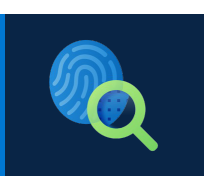
7 Pasos Básicos de Resiliencia Digital

1. Fortalecer credenciales:



La utilización de autenticación de factor múltiple (Multi-Factor Authentication – MFA) reduce la posibilidad de uso indebido o ilícito de credenciales comprometidas en un alto porcentaje. El uso de MFA y de otros mecanismos disponibles para autenticar, autorizar y proteger contra el filtrado de credenciales, reduce el riesgo y aumenta la resiliencia operacional. **Esto no debería ser opcional para los administradores de los servicios y la plataforma; sino un estándar mínimo de seguridad.**

Recomendaciones:

- Habilitar autenticación de factor múltiple (Multi-Factor Authentication - MFA) para usuarios con permisos administrativos en Microsoft Azure, y para contar con acceso condicional automático.
- Minimizar y prevenir el uso de contraseñas débiles, comunes y personalizadas para usuarios administradores de Active Directory (AD).
- Gestionar permisos de usuarios privilegiados a través de Just-in-Time Privilege Identity Management (PIM).
- Incorporar evaluación y mitigación de riesgo de usuario y de inicio de sesión MFA y acceso condicional.

2. Reducir la superficie de ataque:

Dado que el uso de credenciales comprometidas es una condición prevalente, resulta imprescindible deshabilitar el uso de protocolos de seguridad viejos y menos seguros, limitar las vías de acceso a los sistemas, migrar a sistemas de autenticación en la nube, y habilitar controles de acceso administrativo más estrictos. “De nada sirve cerrar la puerta del frente, si se deja abierta la de atrás.”

Recomendaciones:

- Bloqueo de autenticación heredada, incluyendo nuevas herramientas complementarias que liberamos recientemente.
- Monitorear y mejorar la postura de seguridad de sus cargas de trabajo en Azure minimizando la superficie de riesgo.

3. Automatizar la respuesta:

Pensar que un ciberataque sólo va a ocurrir cuando estamos vigilando es un presagio de desastre. Implementar políticas de control de riesgo automáticas reduce la posibilidad de compromiso en un alto porcentaje. Se trata de reducir el tiempo entre la detección de un ataque, y la respuesta al mismo.

Recomendaciones:

- Automatización de respuesta ante alertamientos detección en cargas de trabajo en Azure.

4. Aprovechar las capacidades inteligentes de la nube:

En promedio, los atacantes evitan ser detectados por sus víctimas durante 101 días. La capacidad de registrar y auditar con inteligencia artificial las actividades sospechosas, permite detectar intentos de ataque antes de que sucedan, sean estos externos o internos.

Recomendaciones:

- Habilitar características de seguridad mejoradas de Microsoft Defender for Cloud y monitorear alertamiento.
- Establecer límites de gasto de Azure utilizando las capacidades gratuitas de Azure Cost Management & Billing, de modo que automáticamente se deshabiliten los servicios cuando se llegue al máximo costo permitido.

5. Habilitar Autoservicio:

Se trata de balancear seguridad con productividad, y remover la fricción, empoderando a la organización sin reducir la vigilancia. Dado que el 91% del filtrado de credenciales ocurre vía técnicas de ingeniería social, estos controles aseguran que el tipo de claves de acceso (passwords) utilizadas, las solicitudes de accesos a los recursos y aplicaciones, y el aprovisionamiento de usuarios estén SIEMPRE alineados a las políticas de seguridad de la organización.

Recomendaciones:

- Establecer políticas de gobierno usando Azure Policy y Control de Acceso basado en Rol (Role Based Access Control – RBAC).
- Entrenar usuarios finales en prácticas de seguridad en contra de la ingeniería social.
- Comprender la política de uso de servicios online de Microsoft (Microsoft Product Terms).

6. Reducción de daños que comprometen la cuenta existente:

Recomendaciones:

- Restablecer y cambiar las contraseñas reales de las cuentas con énfasis en las privilegiadas y configurar contraseñas complejas para ellas (mínimo de 12/14 caracteres, incluidos símbolos, números y letras mayúsculas).
- Revisar el acceso de cuentas/aplicaciones a través de registros de auditoría e inicio de sesión de Azure AD. Buscando entradas exitosas/fallidas de diferentes países, así como inicios de sesión simultáneos.

7. Prevención del acceso no autorizado a través del phishing y el compromiso del endpoint:

Recomendaciones:

- Instruir a los usuarios para que estén atentos al phishing y mensajes sospechosos. Los piratas informáticos están explorando el factor humano para obtener acceso a Azure y otros recursos con unos pocos clics. Conoce más sobre las Políticas antiphising de Microsoft.
- Proteja los endpoints tanto como sea posible e incorpore la Estrategia Zero Point.

Todas estas recomendaciones están alineadas con las mejores prácticas de la industria, proveen un ambiente de mitigación mínimo aceptable para prevenir de manera activa usos no autorizados y fraudulentos de recursos de tus aplicaciones e infraestructura de servicios de Microsoft y son consistentes con las recomendadas por organismos reconocidos internacionalmente, como el National Security Agency de los Estados Unidos.