

7 recomendaciones para protegerse de ataques de Ransomware

30 June 2021

1. Comienza analizando tus riesgos.

Hacer frente a los riesgos requiere tenerlos identificados previamente: cuáles son, dónde están y qué consecuencias puede tener sobre mi negocio.

2. Contenido y recepción de emails:

Implementar una política estricta de revisión de correos entrantes que verifique la validez de quién los envía. Establecer un filtro para el contenido de los correos para detectar contenido malicioso y archivos ejecutables, con macros o enlaces web a sitios maliciosos.

3. Gestión de accesos:

El Ransomware no tiene por qué hacerse viral en una empresa. Si se establece un protocolo

de niveles de acceso, con medidas para usuarios generales y otras medidas para usuarios de Sistema, con privilegios de acceso para activos críticos (servidores, aplicaciones, base de datos, etc.) y se refuerza la autenticación multi factor (MFA) cuando sea apropiado (por ejemplo acceso remoto/VPN, y aplicaciones de uso externas).

4. Copias de seguridad de los sistemas

y BBDD: Realizar copias de seguridad frecuentes que sean verificadas y almacenadas de forma segura offline. Utilizar credenciales de acceso sólidas para esos back-ups y almacenarlos de forma segura fuera de las instalaciones. Testear que las copias funcionan correctamente y no

hay problema en restaurar la información.

5. **Formación a los usuarios y**

empleados: Muchos de los ataques buscan el error humano. Formar a los usuarios y empleados identificar intentos de phishing y correos con enlaces o adjuntos maliciosos es de vital importancia. Llevar a cabo ejercicios y simulacros sobre phishing son una forma muy recomendable de entrenar a los equipos.

6. **Actualización y parcheo de sistemas y aplicaciones:**

Es altamente recomendable realizar revisiones de vulnerabilidad y actualizar o parchear

las posibles vulnerabilidades detectadas principalmente en endpoints o puntos de acceso y servidores, especialmente aquellos externos que soportan los sistemas.

7. **Acceso remoto seguro:** Evitar exponer el Remote Desktop Protocol (RDP) directamente en Internet. Es preferible utilizar Remote Desktop Gateway (RDG) o un RDP Seguro autenticado mediante un factor de autenticación múltiple en una red virtual privada (VPN).

The logo for Beazley, featuring the word "beazley" in a lowercase, outlined, serif font.

www.beazley.com

The descriptions contained in this communication are for preliminary informational purposes only. The product is on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd's. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: OG55497).

BZSLXX_US_03/20