ManageEngine
Log360

# Asegure su red empresarial en 5 sencillos pasos

www.manageengine.com/log360

# Introducción

Como administrador de red, ¿a veces siente que siempre tiene que estar en varios lugares a la vez? En un minuto está trabajando para garantizar que las operaciones comerciales críticas se realicen sin interrupciones. Al siguiente, está analizando las amenazas potenciales que podrían conducir a un ataque. Una vez más, algo anda mal con Internet y sus colegas se están impacientando. Además de todo esto, debe asegurarse de que no haya lagunas de seguridad que un atacante pueda aprovechar. Esto se debe al aumento de los ataques cibernéticos, como los ataques DDoS y ransomware, que han paralizado a las organizaciones. ¿Recuerda Pemex? Este es solo uno de los muchos ataques que se han detectado en esta región. Más recientemente, El Ministerio de Trabajo y Economía Social de México también fue víctima de un ataque de ransomware. A todo esto se suman los ataques de phishing temáticos de COVID-19, malware payloads que se están extendiendo como un incendio.

A la luz de esto, hemos recopilado 5 simples pasos que puede tomar para proteger su red. Hemos seleccionado los que no le quitarán demasiado tiempo o sus recursos pero mejorarán significativamente su postura de seguridad una vez implementados.

# 1. Fortalezca su enlace más débil: sus usuarios


Cualquier sistema, no importa lo bien diseñado que esté, es tan fuerte como su eslabón más débil. Como administrador de red, es posible que en algún momento haya sentido que el eslabón más débil en sus configuraciones de seguridad son sus usuarios. En tiempos de incertidumbre, es demasiado humano caer en cualquier noticia que prometa ofrecer alguna información. Por lo tanto, es crucial capacitar a sus usuarios para identificar correos electrónicos de phishing maliciosos con títulos de cebo de clics.

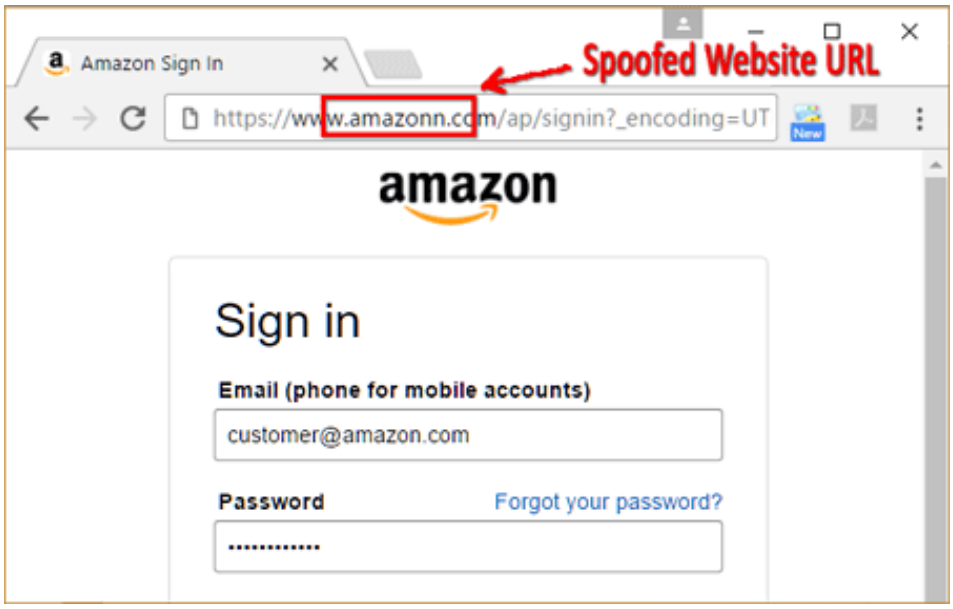
Si desea leer más sobre cómo identificar y mitigar los ataques de phishing temáticos de COVID-19, consulte nuestro e-book.

La situación se ha vuelto más complicada, considerando que muchos de sus usuarios ahora están trabajando remotamente. Aquí hay una lista de medidas que puede tomar para ayudarlos a evitar enlaces maliciosos y mantenerse seguros en línea. Confíe en nosotros, esto también puede contribuir en gran medida a mantener segura la red de su empresa.

- Indique a sus usuarios que desconfíen de cualquier correo electrónico o mensaje que se aproveche de su sentido de miedo, esperanza o curiosidad, especialmente si les pide que hagan clic en un archivo o en un enlace.

- Utilice una red segura para realizar transacciones de cualquier tipo. Evite conectar a wi-fi abierto, especialmente con sus dispositivos de trabajo.

- Preste mucha atención a cualquier sitio donde ingrese credenciales de cualquier tipo. No es inusual que los atacantes clonen sitios web populares como Amazon con un ligero cambio en el dominio para engañar a los usuarios.




