

Las 10 principales amenazas a la seguridad de los datos de las PyMEs

El siguiente artículo es un extracto del white paper "Las 10 principales amenazas a la seguridad de los datos de las PyMEs (y qué hacer contra ellas)", de Scott Pinzon, CISSP del equipo LiveSecurity® de WatchGuard®. Este resumen enumera dichas diez amenazas y una contramedida para cada una. Para obtener más detalles sobre cómo seleccionamos las amenazas, a qué tipo de redes están dirigidas y al menos dos contramedidas para cada una, descargue una copia del white paper completo en www.watchguard.com/whitepapers.

Es difícil hallar informes realistas y precisos acerca de lo que realmente implican las amenazas a la seguridad hoy en día para las empresas promedio.

Desde 1999, el equipo LiveSecurity de WatchGuard está monitoreando cada día las amenazas emergentes a la seguridad de las redes, con foco especial en los problemas que afectan a las empresas pequeñas y medianas (PyMEs). Cuando detectamos un problema que podría impactar negativamente en las PyMEs, alertamos a nuestros suscriptores mediante publicaciones por correo electrónico. Dado que nuestros suscriptores tienen poco tiempo porque son profesionales de TI sobrecargados, los alertamos sólo cuando sabemos que un ataque no es meramente factible, sino probable. Este énfasis en el contexto de negocios y en la practicidad hace nuestro servicio prácticamente único. Este enfoque es constantemente refinado mediante el aporte de decenas de miles de suscriptores, estudios de campo en la sede de los clientes, grupos de discusión y grandes sesiones de "seguridad más cervezas".

El resultado: este paper enumera los 10 vectores más comunes de compromiso de datos según nuestra experiencia como analistas de seguridad en PyMEs. También sugerimos técnicas prácticas y defensas para contrarrestar cada uno.

Amenaza # 10: Ataques desde adentro

El equipo de Respuesta ante Intrusiones de Verizon investigó 500 intrusiones en 4 años y pudo atribuir un 18% de las brechas a personal propio corrupto. De ese 18%, cerca de la mitad provenía del personal mismo de TI¹.

Implemente el principio de control dual. La implementación de controles duales significa que, para cada recurso clave, exista un plan alternativo. Por ejemplo, usted puede tener un técnico como responsable principal de configurar su Web y sus servidores SMTP. Pero, por lo menos, las credenciales de login de dichos servidores deben ser conocidas o estar disponibles para otra persona.

Amenaza # 9: Falta de contingencia

Las empresas que se jactan de ser "ágiles" y "receptivas", a menudo alcanzan esa velocidad mediante el abandono de la estandarización, los procesos maduros y el planeamiento de contingencias. Muchas PyMEs descubrieron que un simple fallo o compromiso de los datos se convierte en un desastre cuando no hay Plan de Continuidad de Negocios, Plan de Recuperación ante Desastres, Política de Respuesta ante Intrusiones, sistema de respaldo actualizado *desde el cual realmente se pueda hacer* una recuperación o almacenamiento en otra ubicación.

Mitigación de la falta de planificación

Ciertamente, si usted tiene suficiente presupuesto, debe contratar un experto para ayudarlo a desarrollar metodologías correctas de seguridad de la información. Si no tiene tanto dinero, aproveche el buen trabajo que han hecho otros y modifíquelo para adaptarse a su organización. El proyecto SANS Security Policy ofrece plantillas gratuitas y otros recursos que pueden ayudarlo a escribir sus propias políticas. Para saber más, visite <http://www.sans.org/resources/policies/>.

Amenaza # 8: Una mala configuración que compromete la seguridad

Las PyMEs inexpertas o con poco presupuesto a menudo instalan routers, switches y otros equipos de networking sin involucrar a nadie que entienda las ramificaciones de seguridad de cada dispositivo. En este escenario, un "chico de redes" amateur estará feliz viendo simplemente que el tráfico de datos va exitosamente de un lado a otro. No se le ocurre que debería cambiar las credenciales de usuario y la contraseña por defecto puestas por el fabricante en cada equipo.

¹ Resumido en http://www.infosectoday.com/Articles/2008_Data_Breach_Investigations_Report.htm. Para tener un PDF del informe, visite <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>.

Mitigación de las malas elecciones de configuración

Lleve a cabo una revisión automática que audite vulnerabilidades. Si usted no puede permitirse contratar consultores, probablemente sí pueda por una vez hacer un chequeo automático en su red. Hay muchos productos de "administración de vulnerabilidades" en el mercado, en todos los rangos de precios. Usarlos regularmente debería formar parte de la rutina de mantenimiento de su red.

