ya.
- Desplegará el malware e infectará sus sistemas y dispositivos conectados con ransomware.

05 La ejecución

Una vez que tengan el **control total**, bajarán las defensas quizás mediante el uso de políticas globales dentro del bosque o del directorio activo, cifrarán sus datos todo a la vez y eliminarán los archivos de copia de seguridad disponibles o conectados, y, además robarán todos los datos posibles de la organización.

En este punto, y si han conseguido exfiltrar datos de la compañía es posible que amenacen con filtrar estos datos si no se paga el rescate, asegurándote que descifrarán tus datos y restaurarán tu acceso a ellos si pagas el rescate. Algo que sin duda realizarán dado que es la clave de su negocio.

06 Algunos **guiños técnicos** para mejorar la resiliencia

Si bien los elementos organizativos serán desarrollados en una segunda entrega, es importante destacar una serie de **medidas técnicas a la altura de cualquier compañía** que ayudan a una detección temprana y facilitan la correlación de alertas e información que permite dificultar la ejecución de este tipo de amenaza.

En este listado de las ***"most wanted cybersecurity meassures against the ransomware"*** es aconsejable coger perspectiva y, manteniendo lo establecido y ampliamente conocido, poner foco en lo que de forma sencilla y asequible incremente el nivel de resiliencia y protección contra el ransomware, algo que ayude a un CISO a proteger por muy diferente que sea el tamaño de su compañía.

1. **Instalación de LAPS (Local Administrator Password Solution)** en todas las workstations

   a. Proporciona la administración de contraseñas de cuentas locales de equipos unidos a un dominio. Las contraseñas se almacenan en Active Directory (AD) y están protegidas por ACL, por lo que solo los usuarios con permisos pueden ver o solicitar su restablecimiento.

2. **Desactivación del servidor SMB (Server Message Block)** en las workstations del dominio

   a. El SMB es un protocolo cliente / servidor que gobierna el acceso a archivos y directorios completos, así como a otros recursos de red como impresoras, enrutadores o interfaces abiertas a la red.

   b. Link a lectura recomendada.

3. **Segmentación de la red**

   a. Quizás es la medida estrella de todas las mencionadas, dado que su principal objetivo es el disminuir la superficie del ataque, aplicando reglas que pueden reducir el riesgo de movimientos laterales además de favorecer un modelo de seguridad basado en la confianza cero (Zero Trust Security Policy), lo que permite que solamente el tráfico autorizado vaya de un origen a un destino autorizado.

4. **Desactivación de Macros** en Words

   a. Una macro es una serie de comandos e instrucciones que se agrupan de forma conjunta como un mismo comando para completar una tarea automáticamente.

5. Establecer políticas de seguridad vía GPO (Group Policy Object) de los Navegadores

a. Las configuraciones como el filtro de phishing, la gestión de contraseñas, la verificación de certificados puede proteger a la organización frente a los ataques basados en la web cuando se configuran centralmente y se implementan en los equipos de una organización. Esto se puede lograr utilizando el GPO proporcionado por Microsoft para Edge e Internet Explorer y las plantillas ADMX para Chrome y Firefox proporcionadas por los respectivos proveedores de navegadores.

6. Protección del LSASS (Local Security Authority Subsystem Service) para evitar la obtención de credenciales

a. El Servicio de Subsistema de Autoridad de Seguridad Local (Local Security Authority Subsystem Service, LSASS) es el proceso responsable de hacer cumplir la política de seguridad en los sistemas operativos Microsoft Windows. Verifica que los usuarios inicien sesión en un equipo o servidor Windows, gestiona los cambios de contraseñas y crea tokens de acceso, y, escribe en el registro de seguridad de Windows. *(Wikipedia)*

b. El Servicio de Subsistema de Autoridad de Seguridad Local (Local Security Authority Subsystem Service, LSASS) es el proceso responsable de hacer cumplir la política de seguridad en los sistemas operativos Microsoft Windows. Verifica que los usuarios inicien sesión en un equipo o servidor Windows, gestiona los cambios de contraseñas y crea tokens de acceso, y, escribe en el registro de seguridad de Windows. (Wikipedia)

c. Link a lectura recomendada.

7. Generación de políticas de Firewall local por rol de servidor y activación del mismo

a. Después de identificar los requisitos y tener disponible la información sobre el diseño de red y los dispositivos, puede empezar a diseñar las reglas y la configuración de GPO que le permitirán aplicar sus requisitos en los dispositivos.

b. Link a lectura recomendada.

8. Implementar Applocker en todas las workstations

a. La herramienta llamada AppLocker permite bloquear ciertas aplicaciones siempre que tengamos los permisos de administrador. De esta forma podemos decidir qué programas se ejecutan en el PC impidiendo así que los usuarios pongan en marcha aplicaciones que consideremos peligrosas o no apropiadas. Se trata de una potente función que nos permitirá aumentar la seguridad de nuestro ordenador frente a amenazas externas.

b. Link a lectura recomendada.

9. Migrar sistemas operativos fuera de soporte

a. Muchas veces se piensa que es mejor trata la infraestructura de TI de forma conjunta, pero eso podría hacer que la obsolescencia se adelante. De hecho, el hardware, el software y las redes se suelen tratar de forma conjunta. Este error habitual provoca que no se tengan en cuenta los efectos de la obsolescencia en cada equipo individual. Ni todos los equipos necesitan el mismo tipo de programas ni todos se usan para el mismo tipo de trabajo. Lo más recomendable es realizar un análisis de cada dispositivo de forma individual para prever la aparición de alteraciones en su funcionalidad.

10. Establecer SMB signing y SMB3 en toda la compañía

a. SMB esencialmente firma cada paquete con una firma digital para que el cliente y el servidor puedan confirmar de dónde se originaron, así como la autenticidad de la llamada. Cuando la firma SMB está activada, si un atacante intenta robar una sesión SMB no podrá modificar los paquetes, lo que le permitirá robar la sesión.

b. Link a lectura recomendada.

07 Pero no solo hay tecnología, también existe **la debida diligencia**

Si se han aplicado diversas medias técnicas y se tiene una relativa seguridad en nuestra resiliencia a nivel de tecnología debemos poner el foco en otro tipo de resiliencia que también va a requerirse durante un ataque de este tipo: **la debida diligencia.** Ya no solo en proporcionar un adecuado marco de ciberseguridad a la compañía, sino en la que los valores de la empresa, y los de las personas que forman las compañías, son los que impulsan al equipo a desarrollar un sobre esfuerzo agotador que permite llevar el barco a buen puerto con rapidez.

Entre algunos de los conceptos que se desarrollarán en la segunda entrega están conceptos como la adaptabilidad, la reacción organizativa o incluso los impactos legales y comerciales pasando incluso por el control de la información sobre el incidente.

ATENTO

www.atento.com