Fuente: Certifid.com

## 2. Hacer cumplir las directivas de contraseña segura

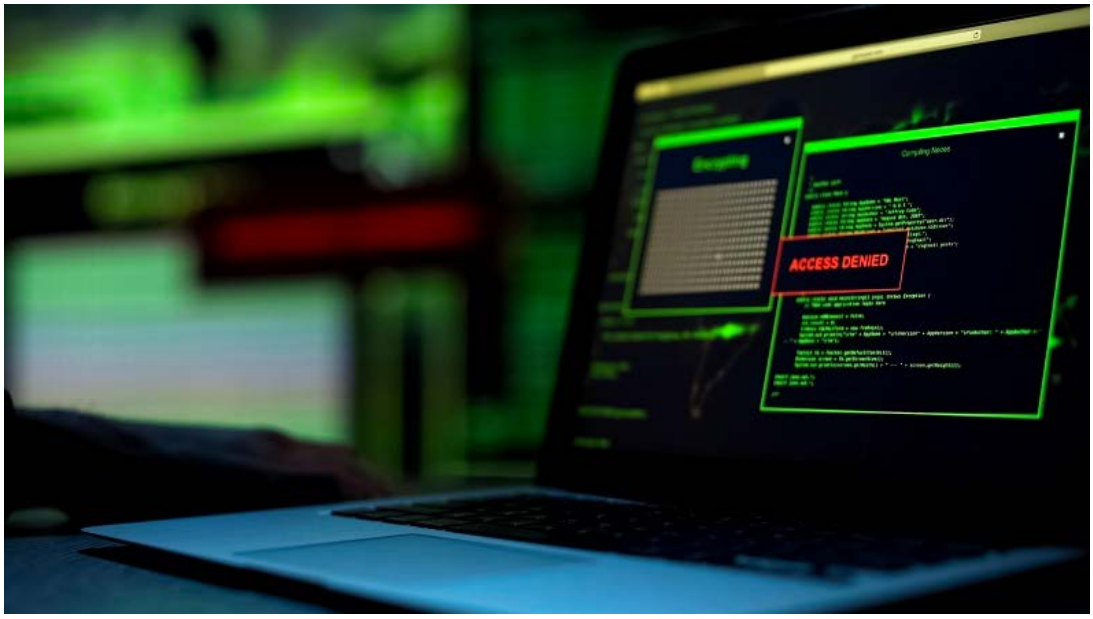

¿Alguna vez se has encontrado con contraseñas como meencantaamiperro? Es probable que alguien de su organización lo haya utilizado en algún momento. Pero, admitámoslo. No es fácil recordar varias contraseñas. Es natural que los usuarios a veces usen contraseñas débiles para recordarlas fácilmente. Por eso, una política de contraseñas segura se vuelve crucial para su postura de seguridad.

- Indique a sus usuarios que eviten el uso de referencias personales en sus contraseñas, como su nombre, su ciudad natal o cualquier información que se pueda obtener de las redes sociales. Un atacante puede usar la fuerza bruta con la ayuda de esta información para reducir el rango de opciones posibles.

- Establezca políticas estrictas de contraseñas que exijan el uso de al menos una letra mayúscula, un carácter especial, un número y un mínimo de 8 caracteres en total. También asegúrese de que estas contraseñas se cambien al menos una vez cada tres meses.

- Indique a sus usuarios que no reutilicen sus contraseñas relacionadas con el trabajo para ninguna otra aplicación, como sitios de comercio electrónico o redes sociales. En caso de una violación de datos en estos sitios, una contraseña para una aplicación crítica estará en el dominio público vinculado a un usuario de su organización.

