



En la economía global de hoy, los negocios dependen de Internet como nunca antes – las empresas aumentan progresivamente el número de transacciones que se realizan por el comercio electrónico además de facilitar el acceso a sus recursos en red a vendedores, socios comerciales, clientes y empleados remotos. Pero aunque se ha vuelto más conveniente realizar negocios online, esto también conlleva la dificultad de garantizar la seguridad y confianza del intercambio de datos y las comunicaciones. El desarrollo de amenazas de seguridad y el cambio regular de los estándares puede hacer que mantener un ambiente de confianza online sea todo un reto para empresas de cualquier tamaño.

En este documento se presentan nuestras 10 prácticas recomendadas para construir una confianza online tanto dentro como fuera de su negocio. Están focalizadas en las áreas más críticas – desde la implementación de SSL en servidores hasta el establecimiento de políticas y procedimientos de seguridad.

1. Sin encriptación SSL, la integridad de los datos está comprometida.

Despliegue Certificados de Servidor SSL por toda la empresa. SSL es el protocolo de seguridad más ampliamente usado en el mundo. Debería ser implantado en todos los servidores para proteger cualquier información personal y confidencial que circule a través del servidor.

2. Sin una robusta seguridad física y de red, los datos de la corporación se encuentran bajo riesgo de intrusión.

El uso de firewalls, detección de intrusos, software antivirus en los pc clientes, chequeos de virus basados en servidores y mantener actualizados todos los sistemas con parches de seguridad prevendrá que la mayoría de amenazas puedan dañar operaciones, comprometer datos sensibles o amenazar la continuidad de su negocio.

3. Construir un sistema PKI interno tomará tiempo y dinero considerables. Opte por servicios PKI administrados.



Tener servicios de seguridad completamente administrados le permitirá centrarse en aplicaciones necesarias para el desarrollo de su negocio mientras una tercera parte de confianza construye la compleja, segura y cara infraestructura de clave pública y la administra por usted.

4. El software gratuito le vulnerará su contraseña en 30 minutos.

Las contraseñas son débiles y se vuelven cada vez más débiles, haciendo sus sistemas vulnerables. Con software de descarga libre, cualquiera puede crackear un contraseña de 6 caracteres en 30 minutos, o uno de 8 caracteres en 6 horas. reduzca dramáticamente esa vulnerabilidad implementando estrictas normas de uso de contraseñas.

5. El e-mail filtra sus secretos de negocio.

Emita certificados digitales a todos los empleados para firmar y cifrar los e-mails y proteger los datos de empresa e incrementar la confianza en el origen, la autenticidad y confidencialidad de todas las comunicaciones de la empresa. Así mismo no permita el uso de software no-seguro de IM (mensajería instantánea).

6. Las soluciones de control de acceso tradicionales son o inefectivas o costosas.

Reemplace puntos de entrada por contraseña, débiles y que toman mucho tiempo en sincronizar, por sistemas seguros con certificados digitales que son mucho más seguros que los contraseñas, más baratos, e incluso cuando son plenamente administrados, fáciles de implementar. Los certificados SSL aportan autenticidad de identidad en ambos lados: Servidor y Cliente. Los certificados SSL de cliente residen en el navegador



y reemplazan en este caso la entrada via Contraseña. Así mismo requiera certificados de cliente instalados para acceso via VPN.

7. Su sitio web puede ser burlado con un click de ratón.

Proyecte y proteja la identidad de su negocio a través de su sitio web usando una máscara de confianza que establezca identidad y seguridad con los visitantes. Utilice sellos para páginas generados dinámicamente, que no pueden ser copiados, para garantizar la legitimidad, autenticidad y validez vía una llamada activa a una tercera parte de confianza

8. Realizar pruebas en producción es tentar al destino.

Cree una zona desmilitarizada (DMZ) para acordonar el riesgo de las actividades de red de sus sectores de producción crítica de negocio, para todo acceso por modem, para simular producción o para permitir a clientes hacer cualquier prueba de aceptación.

9. En enlace más débil en su seguridad es su gente.

Defina sus protocolos de seguridad. Esta es quizá la norma más pasada por alto y la más temida de las 10, aunque es fácilmente la que más impacto tiene: Póngalos por escrito, comuníquelos e impleméntelos. Documente claramente los procedimientos para acceder a las instalaciones y la red de trabajo, así como para que fines se permite el uso de la red de la compañía y su e-mail.



10. “Nadie en la web puede saber quién eres”.

Empiece usando probadas y maduras tecnologías de autenticación para establecer la identidad de los individuos anónimos que se encuentran en la web. Dinamice su negocio usando transacciones sin papeles. Las organizaciones tienen que ser capaces de autenticar si los consumidores son quienes dicen ser y si tienen la capacidad de generar e-firmas.