Amenaza # 7: Uso temerario de redes de hoteles y quioscos

Las redes de los hoteles están notoriamente infectadas con virus, gusanos, spyware y malware y, a menudo, funcionan con malas prácticas globales de seguridad. Los quioscos públicos son un lugar conveniente para que un atacante deje un keylogger, sólo para ver qué cae en su red. Las laptops que no tengan software de firewall personal, antivirus y antispyware pueden verse comprometidas cuando están de viaje. Las defensas tradicionales pueden volverse inútiles cuando el usuario, literalmente, transporta la laptop a lo largo del gateway firewall y se conecta desde el interior de la zona confiable.

Mitigación del uso temerario de las redes de hoteles

Establezca y haga cumplir una política que prohíba a los empleados desactivar las defensas. Según una encuesta encargada por Fiberlink, 1 de 4 "guerreros de las rutas" admitió haber alterado o inhabilitado configuraciones de seguridad en sus laptops. Su política debe ser que los trabajadores nunca desactiven las defensas, a menos que lo llamen y reciban una autorización suya. Muchas soluciones antivirus populares pueden configurarse de modo que no puedan ser desactivadas, aún si el usuario tiene privilegios locales de administrador. Verifique que su actual solución tenga esta capacidad.

Amenaza # 6: Uso imprudente de hotspots inalámbricos

Los hotspots inalámbricos públicos conllevan los mismos riesgos que las redes de los hoteles, e incluso más. Los atacantes comúnmente ponen un acceso inalámbrico no seguro que se anuncia como "Wi-Fi público gratis". Luego esperan que un "guerrero de las rutas" desesperado se conecte. Con un rastreador de paquetes conectado, el atacante puede ver todo lo que el empleado escriba, incluso logins. Este ataque es particularmente nefasto, porque el atacante manda los datos al aire, sin dejar *absolutamente ningún rastro* de compromiso en la computadora de la víctima.

Mitigación del uso imprudente del Wi-Fi

Enseñe a los usuarios a elegir siempre conexiones encriptadas. Haga que se conecten a través de una red privada virtual (VPN). Esto encripta el flujo de datos, de modo que aunque haya fisgones espiando en forma inalámbrica, lo que recibirán será incomprensible.

Amenaza # 5: Datos perdidos en un dispositivo portátil

Gran parte de los datos sensibles se ve comprometida cada año cuando los trabajadores accidentalmente dejan sus teléfonos inteligentes en un taxi, sus memorias USB en un cuarto de hotel o su laptop en un tren de pasajeros. Cuando los datos son almacenados en dispositivos pequeños, es más sabio por parte de los administradores dejar de pensar acerca de lo que harán "si tal aparato se pierde" y, en cambio, pensar "cuando este aparato se pierda...".

Mitigación de la pérdida de datos en dispositivos portátiles

Administre centralizadamente los dispositivos móviles. Considere invertir en servidores y en software que administren en forma centralizada los dispositivos móviles. Blackberry Enterprise Server, de RIM, puede ayudarlo a garantizar que sus transmisiones viajen encriptadas y, si un empleado notifica la pérdida de un teléfono, usted puede eliminar en forma remota los datos del Blackberry extraviado. Este tipo de medidas hace mucho para minimizar el impacto negativo de los dispositivos perdidos.

Amenaza # 4: Servidores Web comprometidos

El ataque de botnets más común hoy se produce contra sitios web y el flanco más débil en muchos de ellos es un código de aplicación mal escrito. Los atacantes comprometen centenas de cientos de servidores de un solo golpe con ataques automáticos de inyección SQL. Los sitios legítimos luego producen la difusión del malware y, sin darse cuenta, esparcen el imperio del amo del bot.

Mitigación del compromiso de los servidores web

Audite el código de su aplicación web. Si (por ejemplo) un formulario Web tiene un campo para que el visitante provea su número telefónico, la aplicación web debería descartar los caracteres en exceso. Si la aplicación web no sabe qué hacer con unos datos o un comando, debería rechazarlos, no procesarlos. Busque la mejor solución que pueda permitirse para auditar código (ya sea un equipo de expertos o una herramienta automática), con énfasis en averiguar si su código hace una adecuada validación de las entradas.

Amenaza # 3: Navegación imprudente por parte de los empleados

Un estudio del 2006 de la Universidad de Washington halló que los sitios que difunden la mayoría del spyware eran (en este orden)

1. Sitios de fans de celebridades (como los que ofrecen lo más actual sobre las locuras de Paris Hilton y Britney Spears);
2. Sitios de juegos casuales (donde uno puede jugar a las damas con un extraño)
3. Sitios porno (que vienen en un sorprendente tercer lugar)

Los sitios de redes sociales como MySpace y Facebook ya han tomado la posta como basureros virtuales de spam, troyanos y spyware. Los empleados que navegan por sitios no relacionados con el negocio terminan invitando a entrar a la red corporativa a clientes de bots, troyanos, spyware, keyloggers, spambots... la gama entera del malware.