# 3. El principio de los mínimos privilegios



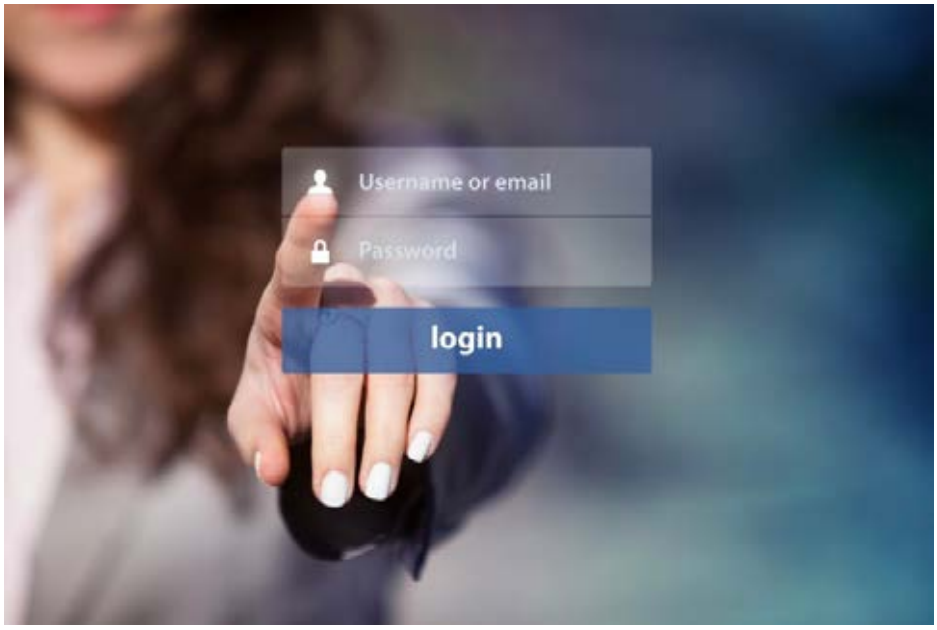

Steve de Marketing a veces solicita acceso a datos financieros. Es posible que sus colegas también lo necesiten. ¿Deberíamos dar el acceso a estos datos a los equipos de marketing y ventas? Este es un escenario que se presentaría con bastante regularidad en las operaciones diarias. Estas preguntas se responden mejor caso por caso, pero siempre es una buena idea adoptar el principio de privilegio mínimo.

- Siempre asegúrese de que cada usuario tenga acceso a la menor cantidad de datos críticos o privilegios de usuario siempre que sea posible. En los casos en que una cuenta de usuario individual se vea comprometida, la extensión del daño será relativamente menor.

- Si está trabajando con AWS, evite usar la cuenta de usuario root para las tareas diarias. Una cuenta de usuario root es una cuenta que se crea cuando se establece su cuenta de AWS. Es siempre mejor crear cuentas de administrador para las tareas diarias. Esto es porque la cuenta root viene con privilegios completos. Restringir el uso de esta cuenta puede ayudar a protegerla de cualquier riesgo.

- Observe de cerca a su administrador y usuarios privilegiados y asegúrese de que no haya casos de escalada de privilegios. En caso de que la cuenta se vea comprometida, esta es una de las primeras cosas que haría un atacante. Si hay una escalada de privilegios, podría haber una infracción. Verifique los logs de su red para descartar la posibilidad de un compromiso, incluso si cree que hay otra explicación.

# 4. Supervisar los logins del dominio




Cualquier red generará miles de registros por segundo. Entendemos que puede ser difícil rastrear todo. De estos registros, los logins de su dominio es esencial, especialmente si hay inicios de sesión únicos.

- Tener un sistema para monitorear los logins inusuales. Si hay varios inicios de sesión desde una cuenta en momentos inusuales, ciertamente vale la pena investigar. Una vez que una cuenta se ve comprometida, el atacante permanece sin ser detectado, a veces durante meses, para extraer la mayor cantidad de datos posible. Verifique los registros de su red para investigar si hay otras actividades sospechosas de la cuenta en cuestión.

- Hacer cumplir una política de bloqueo de cuentas. Si hay varios logins fallidos en rápida sucesión, probablemente sea un ataque de fuerza bruta.

- Aplique la autenticación de dos factores para todos los inicios de sesión de dominio y VPN. Además, asegúrese de que una sesión no dure más de 24 horas, después de lo cual el usuario debe iniciar sesión nuevamente.

# 5. Monitoreo de sus bases de datos críticas

Las bases de datos son los elementos más importantes de la red de una organización, ya que almacenan y procesan los datos comerciales críticos de la empresa. Estos datos son de gran valor para los ciberdelincuentes, que están ideando nuevos métodos para atacarlos todos los días. Por tanto, es fundamental seguir de cerca las actividades en sus bases de datos.

- Supervise de cerca los permisos de los usuarios para asegurarse de que aquí también se aplique el principio de privilegio mínimo. Cuando los permisos y las cuentas de usuario no se administran correctamente, los usuarios pueden obtener derechos elevados y acceso no autorizado a datos confidenciales, que podrán modificar.

- Asegúrese de que todos los parches de seguridad publicados por el proveedor se apliquen lo antes posible. Si no se aplican actualizaciones y parches a su base de datos, su servidor es vulnerable a ciberataques.

- Disponga de una estricta política de gestión de cambios. Por ejemplo, si varios usuarios tienen acceso de escritura a una base de datos, los datos importantes pueden sobrescribirse con valores incorrectos.

# Cómo Log360 puede ayudarle en la seguridad de red

Log360, la solución integral de administración de eventos e información de seguridad puede ayudarle superar los desafíos de gestión de logs y seguridad de red. La solución recoge todos los logs de su red para dar información crítica en forma de informes, gráficos, y alertas. Además de análisis de logs, Log360 se integra con feeds de amenazas se actualiza dinámicamente cada día con millones de direcciones IP, URLs e incluso dominios de phishing que están siendo utilizados por atacantes. La solución también utiliza el aprendizaje automático para detectar cualquier actividad inusual dentro de su red, incluidos los inicios de sesión de dominio y la actividad de la base de datos.

Si cree que una solución de gestión de eventos e información de seguridad (SIEM) le ayudará, puede probar Log360. Además, puede programar una demostración gratuita en la que nuestros expertos en productos responderán a sus preguntas sobre la solución y demostrarán las ventajas de utilizar Log360 en su organización.