Mitigación de la navegación web imprudente

Implemente un filtro de contenidos web. Use software de filtrado web como WebBlocker, de WatchGuard. Las soluciones de filtrado web mantienen bases de datos (diariamente actualizadas) de URLs bloqueados según puntajes de categorías. Más categorías significa más matices. Estas herramientas lo ayudarán a hacer cumplir su Política de Uso Aceptable con tecnología.

Amenaza # 2: Correo electrónico HTML malicioso

El ataque más común por correo electrónico ahora viene como un mensaje en HTML que contiene un enlace hacia un sitio malicioso con alguna trampa caza bobos. Un clic equivocado puede desencadenar una descarga peligrosa. Los riesgos son los mismos que en la Amenaza # 3, "Navegación web imprudente", pero el atacante utiliza el correo electrónico para llevar a la víctima hacia su sitio web malicioso.

Mitigación del correo electrónico HTML malicioso

Implemente un web proxy saliente. Usted puede configurar su LAN para que todos los pedidos de HTTP y las respuestas sean redirigidas hacia un servidor web proxy, lo que provee un punto de choque único donde todo el tráfico web pueda ser monitoreado para ver si es apropiado. El web proxy no interceptará un correo electrónico malicioso entrante pero, si un usuario de su red hace clic en un enlace contenido en ese mensaje en HTML, eso generará un pedido HTTP que el web proxy puede interceptar. Si el pedido HTTP del usuario nunca llega al sitio web caza bobos del atacante, entonces su usuario no se convertirá en víctima.

Amenaza # 1: Explotación automática de una vulnerabilidad conocida

El *Informe sobre investigaciones de filtración de datos* de Verizon del 2008 compila evidencia factual de más de 500 filtraciones de datos a lo largo de 4 años. El equipo RISK de Verizon halló que el 73% de esas filtraciones se produjo gracias a fuentes externas.

Las PyMEs negligentes se convertirán en víctimas si no instalan los parches de Windows en el mismo mes en que se publiquen. Pero su red contiene mucho más que productos de Microsoft. Así que su rutina de parcheado necesita extenderse sistemáticamente a todas las aplicaciones y componentes de sistema operativo que haya en su red.

Mitigación de la explotación automática

Invierta en administración de parches. El software de administración de parches puede ayudarlo a revisar su red, identificar parches faltantes y actualizaciones de software y distribuir parches desde una consola central, incrementando enormemente su posibilidad de tener toda su red actualizada.

Arme una red de pruebas barata. Aún las compañías respetables pueden equivocarse. Por lo tanto, recomendamos instalar un parche en un sistema de prueba y ver cómo se comporta, antes de instalarlo en toda su red. Si usted aún no tiene una red de pruebas, la próxima vez que reemplace computadoras y servidores obsoletos consérvelos y dedíquelos a ser su red de pruebas.

Conclusión

Las contramedidas arriba sugeridas pueden hacer mucho para mitigar su riesgo y proteger su red. Pero son sólo una muestra de los pasos que un administrador de TI diligente puede implementar para incrementar la seguridad de la red. Para ver más consejos acerca de cómo fortificar su red contra los problemas más comunes, descargue una copia gratuita completa del white paper "**Las 10 principales amenazas a la seguridad de los datos de las PyMEs (y qué hacer contra ellas)**" del [sitio web de WatchGuard](#).

WatchGuard® provee dispositivos de seguridad gateway para la administración extensible contra amenazas (XTM) que combaten nueve de las diez amenazas aquí enumeradas (lamentablemente, nuestros dispositivos no pueden evitar que sus empleados pierdan equipos portátiles). Nosotros *podemos* ayudarlo a asegurar su red inalámbrica, chequear la integridad de los clientes que piden acceso a su red, filtrar spam, dar servicios de proxy web, minimizar amenazas internas, crear VPNs y mucho más.

Para más información sobre las soluciones de seguridad de WatchGuard y la protección que proveen contra botnets y otras amenazas a la red, visítenos en www.watchguard.com o contacte a su reseller.

©2008 WatchGuard Technologies, Inc. Todos los derechos reservados. WatchGuard, el logo de WatchGuard, Firebox y LiveSecurity son marcas registradas o marcas comerciales de WatchGuard Technologies, Inc. en los Estados Unidos y/o en otros países. Cualquier otra marca o nombre comercial es propiedad de sus respectivos dueños. Parte. No. WGCE66599_112408